ANEXO I -
MEMORIAL DESCRITIVO TÉCNICO

Outubro / 2026

IMPLANTAÇÃO DO SISTEMA DE DETECÇÃO DE VAZAMENTO (SDV) EM ADUTORAS, TELEMETRIA E SUPERVISÓRIO

1. ESCOPO TÉCNICO

1.1 DO SISTEMA DE MONITORAMENTO E TELEMETRIA

O sistema de telemetria a ser implantado deverá realizar o monitoramento contínuo das variáveis de processo, incluindo vazão, pressão, temperatura, nível e grandezas elétricas associadas às subestações, cabines de medição e conjuntos motobomba.

A arquitetura de comunicação adotada será baseada no modelo IoT do tipo *Publish/Subscribe*, alinhada aos princípios da Indústria 4.0, utilizando o protocolo MQTT *(Message Queuing Telemetry Transport)* como padrão para transmissão e gerenciamento das mensagens entre dispositivos de campo e servidor *broker*.

No âmbito do sistema de telemetria, todas as funcionalidades, customizações, integrações, *scripts*, parametrizações, configurações e demais componentes de software desenvolvidos especificamente para a CONTRATANTE constituirão propriedade intelectual exclusiva da DESO. Ao término da implantação, a CONTRATADA deverá entregar o código-fonte completo do sistema, em formato editável e devidamente documentado, incluindo manuais técnicos e instruções detalhadas para compilação, instalação, configuração, operação e manutenção. Não será admitida qualquer forma de dependência tecnológica, restrição técnica, bloqueio proprietário ou mecanismo que limite ou inviabilize a continuidade de uso,

manutenção, atualização ou evolução do sistema pela CONTRATANTE, diretamente ou por terceiros por ela formalmente designados.

1.2. DO SISTEMA DE DETECÇÃO DE VAZAMENTO (SDV)

O Sistema de Detecção de Vazamentos (SDV) deverá operar por meio do monitoramento contínuo e em tempo real das variáveis hidráulicas de pressão, vazão e temperatura, coletadas em pontos estratégicos definidos em projeto.

Os pontos de monitoramento estabelecidos para cada sistema constituirão a base de dados para a aplicação dos algoritmos de detecção de vazamentos, cabendo à CONTRATADA demonstrar, de forma técnica e fundamentada, a correlação hidráulica entre os pontos monitorados, bem como a coerência do modelo matemático adotado para identificação de anomalias.

A licitante deverá apresentar, em sua proposta técnica, a metodologia e a tecnologia a serem empregadas na detecção de vazamentos, incluindo descrição detalhada de seu princípio de funcionamento, arquitetura do sistema, requisitos operacionais, limitações técnicas, vantagens operacionais e compatibilidade com a solução de telemetria proposta.

O SDV deverá adotar o método de monitoramento interno, sendo implantado exclusivamente por meio de medidores de vazão, pressão e temperatura instalados ao longo das adutoras, conforme indicado nos desenhos técnicos do projeto executivo.

A critério da proponente, e mediante avaliação técnica e aprovação prévia da DESO, poderá ser considerada a instalação complementar de medidores de vazão não intrusivos e/ou medidores adicionais de pressão nas câmaras de interligação das adutoras do São Francisco — tanto em trechos de recalque quanto em trechos por gravidade — bem como nos Tanques de Amortecimento Unidirecionais (TAUs), desde que tal proposição vise assegurar o atendimento aos parâmetros mínimos de desempenho e eficiência do SDV.

Os modelos de equipamentos mencionados neste documento possuem caráter meramente referencial, sendo admitida a utilização de equipamentos tecnicamente equivalentes ou superiores, desde que devidamente comprovada sua compatibilidade e desempenho.

1.2.1 DOCUMENTAÇÃO EXIGIDA

O proponente deverá fornecer, no mínimo:

- Certificado de calibração dos instrumentos rastreável à fábrica;
- Fichas técnicas dos instrumentos;
- Manuais de instalação e operação;
- Memorial de cálculo para os instrumentos propostos considerando os dados de processo das adutoras.

1.2.2 PARÂMETROS DE EFICIÊNCIA DO SDV

- Tempo de detecção ≤ 15 minutos (configurável);
- Sensibilidade mínima de detecção ≤ 1% da vazão medida;
- Precisão de localização ± 5 % da distância entre os medidores de vazão, por trecho da Adutora, podendo ser melhorado com instalação de medição adicional em região intermediária, a critério da empresa proponente;
- Operação Assistida (12 meses);
- Não deverá exceder 01 (um) alarme falso positivo por mês, durante o período de Operação Assitida de 12 (doze) meses. Em caso de alarme falso positivo, a CONTRATADA deverá

relizar uma investigação da causa raíz e executar a recalibração do sistema, sem custo para a DESO;

- Testes reais de vazamento (Spill Tests) deverão ser conduzidos com a equipe DESO;
- Conformidade com as normas API 1130 e API 1175
- SDV ativo em todos os modos de bombeamento: parada, regime permanente e transiente
- Interface OPC UA para integração com supervisório/DCS
- Quatro ou mais métodos independentes de detecção operando em paralelo:
    1. Onda de pressão negativa
    2. Balanço de volume compensado
    3. RTTM – Modelo Transitório em Tempo Real
    4. Monitoramento de queda de pressão em regime transiente;
- Módulos adicionais:
- Tendência histórica de dados de processo e calculados
- Monitoramento de Slack Line (tubulação em canal)
- Monitoramento de MAOP – Máxima Pressão Operacional Admissível
- Visualização do perfil hidráulico
- Arquivamento de dados, eventos e alarmes por no mínimo dois anos
- Sistema interno de relatórios contemplando:
    1. Vazamentos
    2. Falhas de instrumentação
    3. Problemas de comunicação

4. Problemas de sincronização de tempo
5. Relatórios diários com estatísticas de desempenho e disponibilidade
6. Ferramentas de diagnóstico para suporte à identificação e resolução de falhas

1.3 ESTUDO DE RÁDIO ENLACE PARA COMUNICAÇÃO DE RÁDIO

A CONTRATADA deverá elaborar estudo técnico de comunicação por rádio entre os quadros de instrumentação previstos neste escopo, dentro da área de cada uma das localidades atendidas. O estudo deverá contemplar, no mínimo, a análise de propagação do sinal, levantamento de obstáculos físicos, avaliação de possíveis interferências eletromagnéticas, definição da topologia da rede, seleção da faixa de frequência de operação e o dimensionamento dos equipamentos de comunicação necessários. A solução proposta deverá assegurar níveis adequados de confiabilidade, disponibilidade e estabilidade da comunicação entre as unidades do sistema.

A comunicação de cada localidade com o servidor na nuvem é de responsabilidade da DESO.

1.4 DESENHOS DE REFERÊNCIA

– ARQUITETURA GERAL;

– DIAGRAMA P_ID;

– CAPTAÇÃO DO SÃO FRANCISCO – PROPRIÁ E CAIXA DE PASSAGEM;

– QUEBRA CARGA;

– ETAs JOÃO EDNALDO E OVIÊDO TEIXEIRA;

– SISTEMA POXIM.

2. DA VISITA PRÉVIA AO LOCAL

A não realização da vistoria em campo não poderá ser alegada como fundamento para o inadimplento total ou parcial de obrigações previstas em quaisquer documentos integrantes do instrumento convocatório.

3. DO ESCOPO DOS SERVIÇOS

Os serviços objeto da presente licitação compreendem o fornecimento, a montagem, os ensaios, a documentação técnica e a entrega de painéis de automação e telemetria aplicáveis a sistemas de saneamento e monitoramento remoto.

O escopo inclui painéis de telemetria integrados a sistemas supervisórios, utilizando protocolos de comunicação MQTT, assegurando confiabilidade, segurança e integridade dos dados.

4. DA INTEGRAÇÃO COM O C.C.O. - Centro de Controle e Operações

Todas as soluções deverão ser projetadas de forma a garantir plena integração com o novo Centro de Controle Operacional (CCO) multidisciplinar, que será implantado concomitantemente, possibilitando o monitoramento centralizado e em tempo real das informações operacionais.

5. DAS CARACTERÍSTICAS DOS PAINÉIS

Os painéis deverão ser fornecidos completos, incluindo todos os componentes elétricos e eletrônicos, dispositivos de proteção, sistema de alimentação ininterrupta de energia (*no-break*), dispositivos de controle e comunicação, devidamente instalados, parametrizados e testados, em conformidade com as normas técnicas e regulamentações vigentes.

6. DO PROJETO E TESTES

O escopo da contratação inclui o desenvolvimento do projeto executivo, a montagem dos sistemas, a realização dos Testes de Aceitação em Fábrica (TAF), os Testes de Aceitação em Campo (TAC), bem como o treinamento técnico dos profissionais designados pela Contratante.

7. EQUIPAMENTOS DE INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO INCLUÍDOS NO ESCOPO

– Servidores e computadores;

– Licenças de Softwares;

– Firewall , Switchs e Gateways;

8. DAS ADUTORAS E DO SISTEMA DE DETECÇÃO DE VAZAMENTO – SDV

Os sistemas a seguir referem-se às adutoras de água bruta, consideradas estratégicas para o abastecimento da Regional Metropolitana, as quais serão contempladas com monitoramento contínuo no escopo desta contratação.

Cada adutora possui características operacionais próprias, tornando indispensável a implementação de soluções de telemetria e detecção de vazamentos que possibilitem o acompanhamento em tempo real das variáveis hidráulicas. Tais soluções deverão permitir a identificação ágil de eventuais vazamentos, com estimativa do volume perdido e respectivo georreferenciamento, contribuindo para o aumento da eficiência operacional e para a segurança do sistema de abastecimento.

Em cada Estação de Tratamento integrante deste sistema está prevista a instalação de um servidor dotado de um software de visualização e um software historiador, com a finalidade de assegurar o armazenamento local dos dados de processo. Essa estrutura garantirá a

integridade e a continuidade do registro das informações, mesmo em situações de perda de comunicação com o servidor central.

As especificações dos instrumentos e analisadores de água estão detalhados ao final deste documento.

A seguir está descrito o escopo de fornecimento resumido, em cada uma das etapas do projeto. Ver a Planilha de Fornecimento de Materiais e Serviços; e desenhos, para o escopo detalhado.

8.1. SISTEMA SÃO FRANCISCO

8.1.1 ESTAÇÃO DE CAPTAÇÃO DO RIO SÃO FRANCISCO

- Fornecimento, instalação e integração de 02 medidores de vazão;
- Fornecimento, instalação e integração de 02 medidores de pressão;
- Fornecimento, instalação e integração de 01 medidor de nível;
- Fornecimento de instalação e integração de 01 medidor de temperatura;
- Integração do supervisório existente Elipse E3 ao novo supervisório;
- Fornecimento, instalação e integração do painel principal e dos quadros de instrumentação IoT – UTRs 1,2,3,4, e 5;
- Integração das UTRs ao supervisório;

8.1.2 ESTAÇÃO – CAIXA DE PASSAGEM

- Fornecimento, instalação e integração de 04 medidores de vazão;
- Fornecimento, instalação e integração de 04 medidores de pressão;
- Fornecimento, instalação e integração de 02 medidores de nível;
- Fornecimento de instalação e integração de 01 medidor de temperatura;
- Fornecimento, instalação e integração do Painel Principal e dos quadros de instrumentação IoT – UTR 1 e UTR 2;
- Integração das UTRs ao supervisório;

8.1.3 ESTAÇÃO DE QUEBRA-CARGA

- Fornecimento, instalação e integração de 04 medidores de vazão;
- Fornecimento, instalação e integração de 04 medidores de pressão;
- Fornecimento, instalação e integração de 02 medidores de nível;
- Fornecimento de 01 medidor de temperatura da água bruta da adutora;
- Fornecimento, instalação e integração do Painel Principal e dos quadros de instrumentação IoT – UTRs 1,2,3,4;
- Integrar o sistema supervisório existente da empresa VITALUX ao novo supervisório;
- Integração das UTRs ao supervisório;

8.1.4 DERIVAÇÃO PARA O CONSUMIDOR: PETROBRAS

- Fornecimento, instalação e integração de 01 medidor de pressão;
- Fornecimento, instalação e integração de 01 medidor de vazão;
- Fornecimento, instalação e integração de 01 quadro de instrumentação (UTR PETROBRAS);
- Integração da UTR ao supervisório;

8.1.5 DERIVAÇÃO PARA O CONSUMIDOR: STRATOS

- Fornecimento, instalação e integração de 01 medidor de pressão;
- Fornecimento, instalação e integração de 01 medidor de vazão;
- Fornecimento, instalação e integração de 01 quadro de instrumentação (UTR STRATOS);
- Integração da UTR ao supervisório;

8.1.6 ESTAÇÃO DE TRATAMENTO ETA JOÃO EDNALDO

- Fornecimento, instalação e integração de 02 medidores de vazão;
- Fornecimento, instalação e integração de 02 medidores de pressão;
- Fornecimento, instalação e integração de 03 medidores de nível;
- Fornecimento, instalação e integração dos quadros de instrumentação.
- Integração do API da IGUÁ no novo supervisório com as informações dos 03 medidores de vazão de transferência de custódia;
- Integração das UTRs ao supervisório;

8.1.7 ESTAÇÃO DE TRATAMENTO OVIÊDO TEIXEIRA

- Fornecimento, instalação e integração de 01 medidor de vazão;
- Fornecimento, instalação e integração de 01 medidor de pressão;
- Fornecimento, instalação e integração de 01 medidor de nível;
- Fornecimento, instalação e integração dos quadros de instrumentação.
- Integração do API da IGUÁ no novo supervisório com as informações dos 04 medidores de vazão de transferência de custódia;
- Integração ao supervisório/CCO

8.2. SISTEMA POXIM

8.2.1 ESTAÇÃO DE CAPTAÇÃO POXIM – BARRAGEM

- Fornecimento, instalação e integração de 01 medidor de nível;
- Fornecimento, instalação e integração de 01 medidor de vazão;
- Fornecimento, instalação e integração de 01 medidor de pressão;
- Fornecimento, instalação e integração de 01 medidor de temperatura;
- Fornecimento, instalação e integração dos quadros de instrumentação;
- Integração das UTRs ao supervisório;

8.2.2 ESTAÇÃO DE CAPTAÇÃO POXIM – RIO

- Fornecimento, instalação e integração de 01 medidor de nível;
- Fornecimento, instalação e integração dos quadros de instrumentação;
- Configuração de instrumentos de campo e equipamentos IoT;

- Integração das UTRs ao supervisório;
  Obs.: esta captação não tem o SDV, somente o monitoramento.

8.2.3 ESTAÇÃO DE TRATAMENTO DE ÁGUA ETA POXIM

- Fornecimento, instalação e integração de 02 medidores de vazão;
- Fornecimento, instalação e integração de 02 medidores de pressão;
- Fornecimento, instalação e integração de 02 medidores de nível;
- Integração do API da IGUÁ no novo supervisório com as informações dos 02 medidores de vazão de transferência de custódia;
- Fornecimento, instalação e integração dos quadros de instrumentação.
- Integração das UTRs ao supervisório;

9. CENTRO DE CONTROLE OPERACIONAL (CCO)

Implantação de Centro de Controle Operacional (CCO) completo, contemplando o fornecimento, instalação, configuração e comissionamento de toda a infraestrutura tecnológica necessária à supervisão, operação e monitoramento dos sistemas de campo, garantindo a plena operação do processo.

O sistema deverá atender aos requisitos de segurança da informação e cibersegurança estabelecidos pela DESO, assegurando a confidencialidade, integridade, disponibilidade e rastreabilidade dos dados operacionais, em conformidade com as diretrizes e especificações mínimas definidas neste Termo de Referência.

A implantação do CCO deverá contemplar, no mínimo, os seguintes itens e especificações:

9.1. Sistema de Visualização – Videowall

- Fornecimento e instalação de videowall em tecnologia LED ou LCD profissional, composto por 08 (oito) monitores de 50″, configurados em arranjo 4 × 2, com bezel ultrafino e operação contínua 24 horas por dia, 7 dias por semana (24 × 7);
- Estrutura metálica ou chassi dedicado, com sistema de microajustes para alinhamento preciso das telas;
- Controladora de videowall ou matriz HDMI 8 × 8 com suporte a resolução 4K, destinada ao gerenciamento das fontes de vídeo;
- Fornecimento de cabos HDMI e/ou DisplayPort, considerando reserva técnica mínima de 10%;
- Fornecimento e instalação de cabos de alimentação elétrica, canaletas, eletrocalhas e tomadas no padrão ABNT;
- Serviços de instalação, configuração e alinhamento do videowall.

9.2. Mobiliário Operacional e Ergonomia

- Fornecimento de mesa tipo console para operação, com 3 (três) postos de trabalho, dotada de calha técnica embutida para passagem organizada de cabos;
- Fornecimento de 3 (três) cadeiras ergonômicas, em conformidade com os requisitos da NR-17 – Ergonomia;
- Fornecimento de 6 (seis) braços articulados para fixação de monitores auxiliares, permitindo ajustes de posição e ergonomia para os operadores;
- Fornecimento de apoios para os pés, porta-copos e gaveteiros, visando melhores condições ergonômicas e organização do ambiente de trabalho.

10. OBRIGAÇÕES DA CONTRATADA

- Garantir que todas as atividades sejam realizadas em conformidade com as Normas, regulamentos e protocolos operacionais de Saúde e Segurança do Trabalho da DESO e da legislação vigente.
- Dimensionar, planejar e gerenciar a equipe necessária para cumprir o cronograma de implantação previamente apresentado;
- Participar de reuniões de acompanhamento da evolução do contrato, que poderão ser semanais ou mensais. A critério exclusivo da DESO, as reuniões poderão ser presenciais ou por meio de videoconferência.
- Fornecer todos os materiais, equipamentos, licenças de softwares e mão de obra técnica necessária à execução dos serviços;
- Garantir suporte técnico e manutenção corretiva durante o período de operação assistida;
- Elaborar e entregar manual de operação e manutenção preventiva dos sistemas implantados, com cronograma recomendado;
- Manter obrigatoriamente no canteiro de obras, frente de trabalho ou local de serviços, material necessário à prestação de primeiros socorros e pessoas treinadas para este fim, conforme NR-07;
- Assegurar a compatibilidade dos sistemas com os protocolos e plataformas utilizados pela DESO (Modbus, OPC, MQTT, supervisório, HTTPS);
- Atender aos requisitos de segurança da informação e cibersegurança exigidos pela DESO, incluindo uso de VPN, autenticação, criptografia e controle de acessos.
- A comunicação dos dispositivos de campo deverá ser estabelecida diretamente com os servidores da DESO, ou seja, os dados monitorados não poderão passar ou serem compartilhados com nuvem de terceiros.

- Os dados de Pressão, Vazão, Temperatura, Qualidade da Água, etc, coletados deverão ser integrados ao software supervisório a ser fornecido, onde serão tratados, armazenados e disponibilizados aos usuários finais.
- A Contratada deve levar em consideração que a presente contratação se refere ao fornecimento da solução completa do equipamento de telemetria e a conectividade necessários ao pleno funcionamento do monitoramento, em tempo real, dos respectivos pontos definidos nesta especificação com todas as informações incorporadas ao Sistema Integrado de Supervisão do CCO.
- A Contratada deve levar em consideração, que o escopo de fornecimento compreende todos os equipamentos, acessórios, materiais, obras civis e serviços necessários à implantação do monitoramento aqui definidos dentre os quais, destaca-se:

  – Comissionamento, aferição e integração dos pontos de monitoramento com o Sistema Integrado de Supervisão do CCO (Software supervisório); elaboração, comissionamento e testes de interfaces gráficas, históricos e alarmes para monitoramento do sistema implantado, nos softwares supervisório. As representações gráficas a serem implementadas devem ser aprovadas pela DESO, com o intuito de promover a padronização;

11. OBRIGAÇÕES DA CONTRATANTE (DESO)

- Fornecer acesso físico e documental às áreas e instalações envolvidas na execução do contrato;
- Acompanhar e fiscalizar a execução contratual;
- Dar apoio nas intervenções e interligações em redes pressurizas para instalação de medição de pressão e sensores de ruídos, a serem executadas pela CONTRATADA
- Designar equipe técnica responsável pelo acompanhamento, recebimento e validação das entregas;

- Assumir, na contratação, todas despesas relativas as licenças do provedor do sistema supervisório, necessárias relativa ao monitoramento dos respectivos TAGs, assim como ao número de permissões de acessos ao sistema quando houver;
- Realizar as aprovações necessárias dentro dos prazos definidos no cronograma;
- Realizar auditoria, a seu critério, dos dados de disponibilidade dos equipamentos e sensores fornecidos pela CONTRATADA;
- Apurar mensalmente a disponibilidade dos equipamentos e sistemas de telemetria implantados, a partir do relatório fornecido pela CONTRATADA, para realização dos respectivos pagamentos conforme cronograma financeiro vinculado ao avanço físico das etapas e medições, de acordo com os critérios definidos neste presente Termo de Referência.

12. COMISSIONAMENTO

O processo de comissionamento consiste em todas as atividades necessárias a integração, configuração e testes do equipamento de telemetria implantado. Tem como objetivo garantir que o monitoramento operará de forma correta e satisfatória, conforme especificações, normas técnicas e de segurança, aplicáveis.

- A CONTRATADA deve realizar o comissionamento de todos os itens que compreendem o seu escopo de fornecimento, separadamente e de forma integrada.
- Compreendem o comissionamento dos pontos de telemetria, no mínimo, as seguintes etapas, que devem ser executadas pela CONTRATADA:

I) levantamento das informações necessárias à elaboração dos tópicos MQTT e caraterização do local de implantação;

II) levantamento das informações dos instrumentos e equipamento de telemetria, inclusive as informações para gestão dos ativos;

III) elaboração do mapa de memória para o mapeamento MQTT;

IV) realizar o mapeamento MQTT no software supervisório;

V) fazer a validação dos dados transmitidos pelos equipamentos de telemetria e os dados recebidos no software. Nesta etapa, a equipe de campo da CONTRATADA deverá validar junto a equipe de integração também da CONTRATADA, se os dados recebidos estão consistentes. Para o caso da medição de vazão, o valor recebido e tratado no software supervisório (volume acumulado e vazão média – calculada) deve ser validado com as informações do display do medidor. Para o caso da medição de pressão, durante o comissionamento, deve ser utilizado medidor de pressão digital de precisão para que, em comparação com o sensor de pressão implantado, seja validado o valor recebido no software supervisório. O mesmo procedimento deve ser seguido às variáveis de qualidade da água quando aplicáveis;

VI) Realizar a integração do ponto de monitoramento implantado ao software supervisório;

VII) A partir da integração dos dados no software supervisório dará início ao período de avaliação da disponibilidade do ponto de monitoramento para aceite da implantação, conforme descrito neste TR.

13. SEGURANÇA DA INFORMAÇÃO

A CONTRATADA deve zelar pela integridade e sigilo das informações que lhes forem disponibilizadas tratando-as como sigilosas, não estando a mesma autorizada a repassá-las a terceiros. A CONTRATADA deverá emitir termo de confidencialidade assinado por todos os profissionais da mesma que trabalhão no projeto, o modelo do termo de sigilo será disponibilizado pela DESO.

Em hipótese alguma a CONTRATADA poderá copiar ou obter informações dos servidores da DESO sem a expressa autorização, formal e específica, da CONTRATANTE.

Todos os dados trafegados na nuvem devem obedecer e ter conformidade com políticas de cibersegurança da DESO.

14. REFERÊNCIAS NORMATIVAS

Todos os serviços e equipamentos devem observar, no mínimo, as seguintes normas e regulamentações, nas suas versões mais atualizadas:

- Normas técnicas da ABNT (Associação Brasileira de Normas Técnicas);
- Normas de segurança do trabalho (NRs do Ministério do Trabalho);
- ABNT NBR 5410 – Norma de Instalações Elétricas de Baixa Tensão;
- ABNT NBR 5419 – 1,2,3,4 – Norma de proteção contra descargas Atmosféricas.

Normas Regulamentadoras do Ministério do Trabalho e Previdência:

- Normas de Medicina e Segurança do trabalho;
- NR 05 – Formação Básica de Membros de CIPA;
- NR 06 – Utilização, guarda e higienização de EPI;
- NR 07 – Programa de Controle Médico de Saúde Ocupacional (PCMSO).

- NR 10 – Segurança em instalações e serviços em eletricidade;
- NR 12 – Operações em máquinas e Equipamentos, Direção Defensiva;
- NR 15 – Atividades insalubres;
- NR 18 – Condições e Meio Ambiente de Trabalho na indústria da Construção;
- NR 23 – Prevenção e Combate a Princípio de Incêndio;
- NR 24 – Condições Sanitárias e de Conforto nos Locais de Trabalho do Ministério do Trabalho e Emprego;
- NR 33 – Segurança em Espaço Confinado, Supervisor de Entrada em Espaço Confinado;
- NR 35 – Trabalho em altura.
- ABNT NBR IEC 61439 – Conjuntos de manobra e controle de baixa tensão;
- ABNT NBR IEC 60068-2-60 – Ensaio de conformal coating;
- ABNT NBR IEC 61511 – Sistemas instrumentados de segurança;
- ABNT NBR IEC 62381 – Testes de aceitação de sistemas;
- NTS0266 – Norma Geral para Quadros Elétricos; NFPA 36 – Requisitos de segurança industrial.

16. PROJETO EXECUTIVO

A CONTRATADA deverá elaborar e entregar o projeto executivo completo, com memoriais, diagramas, listas de materiais e desenhos 2D. Os arquivos deverão ser fornecidos em formatos editáveis (.docx,.xlsx,.dwg,.stp).

17. GARANTIA

A CONTRATANTE deverá dar garantia mínima de 12 meses para todos os componentes e equipamentos, incluindo substituição de peças e suporte técnico remoto durante o período.

18. SUPORTE TÉCNICO E NÍVEL DE SERVIÇO SLA – Service Level Agreement (Acordo de Nível de Serviço)

A CONTRATADA deverá disponibilizar suporte técnico pelo período mínimo de 365 (trezentos e sessenta e cinco) dias após a entrega definitiva da obra, com a finalidade de assegurar o pleno funcionamento dos sistemas fornecidos, bem como prestar apoio à operação e manutenção dos equipamentos, softwares e infraestrutura implantados.

Durante o período de suporte, deverão ser observados os seguintes níveis de serviço (SLA):

18.1. Disponibilidade de atendimento

- Atendimento remoto: disponibilidade 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, para registro de chamados, diagnóstico de falhas, suporte operacional e orientação técnica à equipe da CONTRATANTE.
- Atendimento presencial: quando constatada a impossibilidade de solução remota, a CONTRATADA deverá disponibilizar atendimento presencial no prazo máximo de 24 (vinte e quatro) horas após a solicitação da CONTRATANTE.

18.2. Classificação de criticidade dos chamados

Os chamados técnicos deverão ser classificados conforme o impacto na operação do sistema:

- Criticidade Crítica: falha total ou indisponibilidade de sistema ou equipamento essencial à operação.

- Criticidade Alta: falha que comprometa parcialmente a operação ou reduza significativamente o desempenho do sistema.
- Criticidade Média: falha que não comprometa a operação principal, mas que exija correção para restabelecimento pleno das funcionalidades.
- Criticidade Baixa: solicitações de ajuste, esclarecimentos ou melhorias que não impactem diretamente a operação.

18.3. Tempo de resposta e solução

Criticidade	Tempo Máximo de Resposta	Tempo Máximo de Solução
Crítica	até 2 horas	até 12 horas
Alta	até 4 horas	até 24 horas
Média	até 8 horas	até 48 horas
Baixa	até 24 horas	até 3 dias úteis

O tempo de resposta corresponde ao período entre a abertura do chamado e o início do atendimento pela CONTRATADA. O tempo de solução corresponde ao período necessário para restabelecimento do funcionamento normal do sistema ou aplicação de solução de contorno aceitável pela CONTRATANTE.

18.4. Registro e acompanhamento de chamados

Todos os atendimentos deverão ser registrados em sistema de gestão de chamados ou meio formal de comunicação, contendo no mínimo:

- data e hora de abertura do chamado;
- descrição da ocorrência;
- classificação de criticidade;
- ações realizadas;
- data e hora de solução.

18.5. Canais de atendimento

A CONTRATADA deverá disponibilizar canais formais de suporte, tais como:

- telefone;
- e-mail;
- sistema eletrônico de abertura e acompanhamento de chamados.

18.6. Penalidades por descumprimento do SLA

O descumprimento dos prazos estabelecidos neste SLA poderá implicar aplicação de penalidades contratuais, conforme definido no contrato administrativo, sem prejuízo de outras sanções previstas na legislação aplicável.

ESPECIFICAÇÕES TÉCNICAS

19. ESPECIFICAÇÕES DOS EQUIPAMENTOS / INSTRUMENTOS DE MONITORAMENTO E SOFTWARES

Os equipamentos deverão ser **novos, com garantia mínima de 12 meses**, assistência técnica disponível no Brasil, e conformidade com normas técnicas e ambientais.

19.1 Todos os equipamentos deverão atender as especificações mínimas constantes a seguir;

19.2 ESPECIFICAÇÃO TÉCNICA – INSTRUMENTOS DE MEDIÇÃO

19.2.1 Medidores de Vazão – Adutoras do São Francisco

Os medidores de vazão serão do tipo ultrassônico clamp-on não intrusivo, com as seguintes especificações mínimas:

- Caminho único de medição, com possibilidade de utilização de 2 a 4 pares de sensores por medição
- Método de medição: tempo de trânsito absoluto e diferencial
- Alimentação: 90–240 V
- Sinais de saída: RS485 Modbus, saída de pulso e saídas analógicas (4–20 mA / 0–20 V)
- Transmissão digital e em rede via tecnologia NBHS ou equivalente
- Precisão: ±1% do valor medido ±0,005 m/s (calibração em campo)
- Repetibilidade: 0,3%
- Turn-down: até 400:1
- Faixa de velocidade: 0,01 a 10 m/s

19.2.2 Medidores de Vazão – Adutoras Poxim e Cabrita

Os medidores de vazão serão do tipo eletromagnético, com as seguintes especificações mínimas:

Modelo de referência: Schneider – Electric - 9500A Magnetic Flow Tube ou equivalente.

- Conexões flangeadas conforme ABNT NBR 7675, ISO 7005 ou equivalente
- Classe de pressão D AWWA (28” a 78”)

- Eletrodos em aço inoxidável AISI 316L (mínimo)
- Transmissor compacto ou remoto, montagem em parede ou pedestal
- Grau de proteção IP66 (transmissor) e IP67 (sensor)
- Alimentação: 100–230 VAC – 50/60 Hz
- Exatidão: ±0,3% do valor medido ±1 mm/s
- Repetibilidade: ≤ ±0,1%
- Faixa de velocidade: 0,3 a 10 m/s

Requisitos mínimos:

1. 01 saída analógica 4–20 mA
2. 01 saída pulso/frequência
3. Comunicação RS485 – Modbus RTU integrada
4. Saídas eletricamente isoladas

Características obrigatórias:

1. Indicação local de vazão instantânea
2. Totalizador
3. Corte para baixa vazão
4. Detecção de tubo vazio
5. Operação em ambiente externo (-10 °C a +60 °C)

19.2.3 Transmissores de Pressão

Os transmissores serão do tipo dois fios (alimentação pelo loop) com comunicação digital integrada.

Modelos de referência: Schneider Electric – IAP10S, IGP10S, IDP10S ou equivalentes.

1. Medição de pressão manométrica
2. Precisão: ±0,05% do valor medido
3. Repetibilidade: ≤ ±0,05% F.E.
4. Estabilidade: ≤ ±0,03% F.E./ano por 10 anos
5. Tempo de resposta: ≤ 100 ms
6. Turn-down: até 400:1
7. Adequado para loops SIL 2
8. Saída: RS485 – Modbus RTU
9. Operação single loop ou multidrop
10. Alimentação: 12–42 Vcc (loop powered)

Recursos adicionais:

- Ajuste local de zero e span
- Diagnóstico interno do sensor
- Configuração via RS485 – Modbus RTU ou software
- Proteção contra inversão de polaridade

19.2.4 Transmissores de Temperatura

Modelo de referência: Endress & Hauser - TMT142B ou equivalente.

- Entrada universal compatível com RTD, termopares, resistência e mV
- Alimentação: 11–36 Vcc
- Interface de saída: RS485 – Modbus RTU

- Precisão ≤ 0,1 K para Pt100
- Isolação galvânica entre entrada e saída
- Display local retroiluminado

Diagnóstico avançado conforme NAMUR NE107

19.2.5 Transmissor de Nível Ultrassônico

Modelo de referência: Alfacomp – TUN21-R ou equivalente.

- Faixa de medição: até 20 m
- Alimentação: 12 a 24 Vcc
- Saída: RS485 – Modbus RTU
- Precisão: 0,3% fundo de escala
- Classe de proteção: IP 67
- Material do invólucro: ABS
- Temperatura de operação: -10 a +60 °C

19.2.6 GATEWAY DE COMUNICAÇÃO – MODBUS RTU / MQTT

Modelo de referência: Westcon – IG502 ou equivalente.

MODEL	IG502
CPU	ARM Cortex-A8 600MHz
RAM	512MB
Storage	8GB
ETH	2x 10/100Mbps

Serial Port	1x RS-232 1x RS-485 or 2x RS-485
I/O	4x digital/ pulse input 3x digital/ pulse output 1x DO
Cellular Type	CAT1, CAT4, 5G (China only)
Wi-Fi	STA/AP, 2.4G (802.11 b/g/n)
Protocols	Modbus RTU e TCP, EtherNet/IP, Siemens, OPC UA MQTT, Sparkplug B, DNP3 e outros.
Open Platforms	Python

19.2.7 GATEWAY DE COMUNICAÇÃO – ABNT 14522 / MODBUS RTU

Este gateway de comunicação é desenvolvido para integração entre medidores de tarifação de energia elétrica baseados no padrão NBR-14522 (CODI/ABNT) via SSU e redes RS-485 (Modbus RTU) ou Wi-Fi/Ethernet (Modbus TCP). Os dados podem ser acessados por CLPs ou sistemas supervisórios (SCADA), permitindo monitoramento local eficiente.

Modelo de referência: IMS – PowerNET A-956

Características Elétricas

Parâmetro	Especificação
Alimentação	9 ~ 30 VDC
Consumo	5 VA

Características Mecânicas

Parâmetro	Especificação
Fixação	Trilho DIN 35 mm
Material	ABS, V-0 UL94
Dimensões (A x L x P)	110 x 141 x 40 mm
Peso Aproximado	145 g
Grau de Proteção	IP20

Condições Ambientais

Parâmetro	Especificação
Temperatura de Operação	-10°C a 60°C
Temperatura de Armazenagem	-10°C a 75°C
Umidade Relativa	Até 90% sem condensação

Comunicação – Wi-Fi

Parâmetro	Especificação
Padrão	IEEE 802.11 b/g/n
Banda	2,4 GHz
Protocolo	Modbus TCP

Comunicação – Ethernet

Parâmetro	Especificação
Tipo	10/100 Mbps
Taxa Efetiva	50 kbps
Conector	RJ-45
Protocolo	Modbus TCP

Comunicação – RS-485 (Modbus)

Parâmetro	Especificação
Número de Portas	1
Padrão Elétrico	RS-485
Velocidade	2400 bps a 115200 bps
Stop Bits	1 ou 2
Bits de Dados	8
Paridade	Nenhuma, Par ou Ímpar

Protocolo	Modbus RTU

Comunicação – SSU (Física)

Parâmetro	Especificação
Número de Portas	1
Interface	Física
Velocidade	110 bps
Protocolo	NBR-14522

Itens Inclusos

• Conector BLZ fêmea de 12 vias

19.2.8 SENSOR DE NÍVEL HIDROSTÁTICO

Um sensor de nível hidrostático é um dispositivo que mede o nível de líquidos com base na pressão gerada pelo peso da coluna de líquido. Essa pressão é diretamente proporcional à altura do líquido, o que permite ao sensor calcular a profundidade do líquido em questão. O sensor é geralmente instalado na parte inferior de um tanque ou reservatório, onde ele detecta a pressão exercida pela coluna de líquido sobre a sua célula de medição.

O funcionamento do sensor de nível hidrostático está relacionado à física dos fluidos. Quando um líquido é armazenado em um recipiente, a pressão exercida pelo líquido nas partes inferiores do recipiente é maior à medida que a profundidade aumenta. O sensor de nível

hidrostático é projetado para medir essa pressão e converter as informações em uma leitura que pode ser utilizada para determinar o nível do líquido.

Transmissor de Nível Hidrostático tipo sonda, fabricado em aço inoxidável 316, com precisão de 0,5% F.E (opcional 0,25% F.E), cabo ventilado no material PU ou PE.

Material do invólucro em aço inoxidável AISI 316 L sensor piezo-resistivo com diafragma material AISI 316, aplicável para tratamento de água e esgoto:

- Material do corpo em inox 316
- Grau de Proteção: IP-68
- Cabo blindado especial com compensação atmosférica
- Prensa cabo: sugestão de 26x2 AWG
- Vedação anel o'ring, borracha nitrílica
- Sensor piezorresistivo 316 L
- Sinal de saída 4 a 20 mA a 2 fios
- Alimentação de 8 a 45 VCC ligação a 2 fios
- Sobre pressão: 2 x fundo de escala ou opcionais 3 x ou 4 x o fundo de escala.
- Montagem suspensa
- Precisão do sinal: < 0,1%
- Tempo de resposta = ou < 1 milissegundo
- Frequência superior ou igual a 200 Hz
- Resolução de saída analógica infinita
- Temperatura do fluído: -20 + 115ºC (opcional até 400ºC)
- Temperatura de operação: 0 a 70ºC
- Impedância: 600 Ohms
- Temperatura do invólucro: Máx. 100ºC
- Proteção contra inversão de polaridade e contra rádio frequência
- Proteção contra surto, limitador de corrente, imune a descargas eletromagnéticas, radiação

de campo eletromagnético e a transientes rápidos
- Precisão: (Histerese, Repetibilidade, Linearidade) 0,5% F.E.
- Livre de calibração
- Faixa de medição de pressão manométrica: 0-10 mca
- Comprimento do cabo: 30 metros

19.2.9 RÁDIO MODEM SERIAL

Permite cobrir longas distâncias com links estáveis e confiáveis. Recursos avançados, tais como Multiple Data Stream, Channel Sharing e Network Bridging, otimizam a transmissão de dados e a utilização da banda.

Funções de Repetidor, Bridge Ethernet e Redundant Hot Stand-by são recursos de série destes rádios. Podem operar também como Gateway Serial (Serial Server), possibilitando a comunicação simultânea de dados via porta serial (protocolo Modbus, por exemplo) e Ethernet.

As duas antenas e o multiplexador interno permitem transmitir e receber dados simultaneamente, melhorando ainda mais a performance da comunicação.

Modelo de referência: Schneider Electric - TRIO J SERIES

Especificações de Rádio

- Faixa de Frequência: 902–928 MHz
- Precisão de Frequência: ±2,5 ppm (900 MHz), ±3,0 ppm (2,4 GHz)
- Modos de Operação: Half Duplex, Pseudo Full Duplex
- Seletividade: >50 dB
- Resposta Espúria: >70 dB
- Modulação: GFSK nível T2
- Potência de Transmissão (900 MHz): 0,01–1 W (+30 dBm), configurável em passos de 0,5 dB

- Potência de Transmissão (2,4 GHz): 0,01–500 mW (+27 dBm), configurável em passos de 0,5 dB

Conexões e Interfaces

- Ethernet: 2 x RJ45 10/100 Mbps (IEEE 802.3, auto-MDIX)
- Serial: 1 x RS232 DB9 (600–115.200 bps assíncrono)
- Controle de Fluxo: CTS/RTS (Porta A) ou interface de 3 fios
- Antena: 2 x conectores TNC fêmea
- Conector de Alimentação: 2 pinos com trava (fornecido)
- Indicadores LED: Pwr, Tx, Rx, Sync, TxD, RxD e LEDs LAN

Recursos Ethernet

- Protocolos: UDP, TCP, DHCP, ARP, ICMP, STP, IGMP, SNTP, TFTP
- Repetição Ethernet: Ponto a Ponto com autoaprendizado automático
- Filtragem de Tráfego: Filtragem configurável por MAC e Unicast
- Compressão: Desligado / Baixo / Médio / Alto
- Servidor Terminal: RS-232 embarcado via UDP/TCP
- Gateway MODBUS: Modbus TCP para Modbus RTU embarcado
- DHCP: Modos Automático e Manual
- SNMP: Compatível com V1/V2c RFC-1213

Desempenho do Modem

- Taxa de Dados RF (900 MHz): 512 / 256 / 128 / 64 kbps
- Taxa de Dados RF (2,4 GHz): 256 / 128 / 64 kbps
- Taxa de Erro de Bit (BER): $<1x10^{-6}$ (dependente da taxa de dados)
- Modos de Operação: Access Point, Remoto, Repetidor, Ponte de Rede
- Tipos de Rede: Ponto-a-Ponto (PtP), Ponto-Multiponto (PtMP), PtMP com Repetidores, Malha (Mesh)
- ChannelShare™ – Sistema de prevenção de colisões

- SmartPath™ – Tecnologia de redundância em malha
- Atualização de Firmware: Local e Over-the-Air (OTA)

Segurança

- Criptografia: AES 256 bits
- Interface HTTP/HTTPS protegida por senha
- Telnet, SSH e Console Serial seguros
- Operação opcional com Access Point confiável (Trusted)

Diagnóstico e Monitoramento

- Gerenciamento remoto de rede (sem necessidade de software adicional)
- Acesso SNMP aos diagnósticos do rádio
- Analisador de Espectro e Bloqueio de Canal
- Compatível com software TVIEW+™
- Parâmetros disponíveis: Potência TX, RSSI, Tensão de Alimentação, Erro de Frequência, Temperatura, VSWR (900 MHz)

Especificações Gerais

- Temperatura de Operação: -40 a +70 °C
- Alimentação: 13,8 Vcc nominal (faixa 10–30 Vcc)
- Corrente de Transmissão: 800 mA nominal
- Corrente de Recepção: <150 mA nominal
- Dimensões: 100 x 34 x 165 mm
- Gabinete: Estrutura robusta em liga metálica fundida

19.3. EQUIPAMENTOS DE TI

19.3.1 ELEMENTOS ATIVOS E DE SEGURANÇA

ITEM	DESCRITIVO	Unidade	Quantidade
1	Firewall DataCenter (Modelo 1)	unid	2
2	Firewall CCO (Modelo 2)	unid	2
3	Firewall Industrial (Modelo 3)	unid	8
4	Equipamento de Comutação Industrial de 16 portas – PoE	unid	6
5	Equipamento de comutação de 24 portas Ethernet	unid	2
6	Centralizador e Analisador de Logs com Visibilidade e Proteção para Protocolos Industriais	unid	1
7	Solução Avançada de Acesso Remoto Seguro	unid	1
8	Solução Avançada de Segurança de Simulação de Ambiente Industrial	unid	1

1. **Características gerais para os equipamentos de Next Generation Firewall (NGFW) – Modelos 1, 2 e 3**
   1.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW), não sendo permitido appliances virtuais ou solução open source (produto montado);
   1.2. Todos os equipamentos NGFW devem ser do mesmo fabricante para garantir compatibilidade com a gestão centralizada;
   1.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

1.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
1.5. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
1.6. Para Telnet e SSH, deve haver opção de configurar a interface de origem ao executar o acesso remoto;
1.7. Os dispositivos de proteção de rede devem possuir suporte a VLANs;
1.8. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
1.9. Deve suportar BGP, OSPF, RIP e roteamento estático;
1.10. Para BGP (IPv4 e IPv6), deve suportar o anúncio apenas quando determinadas condições forem atendidas;
1.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
1.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
1.13. Deve suportar DHCP em IPv4 e IPv6;
1.14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
1.15. Deve suportar tabelas independentes de roteamento, por contexto de firewall;
1.16. Deve suportar NAT dinâmico (Many-to-Many);
1.17. Deve suportar NAT estático (1-to-1);
1.18. Deve suportar NAT estático bidirecional 1-to-1;
1.19. Deve suportar Tradução de porta (PAT);
1.20. Deve suportar NAT de Origem;
1.21. Deve suportar NAT de Destino;
1.22. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
1.23. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
1.24. Deve suportar NAT64;

1.25. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

1.26. Enviar log para sistemas de monitoração externos;

1.27. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

1.28. Proteção anti-spoofing;

1.29. Deve haver suporte ao protocolo ICAP, inclusive de forma segura (SSL);

1.30. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

1.31. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

1.32. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;

1.33. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

1.34. Controle, inspeção e decriptografia de SSL para tráfego de Saída (Outbound);

1.35. A solução deve suportar integração nativa com Let’s Encrypt, para obtenção de certificados válidos, de forma automática;

1.36. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;

1.37. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

1.38. A solução de firewall deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

1.39. A solução de firewall deve permitir integração com threat feeds externos. Suportar ao menos listas de IPs, hashes de malwares e domínios;

1.40. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

1.41. Deve possuir integração com soluções de NAC, para autenticação SSO no firewall de elementos registrados no NAC e execução de políticas de compliance na VPN.

-

1.42. **Políticas**

1.42.1. Deverá suportar controles por zonas de segurança;

1.42.2. Deverá suportar controles de políticas por porta e protocolo;

1.42.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

1.42.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

1.42.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

1.42.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

1.42.7. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

1.42.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

1.42.9. Suporte a objetos e regras IPV6;

1.42.10. Suporte a objetos e regras multicast;

1.42.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

1.43. **Controle de Aplicações**

1.43.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

1.43.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

1.43.3. Reconhecer pelo menos 3000 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

1.43.4. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

1.43.5. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

1.43.6. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

1.43.7. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

1.43.8. Identificar o uso de táticas evasivas via comunicações criptografadas;

1.43.9. Atualizar a base de assinaturas de aplicações automaticamente;

1.43.10. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

1.43.11. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

1.43.12. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

1.43.13. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

1.43.14. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

1.43.15. Deve alertar o usuário quando uma aplicação for bloqueada;

1.43.16. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

1.43.17. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc);

1.43.18. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

1.43.19. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, vendor e popularidade;

1.43.20. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

1.43.21. Deve permitir forçar o uso de portas específicas para determinadas aplicações.

1.44. Prevenção de ameaças

1.44.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

1.44.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

1.44.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

1.44.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

1.44.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

1.44.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

1.44.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

1.44.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.44.9. Deve permitir o bloqueio de vulnerabilidades;

1.44.10. Deve permitir o bloqueio de exploits conhecidos;

1.44.11. Deve incluir proteção contra-ataques de negação de serviços;

1.44.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

1.44.13. Detectar e bloquear a origem de portscans;

1.44.14. Bloquear ataques efetuados por worms conhecidos;

1.44.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

1.44.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

1.44.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

1.44.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

1.44.19. Deve permitir ao administrador adicionar um tempo mínimo para que assinaturas de IPS sejam ativadas;

1.44.20. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, IMAP, SMTP e POP3;

1.44.21. Identificar e bloquear comunicação com botnets;

1.44.22. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

1.44.23. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

1.44.24. Os eventos devem identificar o país de onde partiu a ameaça;

1.44.25. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

1.44.26. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

1.44.27. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

1.44.28. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

1.44.29. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

1.44.30. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

1.45. **Filtro de URLs**

1.45.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.45.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

1.45.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

1.45.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

1.45.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

1.45.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

1.45.7. Possuir pelo menos 60 categorias de URLs;

1.45.8. Deve possuir a função de exclusão de URLs do bloqueio;

1.45.9. Permitir a customização de página de bloqueio;

1.45.10. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

1.45.11. Identificação de usuários

1.45.12. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local, e SAML;

1.45.13. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.45.14. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

1.45.15. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

1.45.16. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

1.45.17. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

1.45.18. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo

visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

1.45.19. Deve suportar o envio e recebimento de credenciais via RADIUS;

1.45.20. Deve suportar SAML como método para autenticação na navegação de Internet e para VPN.

1.46. **Geolocalização**

1.46.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

1.46.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

1.47. **VPN Client to Site**

1.47.1. Suportar IPSec VPN;

1.47.2. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN;

1.47.3. Atribuição de DNS nos clientes remotos de VPN, inclusive com DNS split tunnel;

1.47.4. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.47.5. Suportar leitura e verificação de CRL (certificate revocation list);

1.47.6. O agente de VPN client-to-site deve ser compatível com pelo menos: Windows, Linux e Mac OS.

1.48. **Funcionalidade de filtro de dados - DLP**

1.48.1. Permitir identificar e, opcionalmente, prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

1.48.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.48.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

1.48.4. Permitir identificar e, opcionalmente, prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

1.48.5. Deve funcionar de maneira que consiga impedir que dados sensíveis saiam da rede e também deve funcionar de modo que se previna que dados não requisitados entrem na sua rede;

1.48.6. Deve possuir uma base de dados de dicionários e de padrões de dados pré-definidos, tais como números de cartões de crédito, trechos de código fonte de software etc. Essa base deve ser atualizada de forma automática pelo FABRICANTE da solução.

1.48.7. Deve permitir especificar a informação sensível a ser detectada como palavras, frases e expressões regulares.

1.48.8. Deve permitir a criação e armazenamento de impressões digitais (fingerprint) de documentos.

1.48.9. Deve permitir a aplicação de regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário autenticado;

1.48.10. Em tráfegos em que as regras definidas coincidirem, deve implementar no mínimo as seguintes ações: bloqueio, banimento e quarentena;

1.48.11. Deve armazenar, localmente ou na solução de gerenciamento centralizados de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP, em pelo menos os seguintes protocolos: E-mail, HTTP e mensageiros instantâneos;

1.48.12. Deve permitir a composição de uma ou mais regras DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego filtrado pelo sistema.

1.49. **Funcionalidade de detecção e proteção de dispositivos IoT**

1.49.1. Deve ter a capacidade de identificar automaticamente o tipo de equipamento conectado (profiling), com suporte a dispositivos IoT (Internet of Things);

1.49.2. A identificação de dispositivos deve ser baseada em características do equipamento (Endereço MAC, Sistema Operacionais, entre outros) ou pelo usuário autenticado;

1.49.3. Deve permitir a identificação e mitigação de explorações de vulnerabilidades contra dispositivos IoT, realizando aplicações de patches;

1.49.4. A solução deve possuir uma base de dados de dispositivos IoT, atualizadas de forma regular e automática pelo fabricante da solução;

1.49.5. A solução deve ser capaz de identificar vulnerabilidades conhecidas em dispositivos IoT, fornecendo no mínimo os seguintes detalhes da vulnerabilidade encontrada: descrição, tipo, severidade, número do CVE e o link de referência do CVE;

2. **Características específicas para os equipamentos de NGFW – Modelo 1 - Datacenter**

2.1. Deve suportar, no mínimo, 25 (vinte e cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

2.2. Deve suportar, no mínimo, 2,5 (dois vírgula cinco) milhões de conexões simultâneas;

2.3. Deve suportar, no mínimo, 130.000 (cento e trinta mil) novas conexões por segundo;

2.4. Deve Suportar, no mínimo, 35 (trinta e cinco) Gbps de throughput VPN IPSec;

2.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC Site-to-Site simultâneos;

2.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de clientes VPN IPSEC simultâneos;

2.7. Deve suportar, no mínimo, 5 (cinco) Gbps de throughput de IPS;

2.8. Deve suportar, no mínimo, 3 (três) Gbps de throughput de Inspeção SSL;

2.9. Deve suportar, no mínimo, 2,5 (dois vírgula cinco) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.

2.10. Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

2.11. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores SFP;

2.12. Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet com conectores SFP+;

2.13. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

2.14. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;

2.15. Deve possuir fonte de alimentação AC redundante;

2.16. Deve suportar até 10 instâncias virtuais no mesmo equipamento, sem necessidade de licença;

2.17. Deve estar homologado pela ANATEL.

2.18. ***Visibilidade e proteção de protocolos industriais:***

2.18.1. Deve suportar a criação de regras e objetos baseados em aplicações e protocolos de tecnologia da operação (OT) e de sistema de controle industrial (ICS), independente da porta de uso.

2.18.2. Deve possuir pelo menos 3.300 assinaturas de aplicações de protocolos industriais. São mandatórios os seguintes protocolos de automação e suas funções operacionais, que devem ser suportados de forma nativa:

2.18.2.1. IEC 104 (IEC 60.870-5-104);

2.18.2.2. ICCP (IEC 60.870-6/TASE.2);

2.18.2.3. IEC 61850 Manufacturing Message Specification (MMS);

2.18.2.4. IEC 62056 DLMS/COSEM;

2.18.2.5. DNP3 TCP/IP;

2.18.2.6. MODBUS TCP/IP;

2.18.2.7. OPCA-AE, OPC-DA, OPC-HDA e OPC-UA;

2.18.2.8. Synchrophasor (IEEE C.37.118).

2.18.3. Deve permitir a adição de parametros em protocolos industriais, como por exemplo, UnitID no caso do protocolo Modbus.

2.18.4. Mais de 700 regras de IPS - Intrusion Prevention System - para tecnologias industriais como ABB, Advantech, Allen-Bradley, Delta Industrial Automation, GE, Gemalto, Honeywell, Microsys, Mitsubishi, Moxa, Rockwell, Schneider, Siemens, Yokogawa, dentre outros;

2.18.5. Possibilidade de detecção de dispositivos IT, IoT e OT utilizando apenas o tráfego de rede, de maneira passiva, com mais de 1.300 regras de detecção.

2.18.6. Uso de tecnologia de Virtual Patching, promovendo um metodo de mitigação de exploração de vulnerabilidades em dispositivos OT, com mais de 1.400 regras

2.18.7. Suporte ao protocolo PRP - Parallel Redundancy Protocol - para filtragem de pacotes em redes de alta disponibilidade.

2.18.8. Possibilidade de licenciamento em ambiente air-gapped para dispositivos físicos

2.18.9. Possibilidade de mapeamento de dispositivos industriais, utilizando o Purdue Model, de maneira passiva.

3. **Características específicas para os equipamentos de NGFW – Modelo 2 – CCO**

3.1. Deve suportar, no mínimo, 10 (dez) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

3.2. Deve suportar, no mínimo, 1,4(hum vírgula quatro) milhão de conexões simultâneas;

3.3. Deve suportar, no mínimo, 100.000 (cem mil) novas conexões por segundo;

3.4. Deve Suportar, no mínimo, 7,1 (sete vírgula hum) Gbps de throughput VPN IPSec;

3.5. Deve estar licenciado para suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;

3.6. Deve estar licenciado para suportar sem o uso de licença, no mínimo, 500 (quinhentos) túneis de clientes VPN IPSEC simultâneos;

3.7. Deve suportar, no mínimo, 2,5 (dois vírgula cinco) Gbps de throughput de IPS;

3.8. Deve suportar, no mínimo, 1,4 (hum vírgula quatro) Gbps de throughput de Inspeção SSL;

3.9. Deve suportar, no mínimo, 1,3 (hum vírgula três) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.

3.10. Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

3.11. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

3.12. Deve suportar até 10 instâncias virtuais no mesmo equipamento, sem necessidade de licença;

3.13. Deve estar homologado pela ANATEL.

3.14. ***Visibilidade e proteção de protocolos industriais:***

3.14.1. Deve suportar a criação de regras e objetos baseados em aplicações e protocolos de tecnologia da operação (OT) e de sistema de controle industrial (ICS), independente da porta de uso.

3.14.2. Deve possuir pelo menos 3.300 assinaturas de aplicações de protocolos industriais. São mandatórios os seguintes protocolos de automação e suas funções operacionais, que devem ser suportados de forma nativa:

3.14.2.1. IEC 104 (IEC 60.870-5-104);

3.14.2.2. ICCP (IEC 60.870-6/TASE.2);

3.14.2.3. IEC 61850 Manufacturing Message Specification (MMS);

3.14.2.4. IEC 62056 DLMS/COSEM;

3.14.2.5. DNP3 TCP/IP;

3.14.2.6. MODBUS TCP/IP;

3.14.2.7. OPCA-AE, OPC-DA, OPC-HDA e OPC-UA;

3.14.2.8. Synchrophasor (IEEE C.37.118).

3.14.3. Deve permitir a adição de parametros em protocolos industriais, como por exemplo, UnitID no caso do protocolo Modbus.

3.14.4. Mais de 700 regras de IPS - Intrusion Prevention System - para tecnologias industriais como ABB, Advantech, Allen-Bradley, Delta Industrial Automation, GE, Gemalto, Honeywell, Microsys, Mitsubishi, Moxa, Rockwell, Schneider, Siemens, Yokogawa, dentre outros;

3.14.5. Possibilidade de detecção de dispositivos IT, IoT e OT utilizando apenas o tráfego de rede, de maneira passiva, com mais de 1.300 regras de detecção.

3.14.6. Uso de tecnologia de Virtual Patching, promovendo um metodo de mitigação de exploração de vulnerabilidades em dispositivos OT, com mais de 1.400 regras

3.14.7. Suporte ao protocolo PRP - Parallel Redundancy Protocol - para filtragem de pacotes em redes de alta disponibilidade.

3.14.8. Possibilidade de licenciamento em ambiente air-gapped para dispositivos físicos

3.14.9. Possibilidade de mapeamento de dispositivos industriais, utilizando o Purdue Model, de maneira passiva.

4. **Características específicas para os equipamentos de NGFW – Modelo 3 – Industrial**

4.1. Deve possuir no mínimo 4 (quatro) interfaces Ethernet GE com conector RJ-45 para conexão de equipamentos.

4.2. Deve possuir 2 (duas) portas SFP compartilhadas com as demais portas.

4.3. Deve possuir um par de portas que permita Bypass em caso de falha de energia do dispositivo.

4.4. Deve ser alimentado por -125 até -12 V CC, 12-125 V CC, com 2 entradas de energia.

4.5. Deve possuir no mínimo 1 (uma) interface USB.

4.6. Deve possuir no mínimo 1 (uma) interface Serial DB9.

4.7. Deve ter um throughput de 950Mbps para IPS.

4.8. Deve ter um throughput de 550Mbps para NGFW.

4.9. Deve ter um throughput de 500Mbps para Threat Protection.

4.10. Deve ter uma latência de 3.10 µs utilizando pacotes UDP de 64 bytes.

4.11. Deve suportar até 8.9Mpps (pacotes por segundo).

4.12. Deve suportar até 600.000 sessões concorrentes.

4.13. Deve suportar até 19.000 novas sessões por segundo.

4.14. Deve suportar até 5.000 políticas de firewall.

4.15. Deve ter um Throughput de VPN IPSEC (512 bytes) de 3.5Gbps.

4.16. Deve suportar até 200 túneis VPN IPsec G-t-G.

4.17. Deve suportar até 10 instâncias virtuais no mesmo equipamento, sem necessidade de licença.

4.18. Deve ter IPRating 20.

4.19. Deve suportar temperatura de operação de -40°F até 167°F (-40°C até 75°C).

4.20. Suporte à conversão dos protocolos DNP3, IEC104 e Modbus de serial para IP.

4.21. Deve possuir certificação IEC 61850-3 e IEEE 1613.

4.22. Deve possuir as certificações EN 55032:2015 + A11:2020, Classe A, EN 55035:2017 + A11:2020, EN IEC 61000-6-4:2019, IEC 61000-4-9, IEC 61000-4-10.

4.23. Deve possuir as certificações IEC 62368-1:2014, 2ª Ed., EN 62368-1:2014 + A11:2017, IEC 62368-1: 2018, 3ª Ed., EN IEC 62368-1:2020 + A11:2020.

4.24. Deve possuir as certificações IEC 60945:2002 4ª Ed. e DNV GL Type Approved.

4.25. Deve estar em conformidade com FCC Part 15 Classe A, RCM, VCCI Classe A, CE, UL/cUL, CB.

4.26. Deve possuir as certificações EN IEC 63000:2018 e EN 50581:2012.

4.27. Deve possuir as certificações EMC, Shock and Vibration Compliant, EN 50121-1:2017 EMC, EN 50121-4:2016 EMC, IEC60068-2-27:2008 Shock, IEC 60068-2-6:2007 Vibration.

4.28. Deve estar homologado pela ANATEL.

4.29. ***Visibilidade e proteção de protocolos industriais:***

4.29.1. Deve suportar a criação de regras e objetos baseados em aplicações e protocolos de tecnologia da operação (OT) e de sistema de controle industrial (ICS), independente da porta de uso.

4.29.2. Deve possuir pelo menos 3.300 assinaturas de aplicações de protocolos industriais. São mandatórios os seguintes protocolos de automação e suas funções operacionais, que devem ser suportados de forma nativa:

4.29.2.1. IEC 104 (IEC 60.870-5-104);

4.29.2.2. ICCP (IEC 60.870-6/TASE.2);

4.29.2.3. IEC 61850 Manufacturing Message Specification (MMS);

4.29.2.4. IEC 62056 DLMS/COSEM;

4.29.2.5. DNP3 TCP/IP;

4.29.2.6. MODBUS TCP/IP;

4.29.2.7. OPCA-AE, OPC-DA, OPC-HDA e OPC-UA;

4.29.2.8. Synchrophasor (IEEE C.37.118).

4.29.3. Deve permitir a adição de parametros em protocolos industriais, como por exemplo, UnitID no caso do protocolo Modbus.

4.29.4. Mais de 700 regras de IPS - Intrusion Prevention System - para tecnologias industriais como ABB, Advantech, Allen-Bradley, Delta Industrial Automation, GE, Gemalto, Honeywell, Microsys, Mitsubishi, Moxa, Rockwell, Schneider, Siemens, Yokogawa, dentre outros;

4.29.5. Possibilidade de detecção de dispositivos IT, IoT e OT utilizando apenas o tráfego de rede, de maneira passiva, com mais de 1.300 regras de detecção.

4.29.6. Uso de tecnologia de Virtual Patching, promovendo um metodo de mitigação de exploração de vulnerabilidades em dispositivos OT, com mais de 1.400 regras

4.29.7. Suporte ao protocolo PRP - Parallel Redundancy Protocol - para filtragem de pacotes em redes de alta disponibilidade.

4.29.8. Possibilidade de licenciamento em ambiente air-gapped para dispositivos físicos

4.29.9. Possibilidade de mapeamento de dispositivos industriais, utilizando o Purdue Model, de maneira passiva.

5. **Equipamento de Comutação Industrial**

5.1. Switch Ethernet robusto com suporte a protocolos de Camada 2 e Camada 3 (Layer 2/3), projetado com reforço de hardware para operar em ambientes hostis e redes industriais de Tecnologia Operacional (OT);

5.2. Deve suportar integração direta com Firewalls de Próxima Geração (NGFW) especificados neste processo por meio de protocolo que permita ao switch atuar como uma extensão lógica do firewall, possuindo um console de gerenciamento unificado;

5.3. Deve possuir suporte a provisionamento do tipo *Zero-touch*, com recursos de descoberta automática de múltiplos switches;

5.4. Deve possuir funcionalidade nativa integrada para o *onboarding* seguro e telemetria de dispositivos IoT e equipamentos padrão, aplicável diretamente na porta do switch;

5.5. Deve possuir no mínimo 16 portas de rede RJ45 (10M/100M/1GE) com suporte a PoE.

5.6. Deve possuir no mínimo 4 portas de uplink em fibra SFP/SFP+ de 1G/10G.

5.7. Deve ter uma latência de rede inferior a 1 µs (< 1µs).

5.8. Deve suportar uma taxa de encaminhamento de pacotes de, no mínimo, 166 Mpps (pacotes por segundo) em modo duplex.

5.9. Deve ter uma capacidade de comutação (Switching Capacity) de, no mínimo, 112 Gbps em modo duplex.

5.10. Deve estar preparado nativamente para montagem em trilho DIN (*DIN-rail*);

5.11. Deve suportar o armazenamento de até 16.000 (16k) entradas na tabela de endereços MAC.

5.12. Deve suportar até 4.000 (4k) VLANs ativas.

5.13. Deve suportar até 32 instâncias de protocolo Spanning Tree.

5.14. O equipamento deve suportar autenticação 802.1X (baseada em porta e em MAC), *MAC Access Bypass* (MAB) e quarentena de *host*

5.15. Deve suportar até 2.000 (2k) regras de Listas de Controle de Acesso (ACL).

5.16. Deve suportar a formação de Grupos de Agregação de Links (LAG) com tamanho de até 8 portas por grupo.

5.17. Deve fornecer um orçamento total de energia (PoE Power Budget) de até 360W.

5.18. Deve suportar o fornecimento de energia PoE de até 90W por porta (padrões 802.3af/at/bt) em suas 16 portas base.

5.19. Terminais de entrada de energia redundantes equipados com proteção contra inversão de polaridade

5.20. Suporte a redundância sem perda de pacotes e a *Precision Time Protocol* (PTP - IEEE1588v2) com perfis transparentes e *Boundary Clock;*

5.21. Deve ter um Tempo Médio Entre Falhas (MTBF) superior a 30 anos.

5.22. Deve possuir grau de proteção física contra ingressos de poeira nível IP40.

5.23. Deve ter sistema de resfriamento 100% passivo (fanless), sem a utilização de ventiladores.

5.24. Deve suportar operação em temperaturas extremas de -40°C a 75°C, incluindo a capacidade de inicialização a frio (cold startup) em -40°C.

6. **Equipamento de comutação de 24 portas Ethernet**

6.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 2 do modelo OSI;

6.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

6.3. Deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

6.4. Deve possuir 1 (uma) interface USB;

6.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

6.6. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar no mínimo 180 Mpps (milhões de pacotes por segundo);

6.7. Deve suportar no mínimo 4.000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

6.8. Deve possuir uma tabela MAC com suporte para, no mínimo, 32.000 (trinta e dois mil) endereços;

6.9. Deve operar com latência igual ou inferior à 1µs (microsegundo);

6.10. Deve possuir buffer de pacotes de, no mínimo, 2 MB;

6.11. Deve possuir memória DDR3 de, no mínimo, 512 MB;

6.12. Deve permitir a criação de, no mínimo, 640 (seiscentas e quarenta) listas de controle de acesso (ACL);

6.13. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

6.14. Deve suportar em ambientes com temperatura de até 45º Celsius;

6.15. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

6.16. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

6.17. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

6.18. Deve estar homologado pela ANATEL na data de execução do pregão;

6.19. Devem possuir garantia e suporte do fabricante pelo período de 36 (trinta e seis) meses;

6.20. Os equipamentos devem ser novos, ou seja, de primeiro uso. Na data da proposta, nenhum dos modelos poderão estar listados no site do fabricante em listas de end-of-life e end-of sale.

6.21. **Gerenciamento e sistemas**

6.21.1. Solução que deverá administrar e controlar de maneira centralizada os pontos de acesso wireless e switches do mesmo fabricante da solução ofertada deverá suportar ser configurado e monitorado através de REST API;

6.21.2. Deverá suportar ser configurado e monitorado através de REST API;

6.21.3. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

6.21.4. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

6.21.5. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

6.21.6. Deve permitir o armazenamento local de, no mínimo, 20 (vinte) configurações anteriores para possibilitar a comparação com as configurações atuais presentes no equipamento;

6.21.7. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

6.21.8. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;

6.21.9. Deve implementar serviço de DHCP Relay;

6.21.10. Deve implementar serviço de DHCP Server;

6.21.11. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

6.21.12. Deve permitir ser gerenciado através de IPv6;

6.21.13. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

6.21.14. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

6.21.15. Deve suportar o recurso de Wake-on-LAN (WoL);

6.21.16. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

6.21.17. Deve possuir recursos de automação para facilitar a operação diária dos switchs;

6.21.18. Deve suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via SNMP-trap, alertas no console de configuração e execução de APIs via webhook, acionadas por uma trigger configurada no switch;

6.21.19. Deve permitir que as automações sejam executadas em horários agendados;

6.22. **Segurança e visibilidade**

6.22.1. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem conter os seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

6.22.2. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

6.22.3. Deverá implementar mecanismo de proteção contra-ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

6.22.4. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

6.22.5. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

6.22.6. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

6.22.7. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

6.22.8. Deve suportar MAC Authentication Bypass (MAB);

6.22.9. Deve implementar RADIUS CoA (Change of Authorization);

6.22.10. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

6.22.11. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

6.22.12. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

6.22.13. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

6.22.14. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

6.22.15. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

6.23. **Funcionalidades em Camada 2 (LAYER2)**

6.23.1. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree);

6.23.2. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

6.23.3. Deve implementar Block intra-VLAN traffic;

6.23.4. Deve permitir a configuração de, no mínimo, 16 grupos de agregação de link (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

6.23.5. Deve suportar a comutação de Jumbo Frames;

6.23.6. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

6.23.7. Deve suportar IGMP snooping para controle de tráfego multicast, conforme documentado na RFC 4541, permitindo a criação de, no mínimo, 1.000 (mil) entradas na tabela;

6.23.8. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

6.23.9. Deve implementar os protocolos de prevenção de loop IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) e IEEE 802.1s Multiple Spanning Tree Protocol (MSTP);

6.23.10. Deve permitir implementar no mínimo 32 (trinta e duas) instâncias de Multiple Spanning Tree Protocol (MSTP);

6.23.11. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

6.23.12. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;

6.23.13. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

6.23.14. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

6.23.15. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

6.23.16. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

6.23.17. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

6.24. **Integração e monitoramento**

6.24.1. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

6.24.2. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

6.24.3. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

6.24.4. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

6.24.5. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;

6.24.6. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

7. **Centralizador e Analisador de Logs com visibilidade e proteção para protocolos industriais**

7.1.1. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

7.1.2. Deve suportar a coleta centralizada de logs e a análise profunda de eventos de segurança, consolidando a telemetria em ambientes convergentes de TI e OT.

7.1.3. A solução deve suportar receber, no mínimo, 10 (dez) GB de logs diários;

7.1.4. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;

7.1.5. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1;

7.1.6. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

7.1.7. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

7.1.8. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

7.1.9. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

7.1.10. A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;

7.1.11. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

7.1.12. Possuir suporte para SNMP versão 2 e 3;

7.1.13. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;

7.1.14. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

7.1.15. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

7.1.16. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;

7.1.17. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;

7.1.18. Deve permitir gerar alertas de eventos a partir de logs recebidos;

7.1.19. A solução deve ter relatórios predefinidos;

7.1.20. Permitir importação e exportação de relatórios

7.1.21. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

7.1.22. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

7.1.23. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

7.1.24. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

7.1.25. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

7.1.26. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

7.1.27. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;

7.1.28. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

7.1.29. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

7.1.30. Deve possuir mecanismos de remoção automática para logs antigos;

7.1.31. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

7.1.32. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

7.1.33. Permitir o envio por e-mail relatórios automaticamente;

7.1.34. Deve permitir que o relatório seja enviado por Email para o destinatário específico;

7.1.35. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

7.1.36. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

7.1.37. Deve permitir o uso de filtros nos relatórios;

7.1.38. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

7.1.39. Permitir especificar o idioma dos relatórios criados;

7.1.40. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

7.1.41. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;

7.1.42. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

7.1.43. Deve permitir exportar os logs no formato CSV;

7.1.44. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

7.1.45. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

7.1.46. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

7.1.47. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

7.1.48. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;

7.1.49. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

7.1.50. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

7.1.51. Deve permitir visualizar em tempo real os logs recebidos;

7.1.52. Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);

7.1.53. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

7.1.54. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

7.1.55. Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

7.1.56. Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

7.1.57. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

7.1.58. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

7.1.59. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)

7.1.60. Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;

7.1.61. Deve possuir relatório de uso de aplicações e mídias sociais;

7.1.62. Deve possuir relatório de prevenção de perda de dados (DLP);

7.1.63. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

7.1.64. Deve possuir relatório diário resumido de eventos e incidentes de segurança;

7.1.65. Deve possuir um relatório de tráfego DNS e e-mail;

7.1.66. Deve possuir relatório das 10 principais aplicações utilizadas na rede;

7.1.67. Deve possuir relatório dos 10 principais sites web utilizados na rede;

7.1.68. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);

7.1.69. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;

7.1.70. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;

7.1.71. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

7.1.72. Deve suportar recursos de automação (playbooks) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;

7.1.73. Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança;

7.1.74. Deve possuir uma central de identidade de ativos capaz de listar e centralizar todos os dispositivos detectados no ambiente, exibindo informações detalhadas e as vulnerabilidades conhecidas de cada ativo;

7.1.75. Deve possuir visões e mapeamento nativo de ameaças, vulnerabilidades, eventos e explorações baseados no framework específico MITRE ATT&CK para ICS (*Industrial Control Systems*);

7.1.76. Deve possuir integração nativa e *parsers* de log para ingerir, processar e correlacionar dados de plataformas e fabricantes de terceiros, incluindo soluções específicas do ecossistema de OT, como Nozomi, Dragos e Claroty;

7.1.77. Deve permitir a análise de tráfego e a filtragem de logs com visibilidade em nível de aplicação para protocolos industriais específicos, permitindo, por exemplo, o detalhamento (*drill down*) de tráfego Modbus.

7.1.78. Deve ser capaz de gerar relatórios de risco de segurança de OT, fornecendo um sumário executivo com uma visão arquitetural alinhada ao Modelo Purdue, destacando os dispositivos descobertos, aplicativos de risco e vulnerabilidades no ambiente cibernético-físico.

7.1.79. Deve suportar a geração de relatórios de conformidade para frameworks industriais, como o NERC CIP, incluindo *scorecards* executivos que avaliam o ambiente com aprovações ou falhas de requisitos detalhados por dispositivo;

7.1.80. Deve suportar recursos avançados através de um Serviço de Segurança OT dedicado, incluindo análises avançadas, tratadores de eventos focados em OT e regras de correlação voltadas para casos de uso do ambiente industrial;

8. **Solução de Acesso Remoto Seguro**

8.1.1. Deve permitir o gerenciamento centralizado de acessos privilegiados;

8.1.2. Deve estar dimensionado e licenciado para até 10 (dez) agentes simultâneos;

8.1.3. Entende-se por acessos privilegiados os tipos de acesso a ativos e a sistemas de tecnologia, além dos acessos realizados por um usuário comum, geralmente realizados por administradores de redes, administradores de servidores e administradores de sistemas;

8.1.4. A solução deve controlar o acesso baseado em função, com recursos de auditoria e de segurança, provendo no mínimo as seguintes funcionalidades:

8.1.4.1. *Cofre de credenciais*: funcionalidade onde os usuários não precisam ter conhecimento das credenciais, reduzindo-se o risco de vazamento, incluindo o rotacionamento automático dessas credenciais;

8.1.4.2. *Controle de acesso a contas privilegiadas*: funcionalidade onde é possível estabelecer níveis de privilégios de cada usuário, incluindo funcionalidades de fluxo de aprovação de acessos a determinados recursos;

8.1.4.3. *Monitoramento e registro de eventos*: funcionalidade onde é possível monitorar, registrar e auditar as atividades dos usuários privilegiados, incluindo informações das sessões tais como pressionamento de teclas, eventos de mouse, etc..

8.1.5. A solução deve ser do tipo appliance virtual, compatível com pelo menos os Hypervisors VMware ESXi, Microsoft Hyper-V e Linux KVM, sendo de responsabilidade da contratante a disponibilização dos recursos necessários para a implantação da solução: hardware e software (hypervisor);

8.1.6. As chaves criptográficas devem ser armazenadas internamente na solução e protegidas por tecnologia TPM ou vTPM;

8.1.7. A solução deve prover interface de API para integração com sistemas ou soluções de terceiros;

8.1.8. A solução deve diferenciar os usuários da plataforma entre:

8.1.8.1. *Usuários comuns:* aqueles que apenas executam as tarefas de gerenciamento dos sistemas de destino, como por exemplo a equipe de TI, um contratado da TI, um administrador de banco de dados (DBA). Geralmente estes usuários são Gerentes de TI e Administradores de Sistemas de TI.

8.1.8.2. *Usuários administradores:* aqueles que são responsáveis pelas tarefas de gerenciamento da solução.

8.1.9. A solução deve operar pelo menos nos seguintes modos:

8.1.9.1. *Modo Proxy*: toda conexão aos sistemas de destino é interceptada pela solução, que fica responsável pela conexão final ao sistema de destino. Nesse modo, a máquina cliente não tem acesso direto as credenciais de acesso e o administrador da solução pode interromper conexões se um comportamento estranho for detectado;

8.1.9.2. *Modo Não-Proxy*: toda conexão aos sistemas de destino partem diretamente da máquina cliente e a solução fornece ao cliente as credenciais para esse acesso.

8.1.10. A solução deve armazenar de forma segura o nome de usuário e a senha/chave dos servidores como segredos. Os segredos podem conter informações sobre login, credenciais e o endereço IP do servidor de destino. O usuário final pode usar o segredo para acessar os servidores;

8.1.11. As credenciais reais devem ser protegidas e os usuários da solução não podem acessar as credenciais, exceto em alguns casos configuráveis pelo administrador. As credenciais de login podem ser alteradas automaticamente e manualmente, a depender dos diferentes casos de uso;

8.1.12. A solução deve permitir a configuração de políticas comuns e um sistema de fluxo de aprovação hierárquico e auditável para acesso a informações sensíveis;

8.1.13. Os critérios de gerenciamento de senha devem ser configuráveis para atender à política organizacional de frequência de alteração de senha/controle de aprovação de uso/alteração após o uso;

8.1.14. Deve incluir e não se limitar aos seguintes recursos de Sistemas e Protocolos e Ferramentas: AD, Windows, Linux/Unix, Oracle DB, MS SQL, CISCO, AS400, Microsoft SQL, Microsoft SQL Shell, MySQL CLI, MySQL Shell, PostgreSQL CLI, VNC, WEB SMB, WEB SSH, Web RDP, Web SFTP;

8.1.15. Deve permitir a construção de um conector de plataforma personalizado e integração A2A;

8.1.16. Deve oferecer suporte para aprovação de credencial dupla, exigindo aprovações de usuários designados antes de permitir o acesso a credenciais para contas gerenciadas;

8.1.17. Deve oferecer suporte a funcionalidades de fluxo de trabalho para controles de liberação de senha e sessão, incluindo suporte para vários níveis de autorização, capacidade de agrupar autorizadores;

8.1.18. Deve suportar a capacidade de expirar a solicitação de aprovação após um período definido;

8.1.19. Deve fornecer a capacidade de permitir recursos de check-out e check-in para secrets;

8.1.20. Deve permitir a autenticação de uma sessão sem revelar a senha por meio da máquina do usuário final;

8.1.21. Sessões privilegiadas devem ser transmitidas por proxy por meio de um hardware seguro ou dispositivo virtual;

8.1.22. O proxy de sessão deve ser capaz de entrar em uma conta sem liberar uma senha para o usuário privilegiado;

8.1.23. A solução deve permitir o uso do modo cliente, com o uso de agentes, e deve oferecer suporte ao modo somente navegador, onde nenhum software cliente/agente é necessário;

8.1.24. Os seguintes modos de cliente e navegador devem ser suportados:

8.1.24.1. *Modo cliente*: PuTTY, Windows Remote Desktop, RealVNC, TightVNC e WinSCP etc;

8.1.24.2. *Modo de navegador*: Web SSH, Web RDP, Web VNC, Web SMB, Web SFTP e Web Account.

8.1.25. No modo navegador, deve possibilitar o uso de pelo menos as seguintes funcionalidades: acesso a senhas, sessões e administração da solução;

8.1.26. Deve possuir iniciadores de conexão para pelo menos: MySQL (CLI e Shell), Microsoft SQL CLI, PostgreSQL CLI, SSH (PuTTY, SSH CLI e SecureCRT), Remote Desktop e VNC (TightVNC e VNC Viewer);

8.1.27. As sessões devem permitir a inclusão ou exclusão de comandos executados durante uma sessão sem a necessidade de um agente;

8.1.28. Deve suportar registro/monitoramento de pelo menos os seguintes protocolos de sessão - Telnet, SSH, RDP, ICA, VNC, SQL Plus, SQL Windows, Http & Https, x5250, x3270

8.1.29. Deve permitir a auditoria das atividades administrativas da própria solução;

8.1.30. As solicitações de acesso privilegiado devem ser feitas usando um modelo de solicitação/liberação, no mínimo;

8.1.31. Não deve permitir que um administrador da solução realize o bypass do fluxo de aprovação para obter uma senha ou ativar uma sessão;

8.1.32. A solução deve oferecer suporte à sessão remota de auditoria no modo não transparente ou transparente, sem alteração no fluxo de trabalho para acessar a sessão remota usando ferramentas nativas do cliente, incluindo injeção direta de credencial;

8.1.33. Deve suportar monitoramento e gravação de sessão (para análise posterior) e seu monitoramento em tempo real (para vigilância em tempo real), permitindo que o administrador encerre as sessões, caso necessário;

8.1.34. As gravações do vídeo da sessão devem usar formatos disponíveis publicamente;

8.1.35. Deve ser possível gerar alertas de e-mail quando um usuário executa um comando restrito e a detecção de tais comandos não devem depender do uso de agentes;

8.1.36. Deve suportar diferentes métodos de autenticação e integração com sistemas corporativos como: Active Directory, LDAP, SAML, RADIUS;

8.1.37. Deve possuir suporte a múltiplo fator de autenticação (MFA) através de Token da Solução, SMS e E-Mail;

8.1.38. Deve permitir a configuração de OTP (One Time Password) via e-mail;

8.1.39. Deve permitir a verificação de arquivos transferidos entre o endpoint e os ativos protegidos, realizando-se a varredura contra conteúdos maliciosos;

8.1.40. Deve suportar o uso de verificações contra vazamento de dados (DLP) nos arquivos transferidos;

8.1.41. Deve suportar o bloqueio da área de transferência dos ativos privilegiados, para impedir a cópia de informações desses ativos;

8.1.42. Deve fornecer a funcionalidade de Break Glass para acesso emergencial as credenciais armazenadas na solução;

8.1.43. Deve restringir o acesso a console dos ativos protegidos pela solução;

8.1.44. Deve proteger o acesso à rede dos ativos protegidos pela solução;

8.1.45. Deve armazenar todas as senhas em um cofre seguro com criptografia AES-256;

8.1.46. Deve permitir que qualquer login/senha usado para acesso a ativos protegidos seja armazenado internamente e com segurança e deve permitir que os

usuários se conectem aos ativos protegidos sem o conhecimento do login/senha utilizado;

8.1.47. Deve alterar automaticamente as senhas para um grupo de recursos;

8.1.48. Deve estabelecer acesso granular às senhas;

8.1.49. Deve impedir os usuários vejam a senha em texto puro;

8.1.50. Deve permitir que as credenciais sejam injetadas diretamente nos sistemas, dando acesso aos usuários sem que eles vejam ou forneçam credenciais;

8.1.51. Deve suportar o controle de acesso sem o uso de VPN;

8.1.52. Deve permitir que as sessões sejam mantidas e compartilhadas com os auditores para interação (colaboração de sessão);

8.1.53. Deve permitir que os auditores monitorem usuários privilegiados sob demanda e em tempo real;

8.1.54. Deve integrar um sistema de fluxo de trabalho para permitir o acesso administrativo às máquinas identificadas;

8.1.55. A solução deve permitir acesso ao recurso de destino, sem agente, pelo menos nos protocolos RDP, SSH, TELNET, VNC, HTTPS;

8.1.56. Deve possibilitar o bloqueio do usuário no caso de uma execução de uma ação restrita;

8.1.57. Deve permitir rastreabilidade das conexões;

8.1.58. Deve permitir visualizar todas as conexões ativas;

8.1.59. Deve permitir rastreabilidade e controle de transferências de arquivos;

8.1.60. Deve permitir a configuração de notificações de e-mail em um determinado número de indicadores, como eventos relacionados ao tráfego (falha de conexão, falha de autenticação, etc.);

8.1.61. Deve permitir integração com soluções SIEM para relatórios avançados e processamento em tempo real de detecção de comportamento malicioso;

8.1.62. Deve possuir logs de auditoria completos e pesquisas avançadas, como pesquisas de texto para isolar incidentes;

8.1.63. Os logs de auditoria da solução devem mostrar claramente quem acessou qual dispositivo de destino, bem como a duração (hora de início e hora de término);

8.1.64. Deve fornecer logs para o histórico de aprovação de sessões privilegiadas;

8.1.65. Deve possuir um painel para exibir os usuários conectados no momento;

8.1.66. Deve permitir gerar relatórios personalizáveis.

9. Sistema de Segurança de Simulação de ambiente industrial

9.1. Requisitos do Sistema

9.1.1. A solução deve suportar autenticação administrativa com dois fatores através de integração com RADIUS.

9.1.2. A solução deve suportar autenticação administrativa remota utilizando LDAP/RADIUS.

9.1.3. A solução deve permitir controle de acesso baseado em perfis (RBAC).

9.1.4. A solução deve permitir restrição de acesso administrativo através de Trusted Host.

9.1.5. A solução deve suportar implantação em redes isoladas (Air-Gapped) sem conexão com a internet.

9.1.6. A solução deve permitir personalização do painel de controle através de widgets.

9.1.7. A solução deve suportar o uso de certificado SSL corporativo para acesso administrativo.

9.1.8. A solução deve permitir monitoramento via SNMP (V1, V2c e V3).

9.1.9. A solução deve permitir envio de alertas e relatórios por e-mail com gatilhos personalizados.

9.1.10. A solução deve gerar relatórios de segurança em formatos PDF e CSV.

9.1.11. A solução deve permitir configuração de avisos de login personalizados (login disclaimer).

9.2. **Tipos de Deception Suportados**

9.2.1. A solução deve suportar até 100 decoys simultaneamente.

9.2.2. A solução deve suportar até 20 máquinas virtuais (VMs) para decoys.

9.2.3. A solução deve permitir até 24 endereços IP por decoy.

9.2.4. A solução deve incluir suporte a decoys Linux.

9.2.5. A solução deve incluir suporte a decoys supervisório.

9.2.6. A solução deve incluir suporte a decoys IoT.

9.2.7. A solução deve incluir suporte a decoys customizados.

9.2.8. A solução deve incluir suporte a decoys em nuvem pública (AWS, Azure e GCP).

9.2.9. A solução deve possibilitar decoys Windows como licença adicional.

9.2.10. A solução deve incluir tokens de decepção.

9.2.11. A solução deve suportar 5 VLANs simultaneamente.

9.2.12. A solução deve oferecer Anti-Reconhecimento e Anti-Exploit (ARAE) como licença adicional por VLAN.

9.2.13. A solução deve incluir AV, IPS e Web Filtering.

9.2.14. A solução deve suportar decoys com emulação completa de sistemas operacionais, incluindo Windows 7, Windows 10, Windows Server 2016/2019, Linux (Ubuntu/CentOS), supervisório, IoT, SSLVPN, ESXi, ELK, SAP, ERP, POS, DB, Web e Médico.

9.2.15. A solução deve suportar decoys específicos para ambientes de nuvem pública (AWS, Azure, GCP).

9.2.16. A solução deve possuir framework para customização de decoys permitindo o upload de imagens ISO próprias para integração ao Active Directory, habilitação de serviços SQL, HTTP e credenciais AD como iscas.

9.2.17. A solução deve permitir que decoys sejam integrados diretamente ao Active Directory.

9.2.18. A solução deve suportar emulação de dispositivos comuns de rede com personalização de portas TCP para detectar ataques específicos.

9.2.19. A solução deve suportar decoys para ambientes OT/supervisório com perfis específicos (Rockwell, Siemens, Tridium, Vertiv, Schneider Electric) e permitir instalação de softwares específicos como RAPID supervisório.

9.2.20. A solução deve suportar decoys médicos IoT, incluindo PACS, DICOM e SpaceCom.

9.2.21. A solução deve suportar decoys IoT gerais, como roteadores Cisco, impressoras HP/Brother/Lexmark, roteadores TPLink e câmeras IP.

9.2.22. A solução deve permitir total customização dos serviços expostos pelos decoys, incluindo banners, credenciais, arquivos e configurações de protocolos.

9.2.23. A solução deve detectar ataques na camada 2 (MITM, ICMP Swiping e Responder).

9.2.24. A solução deve permitir a configuração de iscas específicas (RDP, SMB, SSH, credenciais armazenadas, documentos falsos, etc.).

9.3. **Capacidades de Gerenciamento e Implantação**

9.3.1. A solução deve permitir gerenciamento centralizado incluindo ambientes distribuídos e na nuvem.

9.3.2. A solução deve suportar trunking VLAN para exposição centralizada dos decoys em múltiplas VLANs (até 128).

9.3.3. A solução deve suportar extensão de decoys para localidades remotas a partir de um local centralizado.

9.3.4. A solução deve possuir assistente (wizard) para implantação simplificada dos decoys com recomendações automáticas.

9.3.5. A solução deve gerar automaticamente iscas para serviços dos decoys, personalizando-os com informações reais do ambiente.

9.3.6. A solução deve permitir configuração de IPs confiáveis para evitar alertas falsos positivos.

9.3.7. A solução deve suportar descoberta de ativos por varredura ativa e passiva.

9.4. **Detecção e Resposta a Ameaças**

9.4.1. A solução deve monitorar em tempo real interações com os decoys, incluindo IP, credenciais, processos e comandos utilizados pelos atacantes.

9.4.2. A solução deve permitir reset automático dos decoys para o estado original após ataques.

9.4.3. A solução deve possibilitar download de artefatos (PCAPs, executáveis).

9.4.4. A solução deve permitir randomização automática do conteúdo dos decoys (arquivos, nomes).

9.4.5. A solução deve detectar e alertar automaticamente a presença de malware nos decoys.

9.4.6. A solução deve categorizar e relatar URLs acessadas por atacantes nos decoys.

9.4.7. A solução deve permitir integração com Sandbox do mesmo fabricante para análise avançada de malware.

9.5. **Requisitos de Logs e Relatórios**

9.5.1. A solução deve exibir incidentes em linha do tempo e agrupados por campanhas.

9.5.2. A solução deve permitir exportação de indicadores de comprometimento (IOC) para plataformas externas (STIX/TAXII).

9.5.3. A solução deve integrar-se ao SIEM e suportar saída via Syslog e formato CEF.

9.6. **Integrações de Segurança**

9.6.1. A solução deve integrar-se com o NGFW da instituição.

9.6.2. A solução deve permitir integração via REST-API com ferramentas externas.

9.6.3. A solução deve possuir integração com NGFW para quarentena automática conforme a gravidade dos eventos.

9.6.4. A solução deve fornecer integração com NAC e SOAR para quarentena automática de IPs ou usuários, dependendo da gravidade.

A solução deve fornecer integração via REST-API com ferramentas externas.

19.3.2 SERVIDORES DO DATA CENTER PRIMÁRIO

ITEM	DESCRITIVO	Unidade	Quantidade
1	Servidor Rack	unid	2

1 – SERVIDOR RACK

1.1 – Gabinete da CPU

1.1.1 – Gabinete tipo rack padrão 19”, com altura de, no máximo, 1U original do fabricante do equipamento;

1.1.2 – Deverá incluir trilhos deslizantes, bem como um gerenciador de cabos para melhor organização dos mesmos, manuais e quaisquer outros componentes necessários para instalação em rack ofertados como padrão do produto;

1.1.3 – Possuir projeto tool-less, ou seja, não necessita de ferramentas para abertura do gabinete e instalação/desinstalação de placas de expansão;

1.1.4 – O Gabinete deverá ser do mesmo fabricante do equipamento.

1.2 – Sistema de Ventilação

1.2.1 – Possuir ventilação adequada para a refrigeração do sistema interno do equipamento na sua configuração máxima e dentro dos limites de temperatura adequados para operação;

1.2.2 – O sistema de refrigeração deverá ser redundante e interno ao equipamento.

1.3 – Fonte de Alimentação

1.3.1 – Fontes de Alimentação interna, redundantes e hot-pluggable com potência mínima de 800W cada fonte, e potência suficiente para manter o funcionamento do equipamento em sua configuração máxima;

1.3.2 – As fontes de alimentação deverão ser do tipo PLATINUM, devidamente comprovada pela http://www.80plus.org/ na potência ofertada trabalhando 800W;

1.3.3 – Faixa de tensão de entrada de 100-240 VAC em 60 Hz, com chaveamento automático de voltagem;

1.3.4 – Em caso de falha de uma das fontes, a fonte restante deverá suprir potência suficiente para as necessidades do equipamento;

1.3.5 – Fornecer cabos de alimentação para cada fonte de alimentação de forma a possibilitar a instalação em circuitos elétricos distintos, os cabos deverão ser no padrão brasileiro.

1.4 – Processadores

1.4.1 – O servidor deverá possuir 01 (um) processador físico instalado, com no mínimo 24 (vinte e quatro) núcleos físicos e frequência base mínima de 2,6 GHz, devendo apresentar desempenho mínimo de 220 pontos no benchmark SPECint2017 Integer Rate (base ou peak), auditado e publicado pela SPEC - Standard Performance Evaluation Corporation;

1.4.2 – Quantidade mínima de, 24 MB cache L3, em cada processador físico;

1.4.3 – Deverá dar suporte a virtualização Intel-VT ou AMD-v;

1.4.4 – Deverá suporta o software de gerenciamento remoto do Servidor;

1.4.5 – Chipset e Slots de Expansão

1.4.5.1 – A plataforma deverá ser compatível e homologada pelo fabricante do processador instalado;

1.4.5.2 – Deverá possuir no mínimo 3 (três) slots padrão PCI-Express Gen4.

1.5 – BIOS;

1.5.1 – A BIOS deve ser desenvolvido pelo mesmo fabricante do equipamento ou o fabricante deve ter direito de cópia sobre essa BIOS, comprovando através de atestado fornecido pelo fabricante da BIOS, juntamente com a apresentação da Proposta Comercial;

1.5.2 – Possuir recursos de controle de permissão através de senhas, uma para inicializar o equipamento e outra para acesso e alterações das configurações do BIOS;

1.5.3 – A BIOS deve possuir o número de série/serviço do equipamento e campo editável que permita inserir identificação de ativo podendo ser consultada por software de gerenciamento;

1.6 – Memória RAM

1.6.1 – Os módulos de memórias devem ser do tipo DDR4 RDIMM (Registered DIMM) com tecnologia de correção ECC (Error Correcting Code) e velocidade de pelo menos 3.200 MT/s;

1.6.2 – Possuir, no mínimo, 192 GB (cento e noventa e dois gigabytes) de memória RAM instalada em módulos de memória de pelo menos, 32GB cada;

1.6.3 – O equipamento ofertado deverá suportar expansão de memória RAM para até 768GB, sem a substituição dos pentes de memórias do item anterior;

1.6.4 – Suportar espelhamento de memória (Memory Mirroring);

1.7 – Portas de Comunicação

1.7.1 – Todos os conectores das portas de entrada/saída de sinal são identificados pelos nomes ou símbolos;

1.7.2 – O equipamento deve possuir, no mínimo, 03 portas USB, sendo pelo menos 01 (uma) delas situadas na parte frontal do gabinete e 01 (uma) 3.0 na parte traseira;

1.7.3 – Possuir 01 (uma) porta para monitor de vídeo padrão VGA (DB-15);

1.8 – Interfaces de Rede

1.8.1 – Possuir 02 (duas) interfaces de rede RJ-45, com velocidade 1 Gigabit/sec ou superior;

1.8.2 – Possuir 02 (duas) interfaces de rede RJ-45, com velocidade 10 Gigabit/sec ou superior;

1.8.3 – Deverá possuir recurso Large Send Offload (LSO);

1.8.4 – TCP, IP, and UDP checksum offload;

1.8.5 – Permitir implementação de load balance e failover;

1.8.6 – Capacidade de suportar boot iSCSI;

1.8.7 – Suportar boot através de PXE;

1.8.8 – Suportar a tecnologia de Receive Side Scaling (RSS);

1.8.9 – Deverá suportar Jumbo Frames;

1.9 – Controladora RAID

1.9.1 – Controladora RAID, compatível com discos padrão SATA, SAS a 6Gb/s e 12Gb/s;

1.9.2 – Memória cache de no mínimo 2GB com proteção por bateria ou supercapacitor;

1.9.3 – Suportar RAID 0, 1, 5, 6, 10, 50 e 60;

1.9.4 – Suportar expansão de capacidade de forma on-line;

1.9.5 – Deverá permitir a retomada automática após perda de energia durante reconstrução do array;

1.9.6 – Suporte migração de RAID de forma on-line;

1.9.7 – Suportar implementação de disco Global Hot-spare;

1.9.8 – Suportar Self-Monitoring Analysis and Reporting Technology (SMART).

1.9.9 – Não serão aceitas soluções de RAID baseadas em software;

1.10 – Armazenamento

1.10.1 – O equipamento deverá possuir um armazenamento composto de, no mínimo:

1.10.2 – 04 (quatro) unidades de discos sólidos do tipo SSD (Solid State Drive), hot pluggable com capacidade de 800GB cada;

1.10.3 – Os discos deverão ser do tipo Hot plug;

1.10.4 – Não serão aceitos discos em gabinetes externos ao servidor;

1.10.5 – Compatível com a controladora RAID descrita acima;

1.10.6 – O equipamento ofertado deverá possuir no mínimo 06 (seis) slots de discos;

1.11 – Controladora de Vídeo

1.11.1 – Tipo: On board ou placa de vídeo OffBoard;

1.11.2 – Barramento compatível: PCI ou PCI Express;

1.11.3 – Capacidade da memória cache de vídeo ou da placa de vídeo: mínimo de 08 MB;

1.11.4 – Resolução gráfica de 1280 x 1024 pixels ou superior;

1.12 – Gerenciamento e Inventário

1.12.1 – Deverá ser fornecido software de gerenciamento desenvolvido pelo fabricante do equipamento;

1.12.2 – O equipamento ofertado deverá possuir placa de gerenciamento remoto, do mesmo fabricante do equipamento, que possibilite o gerenciamento “out-of-band” através de porta RJ-45, não sendo essa nenhuma das interfaces de controladora de rede solicitada anteriormente nesse item;

1.12.3 – Utilizar de protocolos para criptografia SSL e SSH para acesso a console WEB;

1.12.4 – Possuir interface de linha de comando e Web. Para interface Web, por meio de browser padrão poder realizar as tarefas de monitoração e controle, sem nenhum software adicional e independente do sistema operacional;

1.12.5 – Permitir controle remoto tipo virtual KVM mesmo quando o sistema operacional estiver inoperante;

1.12.6 – Permitir a instalação remota de Sistemas Operacionais Windows, Linux e VMware;

1.12.7 – Ser totalmente compatível com os padrões de gerenciamento IPMI (Intelligent Platform Management Interface) 2.0, SNMPv3 e REST APIs;

1.12.8 – Suportar autenticação via Active Directory e permitir autenticação de dois fatores;

1.12.9 – Possuir tecnologia de mídia virtual possibilitando que imagens ISO e drivers do tipo CD/DVD localizados em estação de gerenciamento remota, sejam emulados no servidor gerenciado, permitindo inclusive a inicialização (boot) através dessas mídias;

1.12.10 – Permitir desligar e reiniciar o servidor através da console de gerenciamento, mesmo em condições de indisponibilidade do sistema operacional;

1.12.11 – Realizar inventário de hardware, BIOS e firmware e possibilitar a geração de relatórios;

1.12.12 – Permitir atualização de firmware da BIOS, placas adaptadoras e de drivers para Windows e Linux;

1.12.13 – Deve informar o status do equipamento, indicando os componentes com falha e notificando o administrador via e-mail ou trap SNMP;

1.12.14 – Possuir nativamente suporta ao Trusted Platform Module (TPM) 2.0;

1.12.15 – Deverão ser fornecidas todas as licenças necessárias para o funcionamento total das funcionalidades aqui solicitadas de gerenciamento e inventário.

1.13 – Sistema Operacional

1.13.1 – O modelo do equipamento ofertado deverá suportar o sistema operacional Windows Server 2022 e 2025. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Microsoft no link: http://www.windowsservercatalog.com;

1.13.2 – O modelo do equipamento ofertado deverá suportar o sistema operacional Red Hat Enterprise Linux 8 ou posterior. Esse item deverá ser comprovado através do HCL (Hardware Compatibility List) da Red Hat no link: https://hardware.redhat.com/hwcert/index.cgi

1.13.3 – O modelo do equipamento ofertado deverá suportar o sistema de virtualização VMware ESX 8 ou posterior. Esse item deverá ser comprovado através do Compatibility Guide da VMware no link: http://www.vmware.com/resources/compatibility;

1.13.4 – O servidor deverá ser fornecido acompanhado de licença perpétua do Microsoft Windows Server 2025 Standard, devidamente licenciada por núcleo (core), contemplando todos os núcleos físicos do processador instalado no equipamento, conforme modelo de licenciamento vigente da Microsoft. A licença deverá garantir, no mínimo:

1.13.4.1 – Direito de execução de até 02 (duas) máquinas virtuais Windows Server no mesmo host físico, conforme regras da edição Standard;

1.13.4.2 – Direito de instalação do sistema operacional no host físico exclusivamente para fins de virtualização (Hyper-V) e gerenciamento das máquinas virtuais;

1.13.4.3 – Fornecimento de mídia original ou acesso oficial para download;

1.13.4.4 – Chave(s) de ativação válida(s);

1.13.4.5 – Documentação comprobatória da legalidade do licenciamento.

1.13.5 – O servidor deverá ser fornecido acompanhado de licença de Acesso (CALs) com pacote mínimo de 20 (vinte) licenças de acesso ao Windows Server (Client Access Licenses – CALs), do tipo Dispositivo, compatíveis com a versão ofertada do sistema operacional. As

CALs deverão ser perpétuas e devidamente documentadas, em conformidade com as políticas de licenciamento da Microsoft.

1.14 – Drivers

1.14.1 – O FABRICANTE do equipamento deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers de dispositivos, BIOS e Firmwares permitindo todas as atualizações de melhoria necessárias;

1.15 – Acessórios

1.15.1 – Devem ser fornecidos junto com o servidor, todos os acessórios e cabos necessários para o pleno funcionamento do mesmo;

1.15.2 – Kit de trilhos e braço organizador de cabos para fixação dos equipamentos em rack padrão 19 polegadas, permitindo o deslizamento do equipamento a fim de facilitar a manutenção;

1.16 – Certificados

1.16.1 – Deverá estar em conformidade com a norma IEC 60950 ou 60950-1 ou 62368-1, para segurança do usuário contra incidentes elétricos e combustão dos materiais elétricos;

1.16.2 – Deverá estar certificado quanto à emissão de radiação radiada e conduzida. Expedido por órgãos competentes comprovando que o equipamento detém da norma CISPR 22 ou EN55022 ou EN55032;

1.17 – Garantia e Suporte

1.17.1 – Garantia de hardware do FABRICANTE de 48 (quarenta e oito) meses. On Síte em Aracaju. Cobertura: 9x5;

1.17.2 – Tempo de atendimento no próximo dia útil;

1.17.3 – A entrega dos equipamentos deverá ser realizada em até 45 (quarenta e cinco) dias corridos após a assinatura do contrato;

1.17.4 – Disponibilidade de site na WEB (indicar endereço) para Suporte e transferência de arquivos de configuração (Devices Drivers e novas versões de ROM e softwares do equipamento);

1.17.5 – A garantia on-site deverá ser executada diretamente pelo próprio FABRICANTE ou rede de assistência técnica autorizada pelo FABRICANTE.

1.17.6 – A abertura dos chamados técnicos relativos à garantia do equipamento deve ser feita através de “Central de Atendimento” do FABRICANTE, por meio de ligação telefônica gratuita;

1.17.7 – Os equipamentos ofertados deverão ser novos e de primeiro uso além de estar na linha de produção atual do fabricante (não-descontinuados) na data de entrega;

1.18 – Documentação necessária

1.18.1 – No ato da proposta, apresentar catálogo oficial do fabricante, de acesso público através de website, onde poderão ser conferidas todas as características exigidas para o item e subitens que compõe o item ofertado, contendo informações referentes à descrição;

22.3.3 MICROCOMPUTADORES E NOTEBOOKS

ITEM	DESCRITIVO	Unidade	Quantidade
1	Microcomputador	unid	9
2	Notebook	unid	2

1 – Microcomputador

1.1 – Gabinete

1.1.1 – O gabinete deverá, obrigatoriamente, ser do mesmo fabricante do equipamento fornecido não sendo aceito o regime de OEM (Original Equipment Manufacturer);

1.1.2 – O gabinete deverá ter volume máximo de 1.200 cm³ (Altura x Largura x Profundidade) ou 1.2 Litro;

1.1.3 – O fluxo de ar no interior do gabinete deve ser horizontal e linear. A entrada de ar deve ser pela parte frontal do gabinete e a saída pela parte traseira, não sendo aceitos gabinetes com saída de ar na parte lateral ou superior;

1.1.4 – Com dispositivo sensor de intrusão integrado ao gabinete, que permita a emissão de alertas ao sistema de gerenciamento do equipamento, em caso de abertura do gabinete, permitindo o monitoramento de violações do equipamento e o armazenamento dos LOGS para consultas futuras;

1.1.5 – Utilizável, de maneira estável, segura e adequada, sem comprometer os componentes internos e o funcionamento do equipamento, nas posições vertical (torre) e horizontal (desktop), sem a utilização de fresagens, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes;

1.1.6 – Base ou pés em material antiderrapante na posição horizontal;

1.1.7 – Com tecnologia “Tool Less” (manuseio sem utilização de ferramentas, apenas utilizando-se as mãos, de maneira simples, rápida e sem necessidade de esforços adicionais), para, no mínimo, executar os procedimentos de abertura do gabinete e módulos de memória RAM. Não serão aceitas adaptações sobre o gabinete original para se atingir essa tecnologia;

1.1.8 – Com sistema de refrigeração adequado ao processador, para garantir a temperatura de funcionamento e vida útil dos componentes;

1.1.9 – Não serão aceitos efeitos de iluminação ou transparências (janelas). A cor do conjunto (teclado, mouse e gabinete) deve ser harmoniosa, apresentando a mesma cor ou uma cor predominante;

1.1.10 – Alimentação: Externa, compatível com 100-220V, com ajuste automático de voltagem, sem a utilização de adaptadores, conversores ou transformadores e capaz de suportar a configuração completa de acessórios e componentes do equipamento;

1.1.11 – Fonte de, pelo menos, 87% de eficiência;

1.1.12 – Para cada equipamento deverá ser fornecido cabo de força (NBR 14136), sem emendas, adequado à potência do equipamento.

1.2 – System Board e Processador

1.2.1 – Arquitetura x86 64bits;

1.2.2 – Deve atingir índice de, no mínimo, 23.500 pontos para o desempenho, tendo como referência a base de dados Passmark CPU Mark disponível no site http://www.cpubenchmark.net/cpu_list.php.

1.2.3 – Processador com no mínimo 14 núcleos e 20 Threads;

1.2.4 – Memória cache total com o mínimo de 24 MB;

1.2.5 – Cooler para o processador de fabricação ou de fornecimento em regime de OEM pelo respectivo fabricante do processador ou equivalente;

1.2.6 – O equipamento ofertado deverá possuir no mínimo de 16 GB de memória RAM instalada, e suportar expansão até 64GB;

1.2.7 – A memória deverá ser do tipo DDR5 com velocidade de no mínimo 4800MT/s;

1.2.8 – Placa-mãe do mesmo fabricante, não sendo aceito placas de livre comercialização no mercado, sujeito a verificação pelos técnicos da DESO com fornecimento de amostra se solicitado.

1.2.9 – Com tecnologia para operar em 64 bits, permitindo a utilização de sistemas operacionais de 64 bits;

1.2.10 – Com suporte a virtualização baseada em hardware (também conhecida como hardware-based virtualization ou hardware-assisted virtualization).

1.2.11 – Possuir Chip de segurança TPM versão 2.0 integrado para criptografia;

1.3 – Setup

1.3.1 – A BIOS deverá ser desenvolvida pelo mesmo fabricante do equipamento ou via Copyright. O fabricante do computador deverá ter direito de edição irrestrito sobre a BIOS, garantindo assim segurança, adaptabilidade e manutenibilidade do conjunto adquirido. Caso a BIOS não seja do mesmo fabricante, deverá ser apresentado documento emitido pelo fabricante da BIOS, informando que o fabricante do computador possui direito de edição da mesma;

1.3.2 – BIOS em Flash ROM, podendo ser atualizada por meio de software de gerenciamento;

1.3.3 – Possibilita que a senha de acesso ao BIOS seja ativada e desativada via SETUP;

1.3.4 – Permite inserir registro de controle patrimonial, de pelo menos 10 (dez) caracteres em memória não volátil;

1.3.5 – BIOS português ou inglês, desenvolvida pelo fabricante em conformidade com a especificação UEFI 2.1 (http://www.uefi.org), e capturáveis pela aplicação de inventário SCCM (System Center Configuration Manager); O fabricante possui compatibilidade com o padrão UEFI comprovada através do site http://www.uefi.org/members, na categoria membros.

1.3.6 – Possuir ferramenta que possibilita realizar a formatação definitiva dos dispositivos de armazenamento conectados ao equipamento, desenvolvida em acordo com o padrão de segurança NIST 800-88 ou ISO/IEC 27040:2015. Caso esta ferramenta não seja nativa da BIOS, deverá ser oficialmente homologada pelo Fabricante do equipamento;

1.3.7 – Possuir sistema integrado de diagnóstico que permita verificar a saúde do sistema em modo rápido e em modo detalhado, bem como diagnóstico na BIOS em modo gráfico, capaz de verificar os seguintes itens:

1.3.7.1 – Alto-falante interno;

1.3.7.2 – Unidades de Armazenamento;

1.3.7.3 – Boot do sistema operacional;

1.3.7.4 – Funcionalidade de portas USB;

1.3.7.5 – Processador;

1.3.7.6 – Memória RAM;
1.3.8 – A mensagem de erro gerada por este diagnóstico deverá ser o suficiente para abertura de chamado do equipamento durante o período de vigência da garantia.

1.4 – Segurança

1.4.1 – Possuir Chip de segurança TPM versão 2.0 integrado para criptografia;
1.4.2 – Suporte para uso de cabo de travamento;

1.5 – Interface (disponíveis pelo exterior do gabinete)

1.5.1 – Deve possuir no mínimo 6 (seis) portas USB externas nativas, sem uso de hubs, placas ou adaptadores, sendo pelo menos 02 (duas) do tipo USB 3.1 ou 3.0;
1.5.2 – Deve possuir placa Wireless interna em conformidade com os padrões 802.11AX dual-band com bluetooth na versão 5.3. Não será aceito nenhum tipo de adaptador externo, seja USB ou qualquer outra interface).
1.5.3 – Deve possuir 01 (uma) porta RJ-45 traseira;
1.5.4 – Possuir no mínimo 01 slot PCI Express e/ou M.2;
1.5.5 – Possuir pelo menos uma porta do tipo VGA;
1.5.6 – Possuir pelo menos uma porta do tipo HDMI;
1.5.7 – Possuir pelo menos uma porta do tipo Display Port 1.2;
1.5.8 – Deve possuir 01 (uma) saída de áudio Frontal;
1.5.9 – Deverá possuir conectores frontais para Headphone e microfone sendo aceita interface tipo combo;

1.6 – Controladora de Áudio

1.6.1 – Controladora de áudio integrada que suporta o padrão AC'97 áudio CODEC ou padrão HD Áudio;

1.6.2 – Alto-falante integrado ao gabinete, não sendo aceito caixa de som externas;

1.7 – Controlador Gráfico

1.7.1 – Deverá possuir controlador gráfico integrado;
1.7.2 – Capacidade de 1.7GB de memória, dedicada ou compartilhada dinamicamente;
1.7.3 – Suporte a DirectX 12;
1.7.4 – Deverá suportar resolução em 4k;
1.7.5 – Deverá suportar OpenGL 4.4 ou superior;
1.7.6 – Capaz de suportar 03 (três) monitores simultaneamente.

1.8 – Interfaces de Rede

1.8.1 – Controladora Gigabit-Ethernet;
1.8.2 – Com conector no formato RJ-45 fêmea;
1.8.3 – Deve suportar as velocidades de transmissão de 10/100/1000 Mbps (Megabits por segundo), com chaveamento automático;
1.8.4 – Deverá suportar o protocolo WOL e PXE;
1.8.5 – Deve possuir placa Wireless interna em conformidade com os padrões 802.11AX dual-band com bluetooth na versão 5.3. Não será aceito nenhum tipo de adaptador externo, seja USB ou qualquer outra interface).

1.9 – Armazenamento

1.9.1 – Deverá ser interno;
1.9.2 – 01 (uma) unidade de estado sólido (SSD) por equipamento;
1.9.3 – Capacidade de armazenamento de, no mínimo, 512 GB (Gigabytes);
1.9.4 – Padrão M2 NVMe;

1.10 – Mouse (obrigatoriamente do mesmo fabricante da CPU)

1.10.1 – O mouse deverá, obrigatoriamente, ser do mesmo fabricante do equipamento fornecido, sendo aceito o regime de OEM (Original Equipment Manufacturer), devendo apresentar declaração do FABRICANTE do computador informando que é um produto OEM. Também deverá possuir a mesma tonalidade do gabinete;
1.10.2 – Dispositivo dotado com 3 botões (sendo um botão para rolagem de telas – “scroll”);
1.10.3 – Com tecnologia óptica (sem esfera);
1.10.4 – Deve funcionar sobre qualquer superfície compatível com tecnologia óptica, não necessitando nenhum tipo de PAD especial;
1.10.5 – Resolução mínima de 1000 dpi;
1.10.6 – Deverá ser Plug-and-Play;
1.10.7 – O conector deverá ser USB, vedado o uso de qualquer adaptador ou conversor de padrão, com respectivo cabo para conexão. O cabo deverá possuir tamanho adequado à perfeita utilização do equipamento pelo usuário, sendo que o comprimento do cabo deverá permanecer fixo não sendo permitido dispositivos de ajuste para redução do cabo;
1.10.8 – Deverá ser acompanhado de mouse-pad;

1.11 – Teclado (obrigatoriamente do mesmo fabricante da CPU)

1.11.1 – O teclado deverá, obrigatoriamente, ser do mesmo fabricante do equipamento fornecido, sendo aceito o regime de OEM (Original Equipment Manufacturer), devendo apresentar declaração do FABRICANTE do computador informando que é um produto OEM. Também deverá possuir a mesma tonalidade do gabinete;
1.11.2 – Padrão ABNT 2;
1.11.3 – Com todos os caracteres da Língua Portuguesa, inclusive “Ç”;

1.11.4 – O conector deverá ser USB, vedado o uso de qualquer adaptador ou conversor de padrão, com respectivo cabo para conexão. O cabo deverá possuir tamanho adequado à perfeita utilização do equipamento pelo usuário, sendo que o comprimento do cabo deverá permanecer fixo, não sendo permitidos dispositivos de ajuste para redução do cabo;
1.11.5 – Deverá possuir bloco numérico separado das demais teclas;
1.11.6 – Não poderá possuir tecla para ativação da funcionalidade de desligamento;
1.11.7 – Deverá possuir teclas ou combinação de teclas com no mínimo as seguintes funções: Volume, mudo, leitura/pausa, retrocesso, avanço.

1.12 - Monitores – (cada desktop deverá ser fornecido com 03 monitores com suporte)

1.12.1 – O monitor deverá, obrigatoriamente, ser do mesmo fabricante do equipamento fornecido, de sua fabricação ou em regime de OEM (Original Equipment Manufacturer);
1.12.2 – Tela: 100% plana de LED com dimensões de 23.8 Polegadas;
1.12.3 – Deverá permitir rotação retrato/paisagem;
1.12.4 – O monitor deverá possuir regulagem de altura, inclinação e giro (eixo horizontal);
1.12.5 – Resolução: suporte à resolução de: 1920x1080 a uma frequência horizontal de 60Hz;
1.12.6 – Possuir tecnologia antirreflexo;
1.12.7 – Ângulo de visão mínimo: 178º H e 178º V;
1.12.8 – Pixel Pitch igual ou menor que 0.250 mm;
1.12.9 – Contraste no mínimo: 1000:1;
1.12.10 – Brilho no mínimo: 250 cd/m2;
1.12.11 – Suporte a Cores: mínimo 16.7 M cores;
1.12.12 – Tempo de Resposta menor ou igual: 5 ms
1.12.13 – Possuir Tensão: Bivolt 100-240 VAC;
1.12.14 – Possuir no mínimo 1 (uma) interface no padrão HDMI;
1.12.15 – Possuir no mínimo 1 (uma) interface no padrão Display Port;
1.12.16 – Possuir no mínimo 1 (uma) interface no padrão VGA;

1.12.17 – Possuir no mínimo 4 (quatro) interfaces USB 3.2 nas laterais ou inferior para fácil acesso;
1.12.18 – Certificações: TUV GS ou TCO Certified Displays;
1.12.19 – Certificação EPEAT BRONZE;
1.12.20 – Está em conformidade com o padrão RoHS;
1.12.21 – O monitor deverá seguir a mesma garantia do computador ofertado, ou seja, 4 (quatro) anos;
1.12.22 – Deverá acompanhar cabo de força, bem como dois cabos para conectividade com a CPU, onde um deve ser DisplayPort ou HDMI e outro no padrão VGA para funcionamento com os computadores legados no ambiente de DESO;
1.12.23 – Deverá ser entregue suporte capaz de fixar o gabinete do computador na parte traseira do monitor. Este suporte não poderá interferir nos ajustes de altura, inclinação, rotação e giro nativos do monitor e também não poderá impactar na funcionalidade toolless do computador, ou seja, não poderá utilizar, para fixar o gabinete junto ao suporte e o suporte junto ao monitor nenhum parafuso que não seja recartilhado. O suporte deve ser obrigatoriamente do mesmo fabricante do computador, sendo aceito em regime de “OEM”, devendo ser entregue documentação comprobatória.

1.13 – Softwares

1.13.1 – Cada equipamento deverá ser acompanhado da licença OEM (Original Equipment Manufacturer) do sistema operacional Microsoft Windows 11 Professional, ou superior, versão em Português do Brasil, com suporte a 64 bits;
1.13.2 – O equipamento deverá ser entregue com uma imagem do sistema operacional e aplicativos pré-configurados baseados em Windows 11 Professional ou superior;
1.13.3 – A licença fornecida deverá garantir atualizações de segurança gratuitas durante todo o prazo de garantia estabelecida pelo fornecedor de hardware, para o sistema operacional Windows 11 Professional 64 Bits, ou superior, em português do Brasil;

1.13.4 – Deverá acompanhar mídia (5% do total de equipamentos) de restauração do sistema operacional, não sendo aceita partição de restore oculta no HD. A mídia poderá ser disponibilizada através de um link para download do site do FABRICANTE do equipamento;
1.13.5 – As licenças devem ser ofertadas para uso corporativo;
1.13.6 – O Contratado deve disponibilizar no seu respectivo website, download gratuito de todos os drivers, BIOS e Firmwares para o equipamento ofertado;

1.14 – Compatibilidade e Certificados

1.14.1 – Conformidade com ROHS Compliance (Restriction of Certain Hazardous Substances, Restrição de Certas Substâncias Perigosas);
1.14.2 – O fabricante ou integradora no Brasil deverá possuir Certificado da série ISO-9001;
1.14.3 – Deve ser comprovado que o computador está preparado para suportar o Windows 11 através do respectivo logo obtido no Windows Compatible Products List;
1.14.4 – Possui certificado IEC60950-1 ou IEC 61 000
1.14.5 – Certificação CISPR;
1.14.6 – Possuir certificado ISO9296;
1.14.7 – Possuir certificado EPEAT Gold;
1.14.8 – A empresa deverá constar como membro do TCG no nível Promoter, comprovado através do link: https://trustedcomputinggroup.org/membership/member-companies/;
1.14.9 – A proponente deverá apresentar documento do fabricante informando que a fonte suporta a configuração máxima do equipamento ofertado.
1.14.10 – O fabricante do referido equipamento, objeto deste edital, deverá ser membro da EICC ou possuir Certificação válida OHSAS 18001, para garantia de conformidade com as questões ambientais, qualidade e segurança do bem-estar de seus funcionários e investimentos ambientais.
1.14.11 – Os equipamentos pertencem à linha corporativa não sendo aceitos equipamentos destinados a publico residencial;

1.14.12 – Os equipamentos são novos e sem uso e serão produzidos em série na época da entrega;

1.15 – Garantia, Suporte, Serviços de Assistência Técnica e Prazos

1.15.1 – Garantia de hardware do FABRICANTE de 48 (quarenta e oito) meses, On Site em Aracaju. Cobertura: 8x5 – De segunda-feira a sexta-feira, exceto feriados, no horário comercial e com atendimento nos próximos seis dias úteis;
1.15.2 – A entrega dos equipamentos deverá ser realizada em até 60 (sessenta) dias corridos após a emissão da Ordem de Fornecimento;
1.15.3 – Disponibilidade de site na WEB (indicar endereço) para Suporte e transferência de arquivos de configuração (Devices Drivers e novas versões de ROM e softwares do equipamento);
1.15.4 – Durante o período de garantia, assistência técnica deverá ser prestada diretamente pelo FABRICANTE ou rede de assistência por ela informada, comprovado através de documento do fabricante;
1.15.5 – A abertura dos chamados técnicos relativos à garantia do equipamento deve ser feita através de “Central de Atendimento” do FABRICANTE, por meio de ligação telefônica gratuita.
1.15.6 – Os equipamentos ofertados deverão ser novos e de primeiro uso além de estar na linha de produção atual do fabricante (não-descontinuados) na data de entrega.
1.15.7 – O FABRICANTE do equipamento deverá informar as assistências técnicas credenciadas e autorizadas a prestar o serviço de garantia no estado de SERGIPE. O documento deve estar incluso na proposta comercial;
1.15.8 – Por questão de segurança e compliance, a Companhia de Saneamento de Sergipe - DESO, deverá reter a unidade de armazenamento defeituosa. Deverá ser apresentado declaração do FABRICANTE para comprovação deste item;
1.15.9 – A garantia do monitor deverá cobrir ainda o reparo ou substituição do monitor no caso do aparecimento de dead pixel (apenas 1 (um) pixel claro queimado);

1.16 – Documentação necessária

1.16.1 – No ato da proposta, apresentar catálogo oficial do fabricante, de acesso público através de website, onde poderão ser conferidas todas as características exigidas para o item e subitens que compõe o item ofertado, contento informações referentes à descrição;

2 – Notebook

2.1 – Gabinete

2.1.1 – O gabinete deverá, obrigatoriamente, ser do mesmo fabricante do equipamento fornecido, não sendo aceito o regime de OEM (Original Equipment Manufacturer);

2.1.2 – O gabinete deverá ter peso máximo de 1,800 Kg com bateria;

2.1.3 – Altura máxima de 2.0 centímetros com bateria;

2.1.4 – Possuir Tela Full HD de 15.6" (1920x1080), 250nits com IPS e Anti Glare;

2.1.5 – Com sistema de refrigeração adequado ao processador, para garantir a temperatura de funcionamento e vida útil dos componentes;

2.1.6 – Alimentação: Compatível com 100-220V, com ajuste automático de voltagem, sem a utilização de adaptadores, conversores ou transformadores e capaz de suportar a configuração completa de acessórios e componentes do equipamento;

2.1.7 – Para cada equipamento deverá ser fornecido cabo de força (NBR 14136), sem emendas, adequado à potência do equipamento.

2.1.8 – Bateria com capacidade mínima de 41WHr;

2.1.9 – Possuir TouchPad.

2.1.10 – Deverá possuir leitor de impressão digital do tipo capacitivo

2.1.11 – Possuir Webcam integrada ao gabinete com resolução HD (1280 x 720) e com tampa de privacidade também integrada;

2.1.12 – Possuir microfone integrado ao gabinete.

3.2 – System Board e Processador

2.2.1 – Arquitetura x86 64bits;

2.2.2 – Deve atingir índice de, no mínimo, 9.000 pontos para o desempenho, tendo como referência a base de dados Passmark CPU Mark disponível no site http://www.cpubenchmark.net/cpu_list.php.

2.2.3 – Processador com no mínimo 4 núcleos físicos e 8 Threads;

2.2.4 – Memória cache total com o mínimo de 8 MB;

2.2.5 – Cooler para o processador de fabricação ou de fornecimento em regime de OEM pelo respectivo fabricante do processador ou equivalente;

2.2.6 – Recurso de shutdown automático em caso de temperatura elevada;

2.2.7 – O equipamento ofertado deverá possuir no mínimo de 16 GB de memória RAM instalada, e suportar expansão até 64GB;

2.2.8 – A memória deverá ser do tipo DDR4 com velocidade de no mínimo 3200MHz;

2.2.9 – O equipamento deverá possuir 02 (dois) slots de memória RAM

2.2.10 – Placa-mãe do mesmo fabricante, não sendo aceito placas de livre comercialização no mercado, sujeito a verificação pelos técnicos da DESO com fornecimento de amostra se solicitado.

2.2.11 – Com suporte a virtualização baseada em hardware (também conhecida como hardware-based virtualization ou hardware-assisted virtualization).

2.2.12 – O chipset deverá pertencer à geração mais recente disponibilizada pelo Fabricante, compatível com o processador ofertado;

2.3 – Setup

2.3.1 – O equipamento possui BIOS desenvolvida pelo mesmo fabricante do equipamento, ou possuir direitos copyright sobre essa BIOS atestado pelo fabricante da BIOS. Caso a BIOS seja ofertada em regime de copyright, o fabricante da BIOS deverá atestar que o fabricante do

notebook possui livre direito de edição sobre ela, garantindo assim adaptabilidade e manutenibilidade do conjunto adquirido;

2.3.2 – Suporta configuração de senhas na BIOS a três níveis: administrador, HD e usuário, que controlem acesso ao boot do Sistema Operacional e à própria BIOS;

2.3.3 – Permite inserir registro de controle patrimonial, de pelo menos 10 (dez) caracteres em memória não volátil;

2.3.4 – BIOS português ou inglês, desenvolvida pelo fabricante em conformidade com a especificação UEFI 2.1 (http://www.uefi.org), e capturáveis pela aplicação de inventário SCCM (System Center Configuration Manager);

2.3.5 – O fabricante deverá possuir compatibilidade com o padrão UEFI comprovada através do site http://www.uefi.org/members, na categoria membros.

2.3.6 – Possuir ferramenta que possibilite realizar a formatação definitiva dos dispositivos de armazenamento conectados ao equipamento, desenvolvida em acordo com o padrão de segurança NIST 800-88 ou ISO/IEC 27040:2015. Caso esta ferramenta não seja nativa da BIOS, deverá ser oficialmente homologada pelo Fabricante do equipamento, comprovado com documento do fabricante;

2.3.7 – Possuir sistema integrado de diagnóstico que permita verificar a saúde do sistema em modo rápido e em modo detalhado, bem como diagnóstico na BIOS em modo gráfico, capaz de verificar os seguintes itens:

2.3.8 – Saídas de vídeo;

2.3.9 – Alto-falante interno;

2.3.10 – Unidades de Armazenamento;

2.3.11 – Funcionalidade de portas USB;

2.3.12 – Interface gráfica

2.3.13 – Processador;

2.3.14 – Memória RAM;

2.3.15 – Bateria;

2.3.16 – A mensagem de erro gerada por este diagnóstico deverá ser o suficiente para abertura de chamado do equipamento durante o período de vigência da garantia.

2.4 – Segurança

2.4.1 – O equipamento deve possuir recurso de segurança TPM versão 2.0, que atenda às especificações do TCG (Trusted Computing Group) e seja compatível com sistemas de criptografia (ex.: BitLocker). São aceitas implementações discretas (chip físico) ou integradas (firmware), desde que reconhecidas nativamente pelo Windows como TPM 2.0.;
2.4.2 – Possuir entrada, integrada ao chassi, para cabo de segurança;

2.5 – Interface USB

2.5.1 – Deve possuir no mínimo 4 (quatro) portas USB externas nativas, sendo:
2.5.2 – Pelo menos 03 (três) portas, ao menos 02 (duas) USB-A 3.2 e 01 (uma) USB-C.

2.6 – Controladora de Áudio

2.6.1 – Controladora de áudio integrada que suporta o padrão AC'97 áudio CODEC ou padrão HD Áudio;
2.6.2 – Possuir pelo menos 02 (dois) alto-falantes internos com potência suportada mínima de 2 Watts;
2.6.3 – Deve possuir pelo menos 01 (uma) saída de áudio P2 do tipo Combo;

2.7 – Controlador Gráfico

2.7.1 – Deverá possuir tela de 15.6 polegadas, resolução Full HD (1920x1080), antirreflexiva;
2.7.2 – Deverá possuir controlador gráfico integrado com as seguintes especificações mínimas:

2.7.3 – Frequência dinâmica mínima de 1.2GHz;
2.7.4 – Memória compartilhada alocada dinamicamente: 1.7GB
2.7.5 – Capaz de suportar 03 (três) monitores simultaneamente, 1 integrado internamente e 2 externos;
2.7.6 – Suporte a DirectX 12.1;
2.7.7 – Deverá suportar resolução em 4K;
2.7.8 – Deverá suportar OpenGL 4.6;
2.7.9 – Possuir pelo menos uma porta do tipo HDMI;

2.8 – Interfaces de Rede

2.8.1 – Controladora Gigabit-Ethernet, com conector no formato RJ-45 integrado ao gabinete, não sendo aceitos adaptadores para suprir essa finalidade;
2.8.2 – Deve suportar as velocidades de transmissão de 10/100/1000 Mbps (Megabits por segundo), com chaveamento automático;
2.8.3 – Deverá suportar os protocolos WOL e PXE;
2.8.4 – Deve possuir Placa wireless interna em conformidade com os padrões 802.11ax dualband, com bluetooth na versão 5.1 ou superior;

2.9 – Armazenamento

3.9.1 – Disco Padrão NVMe com capacidade de armazenamento de, no mínimo, 256 GB (GigaBytes);

2.10 – Softwares
2.10.1 – Cada equipamento deverá ser acompanhado da licença OEM (Original Equipment Manufacturer) do sistema operacional Microsoft Windows 11 Professional, ou superior, versão em português do Brasil, com suporte a 64 bits;

2.10.2 – O equipamento deverá ser entregue com uma imagem do sistema operacional e aplicativos pré-configurados baseados em Windows 11 Professional ou superior;
2.10.3 – A licença fornecida deverá garantir atualizações de segurança gratuitas durante todo o prazo de garantia estabelecida pelo fornecedor de hardware, para o sistema operacional Windows 11 Professional 64 Bits, ou superior, em português do Brasil;
2.10.4 – Deverá acompanhar mídia (5% do total de equipamentos) de restauração do sistema operacional, não sendo aceita partição de restore oculta no HD. A mídia poderá ser disponibilizada através de um link para download do site do FABRICANTE do equipamento;
2.10.5 – As licenças devem ser ofertadas para uso corporativo;
2.10.6 – O Contratado deve disponibilizar no seu respectivo website, download gratuito de todos os drivers, BIOS e Firmwares para o equipamento ofertado;

2.11 – Compatibilidade e Certificados

2.11.1 – Conformidade com ROHS Compliance (Restriction of Certain Hazardous Substances, Restrição de Certas Substâncias Perigosas);
2.11.2 – O fabricante ou integradora no Brasil deverá possuir Certificado da série ISO-9001;
2.11.3 – O fabricante do equipamento possui sistema de gestão ambiental conforme norma ISO 14001;
2.11.4 – Possuir certificado EPEAT Silver ou superior;
2.11.5 – A empresa deverá constar como membro do TCG no nível Promoter, comprovado através do link: https://trustedcomputinggroup.org/membership/member-companies/;
2.11.6 – O fabricante do referido equipamento, objeto deste edital, deverá ser membro da EICC ou possuir Certificação válida OHSAS 18001, para garantia de conformidade com as questões ambientais, qualidade e segurança do bem-estar de seus funcionários e investimentos ambientais.
2.11.7 – Os equipamentos deverão pertencer à linha corporativa não sendo aceitos equipamentos destinados a uso doméstico;

2.11.8 – Os equipamentos são novos e sem uso e serão produzidos em série na época da entrega;

2.12 – Garantia, Suporte, Serviços de Assistência Técnica e Prazos

2.12.1 – 1.1. Deverá possuir 48 (quarenta e oito) meses de garantia para o equipamento e seus periféricos e 36 (trinta e seis) meses de garantia para a bateria, ambos na modalidade on-site em Aracaju/Sergipe. A garantia deverá ser executada pelo FABRICANTE ou rede credenciada, devendo ser comprovado através de documento do fabricante;
2.12.2 – A entrega dos equipamentos deverá ser realizada em até 60 (sessenta) dias corridos após a emissão da Ordem de Fornecimento;
2.12.3 – Disponibilidade de site na WEB (indicar endereço) para Suporte e transferência de arquivos de configuração (Devices Drivers e novas versões de ROM e softwares do equipamento);
2.12.4 – A abertura dos chamados técnicos relativos à garantia do equipamento deve ser feita através de “Central de Atendimento” do FABRICANTE, por meio de ligação telefônica gratuita.
2.12.5 – Os equipamentos ofertados deverão ser novos e de primeiro uso além de estar na linha de produção atual do fabricante (não-descontinuados) na data de entrega.
2.12.6 – O FABRICANTE do equipamento deverá informar as assistências técnicas credenciadas e autorizadas a prestar o serviço de garantia no estado de SERGIPE. O documento deve estar incluso na proposta comercial;
2.12.7 – Por questão de segurança e compliance, a Companhia de Saneamento de Sergipe - DESO, deverá reter a unidade de armazenamento defeituosa. Deverá ser apresentado declaração do FABRICANTE para comprovação deste item;
2.12.8 – A garantia do FABRICANTE, deverá fornecer ainda proteção contra danos acidentais, tais como quedas, derramamento de líquidos e ou sobrecargas elétricas. Deverá ser comprovado por documento do fabricante;

2.13 – Documentação necessária

2.13.1 – No ato da proposta, apresentar catálogo oficial do fabricante, de acesso público através de website, onde poderão ser conferidas todas as características exigidas para o item e subitens que compõe o item ofertado, contendo informações referentes à descrição;

19.4 SOFTWARE SUPERVISÓRIO (SCADA) E PLATAFORMA IoT

As funções principais do software supervisório são de aquisição, controle e visualização de dados provenientes do processo, ou seja:

a) Monitorar e controlar equipamentos e o processo;
b) Coletar e compartilhar dados em tempo real e dados históricos para todos os níveis da empresa;
c) Responder rapidamente às condições do processo e às demandas de mercado;
d) Maximizar a eficiência da planta, aumentar produtividade e reduzir custos e perdas;
e) Ter um sistema de automação totalmente seguro que garanta 100% da integridade dos dados.

O PROPONENTE deverá apresentar, em sua proposta técnica, a especificação dos tipos e quantitativos de licenças do software supervisório, de modo a garantir o atendimento à arquitetura IoT prevista, incluindo o dimensionamento da quantidade de TAGs, telas de supervisão e demais funcionalidades necessárias à operação e expansão do sistema.

O licenciamento deverá contemplar, no mínimo:

- Quantidade de TAGs necessárias para o monitoramento e controle das variáveis de processo previstas no escopo;
- Quantidade de telas de supervisão e operação;
- Licenças de Servers em redundância Hot-Standby, Server Lite, Historiadores, Viewers e Engenharia (desenvolvimento);
- Drivers para comunicação com dispositivos de campo, CLPs, RTUs e demais sistemas integrantes da arquitetura;
- Possibilidade de expansão futura do sistema, sem necessidade de substituição da plataforma supervisória.

19.4.1. Arquitetura do Sistema

O sistema supervisório deverá possuir arquitetura aberta, modular eescalável, compatível com aplicações de Internet das Coisas (IoT), permitindo a integração de equipamentos de campo, estações remotas e centros de operação por meio de protocolos padronizados de comunicação.

A arquitetura deverá contemplar, no mínimo:

- Servidor(es) de supervisão;
- Estações cliente de operação;
- Servidores de historiador de dados;
- Integração com equipamentos de campo (CLPs, RTUs, gateways e instrumentos);
- Integração com o Centro de Controle Operacional (CCO).

A solução deverá permitir expansão futura sem necessidade de substituição da plataforma supervisória.

19.4.2. Arquitetura de Alta Disponibilidade

O sistema supervisório deverá possuir recursos de alta disponibilidade, visando garantir a continuidade da operação em caso de falhas de hardware ou software.

A arquitetura deverá prever, quando aplicável:

- Servidores redundantes em configuração Hot Standby ou equivalente;
- Sincronização automática de dados entre servidores;
- Retomada automática da operação em caso de falha do servidor principal;

- Mecanismos de backup e recuperação de dados.

19.4.3. Edge Computing

A arquitetura do sistema deverá prever a utilização de computação de borda (Edge Computing) nas unidades operacionais ou estações remotas.

Os dispositivos de borda deverão permitir:

- Coleta local de dados de processo;
- Processamento preliminar de informações;
- Execução de lógicas de automação ou análise de dados;
- Armazenamento temporário de dados em caso de perda de comunicação com o servidor central;
- Sincronização automática dos dados após restabelecimento da comunicação.

Essa abordagem deverá garantir maior confiabilidade, redução do tráfego de rede e maior resiliência do sistema.

19.4.4. Arquitetura de Dados – Unified Namespace (UNS)

A solução deverá permitir a implementação de uma arquitetura baseada em Unified Namespace (UNS) para organização e distribuição de dados industriais.

A arquitetura deverá possibilitar:

- Estrutura hierárquica padronizada de dados;
- Publicação e consumo de dados em tempo real por diferentes sistemas;
- Integração com plataformas de analytics, Big Data e sistemas corporativos;

- Redução da dependência de integrações ponto a ponto.

  Essa arquitetura deverá utilizar protocolos baseados em publish/subscribe, como MQTT.

19.4.5. Comunicação e Protocolos

O sistema deverá suportar comunicação com dispositivos e sistemas utilizando protocolos industriais amplamente utilizados, incluindo, mas não se limitando a:

- Modbus TCP/IP
- Modbus RTU
- OPC UA
- MQTT para integração com arquitetura IoT
- Outros protocolos nativamente suportados pelo software supervisório.

A comunicação deverá permitir operação segura e confiável, inclusive em ambientes com conectividade intermitente.

19.4.6. Sistema de Historiador de Dados

O sistema deverá possuir mecanismo de armazenamento histórico das variáveis de processo, alarmes e eventos.

O historiador deverá permitir:

- Armazenamento de dados de processo por longo período;
- Consulta histórica de variáveis;
- Geração de relatórios operacionais;
- Exportação de dados para sistemas corporativos.

Em caso de perda de comunicação com o servidor central, deverá ser garantido o armazenamento local temporário dos dados, com posterior sincronização automática.

19.4.7. Licenciamento de Software

O PROPONENTE deverá apresentar em sua proposta técnica a especificação detalhada dos tipos e quantitativos de licenças necessárias para o pleno funcionamento do sistema supervisório.

O dimensionamento deverá contemplar:

- Quantidade de TAGs de supervisão e controle;
- Quantidade de telas de supervisão e operação;
- Licenças de clientes de operação;
- Licenças de clientes de engenharia;
- Recursos de comunicação com dispositivos de campo;
- Recursos de armazenamento histórico.

Todos os softwares fornecidos no escopo deste contrato deverão possuir licenças legais, originais e válidas, compatíveis com a arquitetura e funcionalidades previstas para o sistema.

Todas as licenças de software fornecidas no escopo deste contrato deverão ser emitidas e registradas em nome da CONTRATANTE, garantindo seu pleno direito de uso.

As licenças deverão ser emitidas e registradas em nome da CONTRATANTE, garantindo seu pleno direito de uso, operação, manutenção e expansão do sistema. O fornecimento deverá incluir todas as chaves de ativação, mídias de instalação, documentação técnica e demais elementos necessários para instalação, reinstalação e manutenção do sistema.

As licenças fornecidas deverão ser permanentes, não vinculadas a assinaturas periódicas. O fornecimento deverá incluir todas as chaves de ativação, mídias de instalação, documentação técnica e demais elementos necessários para instalação, reinstalação e manutenção do sistema.

19.4.8. Segurança Cibernética

O sistema deverá atender boas práticas de segurança cibernética, aplicáveis a sistemas industriais, contemplando:

- Autenticação de usuários por níveis de acesso;
- Registro de eventos e auditoria de usuários;
- Comunicação segura entre dispositivos;
- Criptografia quando aplicável;
- Possibilidade de integração com políticas corporativas de segurança.

19.4.9 Tecnologias Envolvidas e Arquitetura

O software deve possuir e/ou suportar as seguintes tecnologias e arquiteturas de aplicação:

a) Compatibilidade com os seguintes sistemas operacionais: Windows 10, Windows 10 IoT, Windows 11, Windows Server 2019, Windows Server 2022 e Windows Server 2025 da Microsoft.
b) Ser cliente e servidor OPC DA, OPC UA e OPC A&E.
c) Capaz de adicionar controles ActiveX e aproveitar as vantagens de suas propriedades, eventos e métodos.
d) Permitir acesso aos dados do servidor SCADA via conexão ODBC do Windows para os dados em tempo real e para dados históricos.
e) Suporte a Windows 64 bits e à virtualização de máquina (ex: VMWare).
f) Permitir, ainda que com licenciamento separado, acesso às telas via web browser, mobile (ambos com tecnologia HTML5) e via conexão remota, através da tecnologia Remote Desktop Services (RDS) da Microsoft.
g) Possibilitar a configuração de uma arquitetura de alta disponibilidade através da redundância de servidores de dados.
h) Permitir o gerenciamento de estações e configuração de projetos (ex. criação de projetos, edição das bases de dados, das configurações de rede, redundância) de maneira centralizada, preferencialmente via interface web.
i) Possuir um banco de dados temporal nativo ou já incluso, sem custo adicional, que permita a coleta e armazenamento de dados do SCADA para visualização dos dados dentro e fora do mesmo.

19.4.10 Telas

No que diz respeito ao desenvolvimento e uso das telas, o software deve possuir as seguintes funcionalidades:

a) Redimensionamento automático das telas quando houver alteração da resolução do monitor.
b) Personalização de paletas de cores e disponibilizá-las globalmente para o sistema.
c) Recebimento informações direto de servidores OPC, sem passar pela base de dados.
d) Personalização e criação de barras de ferramentas, de modo que cada usuário consiga ter uma “toolbox” com as funcionalidades mais relevantes para si.
e) Possuir assistentes (“wizards"), que permitam a adição de funcionalidades (ex. evento de clique que reconhece um alarme ou navega para uma tela) através de uma interface intuitiva, eliminando a necessidade de gerar ou modificar scripts.
f) Permitir o agrupamento de objetos e manipulação das propriedades desses objetos agrupados de forma independente, isto é, sem a necessidade de desagrupá-los.
g) Os objetos nas telas geradas pelo software devem ter Refresh (atualização dos dados na tela) independentes. Se um tag da base de dados tem uma atualização a cada 1 (um) segundo e outro tag tem 5 (cinco) segundos, a tela deve processar cada objeto de forma independente e correspondente a varredura definida na base de dados.
h) Procurar e substituir tags na tela (Find/Replace) automaticamente.
i) A janela de propriedades para mostrar todas as propriedades de um objeto gráfico.
j) Link de valores indicando estado do tag (manual, automático, manutenção, falha, etc).
k) Link/Fields na tela para acompanhamento do estado das estações e caminhos ativos (PCs e IPs ativos).
l) Possuir suporte a múltiplos monitores, tanto para desenvolvimento quanto para execução das telas.

m) Permitir “voltar a tela no tempo”, habilitando a visualização retroativa dos dados históricos em tela, com controles do tipo “play”, “voltar”, “avançar”, “loop”, além de seleção de data e hora específicas.
n) Possuir interface para salvar anotações feitas pelo usuário, com rastreabilidade de data, hora, operador e estação onde a nota foi feita, além da possibilidade de formatação de cada nota.
o) Possuir ferramenta de visualização de toda a base de dados em modo de operação.
p) Possuir bibliotecas de objetos, paletas de cores e demais elementos no padrão ISA-101, habilitando o desenvolvimento de telas de alta performance.
q) Permitir a estruturação das tags em uma hierarquia de ativos, adicionando contexto e facilitando a busca de tags pelos usuários.
r) Possuir ferramenta de propagação em massa de mudanças em animações e elementos gráficos do sistema, sem necessidade de reedição individual de cada chamada do elemento em tela.
s) Permitir que o operador aplique “zoom” na tela, aumentando o tamanho dos elementos conforme necessário. Também deve permitir deslocar o zoom dentro da tela.
t) Permitir tornar um objeto gráfico visível apenas quando determinado nível de zoom for aplicado, eliminando poluição visual quando necessário.
u) Possuir um contêiner configurável que permita separar sub-telas em abas e incluir objetos dentro delas, de modo similar às abas de um “web browser”.

19.4.11 Gráficos

No que diz respeito aos gráficos de tendência, devem possuir os seguintes recursos:

a) Apresentar informações de tags em tempo real e informações de dados históricos coletados em um único gráfico para permitir comparação de processo atual com histórico de produção.

b) Somar valores e funções diretamente na pena do gráfico, sem ter que acrescentar tags na base de dados. Exemplo: apresentar no gráfico a diferença entre os valores de duas vazões.
c) Variar automaticamente a escala do valor do eixo de variáveis, apenas clicando sobre a variável desejada.
d) Permitir configuração on-line de variáveis, escala, tempo de duração, intervalo de atualização, zoom etc.
e) Não ter limite de número de variáveis por gráfico e não ter limite de número de gráficos por tela.
f) Possuir recursos gráficos para apresentação de informações estatísticas: gráfico X-Y, X-bar, histograma, CEP etc.
g) Possuir um gráfico “instantâneo”, de modo a gerar um gráfico de uma ou mais tags selecionadas instantaneamente, não precisando criar e configurar objetos para análises pontuais.

19.4.12 Alarmes

Em relação aos alarmes do SCADA, as seguintes funcionalidades devem estar presentes:

a) Geração automática de log de alarmes em arquivos ASCII, banco de dados relacional, sumário de alarmes e link de dados na tela do operador. Isso deve estar disponível no software via configuração. Não é aceitável programas externos ou macros via scripts.
b) Habilitar/Desabilitar alarmes de um tag de acordo com um evento do campo.
c) Possibilidade de gerar log de eventos automaticamente (comandos, ação de operador etc.).
d) Sincronismo de reconhecimento de alarmes entre as estações. Ao reconhecer um alarme em uma estação, esse alarme tem que ser reconhecido em todas as outras estações instantaneamente.
e) Possuir característica de gerar e permitir consultas no protocolo OPC A&E (OPC para alarmes e eventos).
f) Possuir o recurso de “Alarm Shelving”, que possibilita o silenciamento temporário de alarmes. Também deve estar presente o contador de alarmes que estão em “Shelving”.
g) Permitir alteração de alarmes e possibilidade de desabilitar os mesmos, permitindo ao operador fazer comentários nos alarmes desabilitados.
h) Permitir a visualização dos tags e alarmes desabilitados.

19.4.13 Base de dados de processo

Em relação à base de dados de processo do SCADA, os seguintes recursos devem estar inclusos:

a) Permitir que sua base de dados seja exportada/importada em padrão CSV (Comma Separated Value - MS Excel).
b) Permitir a geração automática de tags na base de dados com campos similares. Por exemplo, gerar 1000 (mil) tags digitais variando de TAG1 a TAG1000, endereço 1 a 1000, descritivo TAG1 a TAG1000, de uma só vez.

c) Geração automática de número de série vinculada a toda alteração feita na base de dados.
d) Na manipulação da base de dados (modificar, acrescentar e/ou apagar) todos os tags têm que estar em operação, a menos do bloco que está sendo manipulado naquele instante. Na manipulação da base de dados, o carregamento da mesma deve ser automático.
e) Permitir consultas (“queries”) para filtrar tags com nomes, drivers, tipos etc. específicos.
f) Permitir configuração da base de dados do Sistema Historiador descrito no item 2.2 deste documento (configuração da taxa de coleta, unidades etc.) de maneira integrada, dentro do próprio editor de base de dados do sistema SCADA.
g) Todos os blocos a seguir descritos devem estar disponíveis na base de dados, independentemente da visualização gráfica (HMI) e sem necessidade de customização em script:
    a. Blocos de Linguagem Estruturada (Dados SQL e Disparo SQL).
    b. Blocos de Gerenciamento de Batelada (Controle de Dispositivo e Program).
    c. Controle Estatístico de Processo (com Histograma e Dados Estatísticos).
    d. Blocos de Controles de algorítmos definidos (Lead-Lag, PID, Rampa, Liga-Desliga).

19.4.14 Segurança

Em relação à segurança, o software SCADA deve possuir os seguintes recursos:

a) O software deve ter um módulo de segurança que permita configuração de usuários, grupo de usuários e acesso às telas, tags e alarmes.
b) Permitir usar o usuário do próprio Windows para fazer login.
c) Log de eventos que registra toda vez que alguém se conecta e desconecta na aplicação.
d) Deve ter um “time out” por conta/usuário/senha. Se o usuário não fizer nenhuma atuação na aplicação ele será desconectado.
e) Deve suportar a criação de uma estrutura de segurança centralizada utilizando UAA que seja possível integrar com controladores de domínio via LDAP ou SAML.

19.4.15 Agendamento de eventos e tarefas

O software deve permitir agendar eventos e tarefas, e os seguintes recursos devem estar presentes:

a) Associar eventos de processo (tags) ou de tempo a ações (como instruções e mensagens ao operador, chamada de relatório, execução de receitas, execução de programas externos etc.).
b) Geração de relatórios por evento de tag ou tempo.
c) Discagem a estações remotas por evento de tag ou tempo.
d) Envio de alarmes remotos por evento de tag ou tempo.

19.4.16 Scripting

Em relação ao uso e desenvolvimento de scripts, o software deve possuir as seguintes funcionalidades:

a) Linguagem de comando (script) padrão e aberta para reaproveitamento em todos os projetos.
b) Não ter limitação de linhas de comando.
c) A atualização da tela não pode ser interrompida enquanto comandos são executados.
d) A linguagem de comando deve suportar lógicas como “If/Else”, “For” e “While”.
e) A linguagem de comando deve ter categorização de scripts. Os scripts devem ser associados à tela ou a um elemento global para que todo o projeto tenha acesso.

19.4.17 Drivers de comunicação

O sistema de supervisão deve ter compatibilidade nativa com os protocolos, mais comuns de mercado, dos principais fabricantes de equipamentos de automação, compatíveis com as tecnologias Ethernet/IP, MQTT, Modbus TCP, Modbus RTU, IoT, como por exemplo: ABB, Allen-Bradley, Siemens, GE, Schneider Electric.

19.4.18 Backup de aplicação

O software deve ter ferramentas de backup automático e manual da aplicação, com as seguintes funcionalidades:

a) Um utilitário para fazer backup da aplicação: telas, base de dados, configuração de driver de comunicação, schedules, grupos de tags, alarmes, dados históricos, receitas e configuração da estação.
b) O mesmo utilitário do item a) deve ser utilizado para restauração dos backups.

c) O software deverá fazer backup automaticamente dos arquivos de telas, de bases de dados e de configuração de projetos, sem que nenhuma ação manual seja necessária.

19.4.19 Ferramentas de diagnóstico e manutenção

A solução SCADA deve possuir os seguintes recursos para manutenção e solução de problemas:

a) Conter campos informativos de transmissão, recepção, erro de protocolo, timeouts e retries;

19.4.18 Backup de aplicação

O software deve ter ferramentas de backup automático e manual da aplicação, com as seguintes funcionalidades:

d) Um utilitário para fazer backup da aplicação: telas, base de dados, configuração de driver de comunicação, schedules, grupos de tags, alarmes, dados históricos, receitas e configuração da estação.
e) O mesmo utilitário do item a) deve ser utilizado para restauração dos backups.
f) O software deverá fazer backup automaticamente dos arquivos de telas, de bases de dados e de configuração de projetos, sem que nenhuma ação manual seja necessária.

19.4.19 Ferramentas de diagnóstico e manutenção

A solução SCADA deve possuir os seguintes recursos para manutenção e solução de problemas:

b) Conter campos informativos de transmissão, recepção, erro de protocolo, timeouts e retries;
c) Datascope para verificar e acompanhar a comunicação com o PLC;

d) Histórico de dados: o software deve monitorar o coletor de dados históricos, verificando se ocorre perda de dados (overruns);
e) Informar a execução dos comandos SQL entre o software supervisório e o software do banco de dados relacional;
f) Prover relatório estatístico sobre o processamento da base de dados (informações de número de ciclos/segundo, número de ciclos/minuto, número de blocos processados, número de blocos processados/segundo).
g) Simular a perda de comunicação e verificar a indicação dos datalinks de valores na tela e mensagens ao operador. Deve ter a possibilidade de personalizar estas mensagens.

20. OPERAÇÃO ASSISTIDA E TREINAMENTOS

20.1 Execução de operação assistida pelo período mínimo de 365 (trezentos e sessenta e cinco) dias, contemplando acompanhamento técnico presencial e remoto pela CONTRATADA, destinado à estabilização operacional dos sistemas implantados, realização de ajustes de parametrização, calibrações finais, testes de desempenho e verificação funcional, bem como à validação da integração e da interoperabilidade com o Sistema de Detecção de Vazamentos e com o Centro de Controle Operacional (CCO), até a plena aceitação operacional pela CONTRATANTE;

20.2 Treinamento da equipe técnica a ser definida pela DESO, abrangendo:

– Procedimentos de operação e manutenção dos equipamentos instalados;
– Análise e interpretação de dados operacionais, bem como procedimentos de resposta a alarmes e eventos;

– Utilização, navegação e configuração das ferramentas disponibilizadas no CCO;

– Software supervisório: elaboração de telas, configuração de tags, scripts, drivers de comunicação, etc;

– Configuração dos equipamentos de IoT: gateways, radio-modem, etc

– Configuração dos instrumentos de campo: medidores de vazão, pressão, temperatura, nível, MGE;

21. ENTREGÁVEIS DO PROJETO

Ao final da implantação, a CONTRATADA deverá entregar à CONTRATANTE os seguintes produtos e documentos técnicos:

21.1. Sistema de Monitoramento Remoto

Implantação de um sistema de monitoramento remoto plenamente operante, permitindo à DESO acompanhar em tempo real todas as etapas do processo, desde a captação até o ponto de entrega da água tratada à concessionária.

O sistema deverá estar integrado ao Centro de Controle Operacional (CCO) a ser implantado no Estado de Sergipe, possibilitando a supervisão, registro e análise das variáveis operacionais do sistema.

21.2. Relatórios Técnicos de Implantação

Deverão ser fornecidos relatórios técnicos contendo o registro das atividades realizadas durante a implantação do sistema, incluindo:

- Relatórios de execução dos serviços;
- Relatórios de testes de funcionamento;
- Registros de calibração dos instrumentos;
- Relatórios de validação operacional do sistema.

21.3. Sistema Integrado e Comissionado

Entrega do sistema em plena operação, com todos os equipamentos, softwares e interfaces devidamente instalados, configurados e integrados ao CCO, com funcionamento comprovado por meio de testes de comissionamento e validação operacional.

21.4. Documentação Técnica “As Built”

Deverá ser entregue a documentação final atualizada do sistema implantado (As Built), incluindo, no mínimo:

- Diagramas elétricos;
- Diagramas hidráulicos;
- Diagramas de arquitetura de comunicação;
- Diagramas de lógica de controle e automação;
- Topologia de rede e comunicação dos equipamentos.

21.5. Manuais Técnicos e Operacionais

Fornecimento de manuais técnicos e operacionais completos, contendo orientações para:

- Operação do sistema;
- Manutenção preventiva e corretiva;
- Configuração básica dos equipamentos e softwares;
- Procedimentos de diagnóstico e solução de falhas.

21.6. Treinamento e Operação Assistida

Realização de treinamento técnico para a equipe da CONTRATANTE, contemplando a operação e manutenção do sistema implantado.

Deverão ser fornecidos:

- Certificados de participação no treinamento;
- Registro formal das atividades de operação assistida, realizadas durante o período de acompanhamento inicial da operação do sistema.

22. TESTES DE ACEITAÇÃO EM CAMPO DO SISTEMA DE MONITORAMENTO

O Teste de Aceitação em Campo (TAC) tem como objetivo verificar e validar, em ambiente operacional, o correto funcionamento de todos os equipamentos, sistemas e integrações fornecidos no escopo do contrato.

O TAC deverá ser realizado após a conclusão das etapas de instalação, configuração e testes preliminares do sistema, sendo conduzido pela CONTRATADA na presença de representantes da CONTRATANTE.

A aprovação do TAC será condição para a aceitação provisória do sistema.

22.1. Objetivos do TAC

O TAC deverá comprovar que:

- Todos os equipamentos foram instalados conforme projeto;
- Os sistemas de automação e telemetria estão operando corretamente;
- A comunicação entre os dispositivos de campo e o sistema supervisório está funcional;
- As variáveis de processo estão sendo corretamente monitoradas e registradas;

- O sistema está integrado ao Centro de Controle Operacional (CCO).

22.2. Escopo dos Testes

Os testes deverão abranger, no mínimo:

- Instrumentação de campo;
- Painéis de automação;
- Painéis Elétricos;
- Unidades de Telemetria Remotas UTRs;
- Sistemas de comunicação e telemetria;
- Sistema supervisório (SCADA);
- Integração com o CCO;
- Sistema de armazenamento histórico de dados.

22.3. Procedimentos de Teste

Durante o TAC deverão ser realizados, no mínimo, os seguintes procedimentos:

22.3.1 Verificação de Instalação

- Conferência da instalação física dos equipamentos;
- Verificação da identificação e etiquetagem dos dispositivos;
- Conferência da alimentação elétrica e proteção dos equipamentos.

22.3.2 Testes de Instrumentação

- Verificação da leitura das variáveis de processo (pressão, vazão, nível, entre outras);

- Conferência das calibrações realizadas;
- Verificação da correspondência entre o sinal de campo e a variável apresentada no sistema supervisório.

22.3.3 Testes de Comunicação

- Verificação da comunicação entre instrumentos e UTRs;
- Verificação da comunicação entre UTRs e o sistema supervisório;
- Verificação da comunicação com o CCO.

22.3.4 Testes do Sistema Supervisório

- Verificação do funcionamento das telas de supervisão;
- Teste de geração e registro de alarmes;
- Teste de registro histórico de variáveis;
- Teste de atualização em tempo real das informações de processo.

22.3.5 Testes de Integração

- Verificação da integração entre os sistemas locais e o CCO;
- Verificação da transmissão de dados históricos e em tempo real.

22.4. Registro dos Testes

Todos os testes realizados deverão ser registrados em relatórios de teste, contendo:

- Descrição do teste executado;
- Resultados obtidos;
- Eventuais não conformidades identificadas;

- Ações corretivas adotadas.

Os relatórios deverão ser assinados por representantes da CONTRATADA e da CONTRATANTE.

22.5. Critérios de Aprovação

O TAC será considerado aprovado quando:

- Todos os testes previstos forem executados com resultados satisfatórios;
- Eventuais não conformidades forem corrigidas;
- O sistema demonstrar operação estável e confiável.

22.6. Aceitação Provisória e Definitiva

Após a aprovação do SAT, poderá ser emitido o Termo de Aceitação Provisória, permitindo o início do período de operação assistida.

A aceitação definitiva ocorrerá após o término satisfatório do período de operação assistida e da entrega de toda a documentação técnica final.

23. TESTES DE ACEITAÇÃO EM CAMPO DO SISTEMA DE DETECÇÃO DE VAZAMENTO SDV - Conforme descrito no item 1.2 deste documento.