JUSTIÇA FEDERAL
CONSELHO DA JUSTIÇA FEDERAL

CONTRATO CJF N. 029/2019

que entre si celebram o **CONSELHO DA JUSTIÇA FEDERAL** e a **MTEL SOLUÇÕES S.A**, para a aquisição de solução de infraestrutura de rede de comunicação de dados, incluindo serviços de instalação, configuração, migração, suporte técnico onsite, transferência de conhecimento e garantia dos equipamentos e softwares pelo período de 60 (sessenta) meses.

O CONSELHO DA JUSTIÇA FEDERAL - CJF, órgão integrante do Poder Judiciário, inscrito no CNPJ/MF n. 00.508.903/0001-88, com sede no Setor de Clubes Esportivos Sul, Trecho III, Polo 8, Lote 9, Brasília - DF, doravante denominado **CONTRATANTE**, neste ato representado por sua Secretária-Geral, a Exma. Juíza Federal **SIMONE DOS SANTOS LEMOS FERNANDES**, brasileira, CPF/MF n. 418.381.906-78, Carteira de Identidade n. 1075089 – SSP - MG, residente em Brasília - DF, e a **MTEL SOLUÇÕES S.A**, pessoa jurídica de direito privado, inscrita no CNPJ/MF n. 05.280.162/0001-44, estabelecida na Alameda Araguaia n° 500, 21° andar - Torre II, Barueri, São Paulo - SP, CEP n° 06454-000, doravante denominada **CONTRATADA**, neste ato representada por seu Diretor Presidente, o senhor **FREDERICO SAMARTINI QUEIROZ ALVES**, brasileiro, CPF/MF n. 013.465.086-74 e Carteira de Identidade n. MG8634418 - SSP/MG, residente em São Paulo - SP, e por sua Diretora de Contabilidade e Controladoria, a senhora **GABRIELLY ANDRESSA NAGY**, brasileira, CPF/MF n. 071.700.579-80 e Carteira de Identidade n. 59.616.486-5 - SSP/SP, residente em Barueri - SP, celebram o presente contrato com fundamento na Lei n. 8.666/1993 e alterações, Lei n. 12.846/2013, Lei n. 10.520/2002 e, em conformidade com as informações constantes do Processo SEI n. 0002279- 11.2019.4.90.8000, mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1 Constitui objeto deste contrato a aquisição de solução de infraestrutura de rede de comunicação de dados, incluindo serviços de instalação, configuração, migração, suporte técnico on-site, transferência de conhecimento e garantia dos equipamentos e softwares pelo período de 60 (sessenta) meses, compreendendo os seguintes lotes:

1.1.1 Lote 1: Fornecimento de solução de comunicação de dados incluindo equipamentos para rede LAN e Datacenter (switches para camadas acesso, leaf, spine e SAN), software de gerência dos ativos, rack de rede, cabos (patch cords) de 1,5m e 2,5m e serviço de organização e troca do cabeamento das salas técnicas dos andares;

1.1.2 Lote 2: Fornecimento de solução de rede sem fio, incluindo controladora, pontos de acesso tipo 1 e tipo 2, tags ble/wifi, software de gerência e software de controle de acesso.

1.2 As especificações constantes do edital de licitação (Pregão Eletrônico n. 17/2019), do termo de referência e da proposta comercial da CONTRATADA, fazem parte deste instrumento, independentemente de transcrição.

CLÁUSULA SEGUNDA - DOS SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, MIGRAÇÃO DOS EQUIPAMENTOS, DO PLANO DE INSTALAÇÃO, DOS PRAZOS

2.1 A solução de infraestrutura de rede de comunicação de dados, composta pelos lotes 1 e 2 deverá ser instalada e devidamente configurada bem como feita a migração do atual ambiente para a novo por técnico(s) plenamente qualificado(s), devendo possuir certificação emitida pelos fabricantes dos equipamentos e softwares da solução ofertada.

2.1.1 É imprescindível a apresentação de documentação do fabricante ou outra que comprove a certificação técnica da equipe a ser alocado, juntamente com o Plano de Implantação.

2.2 Será de responsabilidade da CONTRATADA o fornecimento e instalação de todo o cabeamento de fibra ótica e/ou ethernet categoria 6, além dos previstos no Anexo I - Especificação Técnica, que seja identificado como necessário para conexão dos equipamentos ativos CORE (SPINE), topo de rack (LEAF), Switches de acesso, Switches SAN, Empilhamentos, Pontos de Acesso aos elementos do ambiente de TI do CONTRATANTE;

a) Lote 1 - Rede LAN:

a.1) aceitar que o processo de instalação e configuração dos equipamentos, peças, componentes, cabeamento e softwares seja acompanhado pela equipe técnica indicada pelo CONTRATANTE. a.2) toda instalação que envolva ativos de produção da CONTRATANTE devera obedecer a janelas de mudanças aprovadas previamente pela CONTRATANTE, evitando indisponibilidade.

b) Lote 2 - Rede Sem Fio:

b.1) aceitar que o processo de instalação e configuração dos equipamentos, peças, componentes e softwares seja acompanhado pela equipe técnica indicada pelo CONTRATANTE.

b.2) toda instalação que envolva ativos de produção da CONTRATANTE devera obedecer às janelas de mudanças, aprovadas previamente pela CONTRATANTE, evitando indisponibilidade. No caso de novos pontos de rede sem fio, toda instalação, cabeamento ativação de ponto no switch e configuração no ambiente de produção, deverá ser feito pela CONTRATADA sem ônus para o CONTRATANTE.

2.3 A Migração das configurações para os novos equipamentos devem ser realizadas pela contratada, obedecendo os itens mínimos:

2.3.1 Switch CORE H3C para SPINE-and-LEAF:

a) migrar configurações por meio de script ou manual para o novo equipamento que contemple: Roteamento de Vlans, configurações SNMP, Configurações da Vlan VOIP AVAYA, configurações referentes a VXLAN e configurações diversas adicionais que existam atualmente deverão todas serem migradas e validadas pela equipe do CONTRATANTE.

b) conectar os equipamentos de borda no Switch SPINE bem como os Switches LEAF e SAN.

2.3.2 Switch CORE e TOR para Switch LEAF e SAN:

a) configurações de Vlans, zonning, ativação dos equipamentos de rede , storage, backup, servidores rack e da solução de segurança via Gbics ou UTP além de configurações SNMP, configurações da Vlan VOIP AVAYA, configurações referentes a VXLAN e configurações diversas adicionais que existam atualmente, deverão todas serem migradas e validadas pela equipe do CONTRATANTE.

2.3.3 Switch Acesso H3C para Switch Acesso REDE CJF

a) migração das pilhas de switches dos andares para os novos equipamentos, respeitando a organização de cabeamento conforme boas práticas de cabeamento estruturado preconizadas no Anexo I - Especificação Técnica.

2.3.4 Switch Acesso H3C para Switch Acesso REDE CFTV

a) migração das pilhas de switches dos andares para os novos equipamentos, respeitando a organização de cabeamento conforme boas práticas de cabeamento estruturado preconizadas no Anexo I - Especificação Técnica.

2.3.5 Migração Controladora Wirelless H3c para solução Wifi adquirida.

a) migração das configurações atuais para nova solução WIFI, respeitando os requisitos préaprovados, em conjunto com a STI – Secretaria de Tecnologia do CONTRATANTE, com vias a manter logs de acesso, disponibilidade de customizar o portal de acesso a rede wifi, a ativação, a configuração de autenticação com nosso Active Directory(AD) e monitoramento dos equipamentos que fazem parte da solução.

b) integração por meio de agente ou certificado digital para os equipamentos que conectarem à rede WIFI.

2.3.6 Migração Access Point H3C para Ponto de Acesso da solução adquirida.

a) migração das configurações atuais para os novos equipamentos.

2.3.7 Instalação TAGS BLE/WIFI

a) instalar as 50 Tags nos dispositivos móveis corporativos do CONTRATANTE.

b) ativar, configurar e testar as Tags BLE/WIFI no software de gerenciamento das mesmas.

2.3.8 A mudança dos equipamentos antigos para os novos equipamentos da sala cofre, auditório, andares do edifício-sede do CONTRATANTE e do prédio da Seção de Serviços Gráficos, será de responsabilidade da CONTRATADA, sem ônus para o CONTRATANTE e deverá obedecer aos critérios de mudanças da CONTRATANTE, evitando indisponibilidade, quando possível.

2.4 Dos locais de prestação dos serviços

2.4.1 Todos os equipamentos e serviços objeto deste contrato deverão serem entregues e prestados no edifício-sede do CONTRATANTE e no prédio da Seção de Serviços Gráficos, respectivamente nos endereços:

a) Setor de Clubes Esportivos Sul – SCES Trecho III, Polo 8, Lote 9, Asa Sul – Brasília – DF. CEP 70200-003;

b) SAAN, Quadra 01, Lotes 10/70, Brasília - DF, prédio da Seção de Serviços Gráficos do CONTRATANTE.

2.5 Do Plano de Instalação

2.5.1 A CONTRATADA deverá apresentar um Plano de Instalação, em até 10 (dez) dias da emissão pelo CONTRATANTE, da Ordem de Serviço da etapa 2 prevista no Anexo II – Cronograma de Implantação, contendo a documentação detalhada das atividades de instalação, configuração, migração, organização do cabeamento, testes dos equipamentos e softwares e a transferência de conhecimento que compõe a solução.

2.5.2 O Plano de Instalação deverá dispor também sobre o cronograma de execução das atividades, previsão de recursos, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação,

contendo também os seguintes itens: a) detalhar informações sobre as etapas de instalação física dos equipamentos, incluindo: distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e endereçamento de gerência IP.

b) elaborar e documentar topologia lógica de rede LAN, SAN e Wifi, interligando os elementos de conectividade fornecidos aos existentes no CONTRATANTE;

c) atender a todos os tópicos previstos no item 10 do termo de referência.

d) elaborar planos de testes para os diversos componentes da solução que comprovem o funcionamento dos recursos de tolerância a falhas dos equipamentos e softwares da solução.

2.6 Dos prazos

2.6.1 A CONTRATADA deverá concluir no prazo de 90 (noventa) dias corridos, a contar da emissão da Ordem de Serviço, os serviços de instalação, configuração, migração, organização do cabeamento e transferência de conhecimento da solução conforme atividades definidas para os lotes 1 e 2, em plena compatibilidade com o ambiente computacional do CONTRATANTE, cumprindo ainda todas as demais cláusulas de garantia e suporte técnico constantes do contrato, nos prazos e termos ali estipulados.

2.6.1.1 Após o serviço de instalação ser concluído e homologado pelo CONTRATANTE, será emitido o Termo de Recebimento Definitivo - TRD da Etapa 2.

2.6.2 Após a emissão do Termo de Recebimento Definitivo - TRD da Etapa 2, a CONTRATADA deverá prestar serviço de operação assistida (on-site) por um período de 30 (trinta) dias corridos, com duração mínima de 6 (seis) horas diárias.

2.6.2.1 Os técnicos alocados para realizar o serviço de operação assistida on-site deverão ser plenamente qualificados, devendo possuir certificação emitida pelos fabricantes dos equipamentos e softwares da solução ofertada para os lotes 1 e 2.

2.6.3 Os prazos para atendimento de chamados técnicos serão interrompidos somente se ficar caracterizado que se trata de falha de laboratório (bug), sendo necessário o encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução.

2.6.4 A CONTRATADA deverá devolver, em perfeito estado de funcionamento, no prazo máximo de 30 (trinta) dias corridos, a contar da data de retirada dos equipamentos, os equipamentos que necessitem ser temporariamente retirados para conserto, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA.

2.6.5 É de responsabilidade da CONTRATADA entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até 30 (trinta) dias, a contar da data de assinatura do contrato, conforme Etapa 1 do Anexo II - Cronograma de Implantação.

CLÁUSULA TERCEIRA - DA TRANSFERÊNCIA DE CONHECIMENTO

3.1 A transferência de conhecimento da solução de infraestrutura de rede de comunicação de dados, composta pelos lotes 1 e 2 compreenderá necessariamente os seguintes tópicos:

Lote 1

a) Configuração e operação dos equipamentos, com o seguinte conteúdo mínimo:

- Apresentação da nova arquitetura LAN e SPINE-and-LEAF do CJF;
- Descrição da arquitetura de cada equipamento;
- Descrição do hardware e software disponíveis para cada equipamento;
- Estratégias de implementação dos equipamentos;
- Configuração boas práticas e administração dos equipamentos;
- Ativação e desativação de pontos físicos via CLI FC e UTP.

b) Gerenciamento dos equipamentos ativos, com o seguinte conteúdo mínimo:

- Descrição geral da plataforma de gerência;
- Gerência de configuração e de falhas;
- Funções do gerenciador;
- Diagnóstico de problemas;
- Configuração de alarmes;
- Representação gráfica da rede;
- Coleta de dados e configuração de eventos;
- Gerência de desempenho e segurança;
- Ajustes na rede;
- Personalização avançada;
- Manipulação de objetos MIB, SNMP e RMON.

Lote 2

a) Configuração e operação dos equipamentos de rede sem fio, com o seguinte conteúdo mínimo:

- Tecnologia “wireless”: conceitos e fundamentos da tecnologia;

- Arquitetura e protocolos;

- Estratégias de avaliação do ambiente (“site survey”);

- Tecnologias e mecanismos de segurança da solução;

- Operação, configuração e suporte de todas as funcionalidades oferecidas pela tecnologia wireless envolvendo todos os componentes;

- Resolução de problemas (“troubleshooting”);

- Gerenciamento de toda a solução, abrangendo todas as ferramentas a serem utilizadas.

- Trilhas de auditoria para usuários e equipamentos.

- Instalação e pareamento das TAGS BLE/WIFI além do uso do aplicativo para monitoramento dos equipamentos para equipe a ser indicada pela CONTRATANTE.

3.2 O repasse de conhecimento deverá ser realizado para até 4 (quatro) técnicos do CONTRATANTE, perfazendo um total mínimo de 20 (vinte) horas/aula para cada lote;

3.3 A transferência de conhecimento estará centrada na solução fornecida, privilegiando atividades práticas que permitam uma melhor fixação do aprendizado, bem como possibilite a equipe técnica do CONTRATANTE gerenciar a solução implantada;

3.4 O programa para a transferência de conhecimento deverá ser previamente aprovado pelo CONTRATANTE e eventuais mudanças de conteúdo solicitadas deverão constar no material didático;

3.5 O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissão da Ordem de Fornecimento na reunião de planejamento;

3.6 A CONTRATADA fornecerá, no início de cada tópico, material e apostilas em formato eletrônico que abordem todo o conteúdo programático, as quais poderão estar no todo ou em parte, em português e/ou inglês;

3.7 Deverá ser disponibilizado material didático impresso e em mídia, sem custo adicional para o CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês);

3.8 Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária;

3.9 Para todos os efeitos, inclusive de emissão do Termo de Recebimento Definitivo da etapa 2 do Anexo II - Cronograma de Implantação, a transferência de conhecimento faz parte do processo de instalação e configuração da solução;

3.10 Caso a transferência de conhecimento não seja satisfatória em relação aos aspectos carga horária, programa apresentado e estrutura de, deverá ser realizado novamente, sem ônus adicional ao CONTRATANTE.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATADA

4.1 Além das obrigações assumidas neste contrato, a CONTRATADA compromete-se a:

4.1.1 Obrigações Gerais:

a) executar e concluir as atividades previstas no contrato em estrito cumprimento aos prazos previstos no Anexo II - Cronograma de Implantação;

b) instalar, configurar, migrar, organizar o cabeamento e realizar a transferências de conhecimento nas datas e horários definidos pela equipe técnica do CONTRATANTE, que supervisionará os trabalhos;

c) entregar os equipamentos, as licenças de softwares e os respectivos componentes, às suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento da solução ofertada;

d) entregar os equipamentos devidamente protegidos e embalados contra danos de transporte e manuseio, efetuando a desembalagem dos equipamentos após a entrega nas dependências do CONTRATANTE;

e) entregar equipamentos novos e de primeiro uso, juntamente com todos os itens acessórios de hardware e dos softwares necessários à perfeita instalação e funcionamento, incluindo, mas não se limitando a: cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração, conforme especificações técnicas constantes do Anexo I – Especificação Técnica;

f) entregar, como requisito para a emissão do Termo de Recebimento Definitivo - TRD da etapa 2, a seguinte documentação:

f.1) certificado de garantia ou documento similar, comprovando que todos os equipamentos e softwares que compõe a solução estão cobertos por garantia e suporte técnico on-site, diretamente do fabricante, pelo prazo de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo - TRD da Etapa 2.

f.2) caso não seja comercializado item de garantia com o prazo nos moldes exigidos no item anterior, deverá ser entregue pela CONTRATADA declaração oficial, emitida pelo fabricante dos equipamentos, atestando a contratação do serviço de garantia e suporte técnico on-site com o nível de serviço e duração solicitados;

f.3) termo de cessões de direito de uso perpétuo dos softwares fornecidos ou documento similar. Os termos de licenciamento de todos os softwares fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão direito

pertencentes ao CONTRATANTE;

f.4) comprovante do serviço de suporte e direitos de atualização de versão ou documento similar pelo período de 60 (sessenta) meses de garantia, de todos os softwares fornecidos. Abrangerá todos os softwares e licenças a serem fornecidos na solução. Os termos de licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e comporão direito pertencente ao patrimônio do CONTRATANTE;

g) receber cópia do Termo de Recebimento Definitivo da Etapa 1, após entrega dos equipamentos, licenças de softwares e acessórios. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE;

h) receber cópia do Termo de Recebimento Definitivo - TRD da Etapa 2, que deverá ser providenciado pela CONTRATANTE no prazo máximo de 10 (dez) dias corridos, após a conclusão de todas as fases do Anexo II – Cronograma de Implantação e desde que a CONTRATADA atenda a todas as solicitações da Comissão de Recebimento e Fiscalização do CONTRATANTE;

i) garantir o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que venham a ter acesso em razão desta contratação, não podendo, sob qualquer pretexto, revelá-los, divulgá-los ou reproduzi-los;

j) fornecer manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração e operação, por meio eletrônico;

k) fornecer aos seus técnicos todos os instrumentos necessários à execução dos serviços;

l) responsabilizar-se técnica e administrativamente pelo objeto contratado, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros;

m) responder por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de seus prepostos, independentemente de outras combinações contratuais ou legais a que estiver sujeita;

n) responder pelas despesas relativas a encargos trabalhistas, de seguros de acidentes, impostos, contribuições previdenciárias e quaisquer outras que foram devidas e referentes aos serviços executados pelos seus empregados, uma vez que os mesmos não têm nenhum vínculo empregatício com o CONTRATANTE;

n.1) não cobrar valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional;

o) reparar, corrigir, remover ou substituir, às suas próprias expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções, no prazo de 10 (dez) dias corridos, contadas do recebimento da notificação em formato eletrônico emitida pelo CONTRATANTE;

p) prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CONTRATANTE, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações;

q) responsabilizar-se pelos prejuízos causados ao CONTRATANTE em virtude do descumprimento das condições fixadas;

r) cumprir todos os prazos e as condições estabelecidas neste instrumento;

s) apresentar os documentos fiscais de cobrança em conformidade com o estabelecido no contrato;

t) comunicar, formalmente, ao gestor do contrato, eventual atraso ou paralisação na execução do objeto, apresentando razões justificadoras, que serão objeto de apreciação pelo CONTRATANTE;

u) manter todas as condições de habilitação e qualificação exigidas na licitação, durante a execução do objeto do contrato, em compatibilidade com as obrigações assumidas;

v) dar ciência aos seus empregados acerca da obediência ao Código de Conduta do Conselho e da Justiça Federal de primeiro e segundo graus, nos termos da Resolução n. 147 de 15 de abril de 2011. http://www.cjf.jus.br/cjf/conheca-o-cjf/codigo-de-conduta.

4.1.2 Obrigações Quanto aos Serviços (GARANTIA):

a) tornar disponível os serviços de suporte (incluindo manutenção de hardware) durante 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia, executando-os sempre que acionada pelo CONTRATANTE, mediante a abertura de chamado técnico;

b) substituir as peças quebradas, com defeito ou gastas pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados;

c) dispor e tornar disponível ao CONTRATANTE estrutura de suporte técnico, incluindo central de suporte, técnicos, especialistas e estoque de peças de reposição, visando à prestação dos serviços de suporte e garantia durante o prazo de 60 (sessenta) meses, contados a partir da emissão do Termo de Recebimento Definitivo - TRD da Etapa 2;

d) dispor de serviço de esclarecimento de dúvidas relativas à utilização dos equipamentos e de abertura de chamado técnico por e-mail e por telefone 0800 (gratuito), ou telefone local em Brasília por todo o período de garantia dos equipamentos;

e) efetuar, sem que isso implique acréscimo aos preços contratados, a substituição de qualquer equipamento, componente ou periférico por outro novo, de primeiro uso, com características idênticas ou superiores, no prazo de 24 (vinte e quatro) horas, independente do fato de ser ou não fabricante dos equipamentos fornecidos, nos seguintes casos:

e.1) se apresentar divergência com as especificações descritas na proposta apresentada;

e.2) se no período de 15 (quinze) dias corridos, contados após a abertura do chamado técnico, ocorrerem defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de peças e componentes mecânicos ou eletrônicos.

f) iniciar o atendimento técnico em prazo não superior a 02 (duas) horas, contadas a partir da solicitação efetuada por meio de telefone ou à central de atendimento, a ser informada e-mail pela CONTRATADA.

g) realizar os atendimentos observando a classificação dos problemas reportados de acordo com seu grau de severidade, segundo a seguinte classificação:

Criticidade	**Descrição**	**Prazo máximo para início de atendimento (contados a partir da abertura do chamado)**	**Prazo máximo para restauração de serviço (contados a partir da abertura do chamado)**
Severidade 1 (Alta)	Atuação ON-SITE visando sanar problemas que tornem a solução de infraestrutura de rede inoperante, causando alto impacto nas operações de TI do CJF.	Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 6 (seis) horas
Severidade 2 (Média/Alta)	Atuação ON-SITE visando sanar problemas que prejudicam a operação normal da solução, mas não interrompem o acesso aos sistemas de TI, causando impacto no ambiente de produção ou restrição de funcionalidade.	Em até 4 (quatro) horas deve ter um técnico da CONTRATADA ON-SITE.	Em até 12 (doze) horas
Severidade 3 (Média/Baixa)	Atuação REMOTA visando sanar problemas ou dúvidas que criem restrições a operação normal da solução de infraestrutura de servidores não gerando impacto ao negócio.	Em até 4 (quatro) horas um técnico da CONTRATADA entra em contato.	Em até 24 (vinte e quatro) horas
Severidade 4 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução de infraestrutura de servidores, ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 72 (setenta e duas) horas

g.1) os equipamentos deverão operar de forma a garantir, disponibilidade e funcionalidades adequadas aos requisitos do CONTRATANTE;

h) substituir, temporária ou definitivamente, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso, quando então, a partir de seu efetivo funcionamento, ficará suspensa a contagem do prazo de reparo, nos casos em que não seja possível o reparo dentro dos prazos máximos estipulados;

i) responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste contrato ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas;

j) emitir, após concluído o atendimento a chamados técnicos, incluindo manutenção de qualquer hardware, Relatório de Serviços de Suporte onde constem informações referentes às substituições de peças (se for o caso), número e descrição do chamado técnico, data e hora da abertura do chamado e dos andamentos, data e hora do término do atendimento e descrição da solução;

k) prestar os serviços de suporte nas dependências do CONTRATANTE, no local onde os equipamentos estiverem instalados;

l) fornecer e aplicar os pacotes de correção, em data e horário a serem definidos pelo CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em microcódigo que integre o hardware objeto deste contrato;

m) comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos, fazendo constar a causa de inadequação e a ação devida para a correção;

n) o serviço de suporte técnico deverá permitir o acesso do CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos, provendo informações, assistência e orientação para:

n.1) instalação, desinstalação, configuração e atualização de imagem de firmware; aplicação de correções (patches) de firmware; diagnósticos, avaliações e resolução de problemas; características dos produtos; e demais atividades relacionadas à correta operação e funcionamento dos equipamentos;

n.2) neste serviço, as atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB e fornecidas em CD, quando desta forma forem solicitadas ou não for possível obter de outra maneira;

o) acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços.

4.1.3 Obrigações quanto ao suporte às licenças dos softwares:

a) atualizar, durante o período de vigência do contrato, as licenças de softwares colocados à disposição do CONTRATANTE, imediatamente, sem que isso implique acréscimo aos preços contratados, em relação às novos versões e releases lançados pelo fabricante, as respectivas mídias de instalação, os manuais técnicos originais e os documentos comprobatórios do licenciamento.;

b) prestar o serviço de suporte remoto para as licenças de software fornecidas, sempre que houver chamado técnico do CONTRATANTE, durante o período de vigência do contrato, proporcionando toda a orientação técnica requerida para a resolução de problemas, esclarecimento de dúvidas e orientação com relação aos produtos;

c) atender às demandas da CONTRATANTE para atualização de licenças de software adquirido, fornecendo as mídias de instalação e manuais para as novas versões e releases do produto, bem como alocar pessoal técnico para realizar a atualização dos sistemas de forma remota quando necessário, durante todo o período de vigência do contrato;

d) comunicar formalmente ao CONTRATANTE, durante o período de garantia de funcionamento dos produtos, a disponibilidade de novas versões e releases das licenças de software, reservando-se, o CONTRATANTE, o direito de exigir a atualização dos mesmos, sem que isso implique acréscimo aos preços contratados;

e) permitir ao CONTRATANTE a possibilidade de realizar a aplicação de pacotes de correção e migração de versões e releases das licenças de software, quando lhe for conveniente, cabendo à CONTRATADA orientar e colocar à disposição um técnico para contato por meio telefônico, em caso de dúvidas ou falhas;

f) caso haja necessidade, a CONTRATADA poderá solicitar atendimento on-site para atualizações de licenças de software e/ou firmware da solução.

g) tornar disponível o suporte técnico às licenças de software durante 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia;

g.1) os prazos para atendimento de chamados técnicos serão interrompidos somente se ficar caracterizado que se trata de falha de laboratório (bug), sendo necessário o encaminhamento da falha ao laboratório do fabricante e acompanhamento de sua solução.

CLÁUSULA QUINTA - DAS OBRIGAÇÕES DO CONTRATANTE

5.1 O CONTRATANTE se compromete a dar plena e fiel execução ao presente contrato, respeitando todas as condições estabelecidas, obrigando-se ainda a:

a) permitir o acesso dos empregados da CONTRATADA, devidamente identificados, nas suas dependências, para a entrega dos equipamentos e materiais, nos horários estabelecidos;

b) dar providências às recomendações da CONTRATADA concernentes às condições e ao uso correto dos equipamentos e materiais;

c) efetuar, no prazo estabelecido neste instrumento, o pagamento do objeto contratado;

d) receber a comunicação de defeito realizada pelos usuários e, se for o caso, encaminhar o chamado à CONTRATADA;

e) manter atualizados os registros dos equipamentos em manutenção;

f) relatar, por escrito, com a devida comprovação, as eventuais irregularidades na prestação do serviço;

g) sustar a execução de quaisquer trabalhos por estarem em desacordo com o especificado ou por qualquer outro motivo que caracterizem a necessidade de tal medida;

h) acompanhar e fiscalizar, sempre que entender necessário, os técnicos da CONTRATADA em suas visitas;

i) zelar pela segurança dos softwares e dos equipamentos, evitando o manuseio por pessoas não habilitadas.

CLÁUSULA SEXTA - DAS GLOSAS PELOS NÍVEIS DE QUALIDADE DO SERVIÇO DE SUPORTE TÉCNICO

6.1 O não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico, independentemente das Sanções Administrativas previstas no Contrato, implicará em redutor na fatura mensal do serviço de suporte técnico (glosa), nos seguintes casos:

6.1.1 glosa de 5% (cinco por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com severidade alta, limitada até 06 (seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

6.1.2 glosa de 3% (três por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com severidade média/alta, limitada até 12 (doze) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

6.1.3 glosa de 2% (dois por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com severidade média/baixa, limitada até 18 (dezoito) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

6.1.4 glosa de 1% (dois por cento), calculada sobre o valor do serviço de suporte técnico do componente da solução afetado, para cada hora de atraso, pela não resolução dos chamados com severidade baixa, limitada até 36 (trinta e seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

6.2 Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas previstas, a cada ocorrência a CONTRATADA receberá uma Sanção de Advertência, a ser aplicada pelo CONTRATANTE.

6.3. A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços.

6.4 No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses, serão aplicadas as Sanções Administrativas previstas no contrato.

6.5 No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa.

6.6 Se a decisão da Administração for favorável ao recurso da CONTRATADA, deverá ser emitida nota fiscal adicional para que seja efetuado o pagamento referente ao valor glosado.

6.6.1 A nota fiscal deverá ser atestada pelo gestor do contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

CLÁUSULA SÉTIMA - DO RECEBIMENTO

7.1 O recebimento e a aceitação obedecerão ao disposto nos arts. 73 a 76 da Lei n. 8.666/1993.

7.2 Caso o CONTRATANTE constate que os serviços foram prestados em desacordo com o contrato, com defeito, fora de especificação ou incompletos, a CONTRATADA será formalmente notificada, sendo interrompidos os prazos de recebimento, e os pagamentos suspensos, até que a situação seja sanada.

7.3 O recebimento definitivo não exclui a responsabilidade civil da CONTRATADA pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou por este instrumento.

CLÁUSULA OITAVA - DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

8.1 O CONTRATANTE designará, na forma da Lei n. 8.666/1993, art. 67, um servidor com autoridade para exercer, como seu representante, toda e qualquer ação de orientação geral, acompanhamento e fiscalização da execução contratual.

8.1.1 O servidor designado atuará orientando, fiscalizando e intervindo no interesse do CONTRATANTE, a fim de garantir o exato cumprimento das cláusulas e condições contratuais, promovendo a aferição qualitativa e quantitativa dos serviços prestados, sem prejuízo da fiscalização exercida pela CONTRATADA.

8.2 O CONTRATANTE reserva-se o direito de - sem que, de qualquer forma, restrinja a plenitude da responsabilidade da CONTRATADA - exercer a mais ampla e completa fiscalização sobre os serviços, diretamente ou por preposto designado.

8.3 A existência e a atuação da fiscalização pelo CONTRATANTE em nada restringem a responsabilidade única, integral e exclusiva da CONTRATADA, no que concerne à execução do objeto contratado.

CLÁUSULA NONA – DA VIGÊNCIA

9.1 A vigência do contrato deverá ser de:

a) **6 (seis) meses**, contados da assinatura do contrato para a conclusão das etapas:

Etapa I - Entrega pela CONTRATADA dos equipamentos e softwares adquiridos;

Etapa II - Conclusão pela CONTRATADA dos serviços de instalação, configuração, migração, organização do cabeamento e transferência de conhecimento;

b) **60 (sessenta) meses** contados da data de **emissão do Termo de Recebimento Definitivo** (TRD) da Etapa 2, referente à garantia e suporte técnico dos equipamentos e softwares adquiridos.

CLÁUSULA DÉCIMA – DO VALOR

10.1 O valor total contratado fica estimado em **R$ 3.088.459,07 (três milhões, oitenta e oito mil, quatrocentos e cinquenta e nove reais e sete centavos)**, conforme especificado no Anexo III - Planilha de Preços.

10.2 Os valores estabelecidos nesta cláusula incluem todos os tributos, contribuições fiscais e parafiscais previstos na legislação em vigor, incidentes direta ou indiretamente, bem como as despesas de quaisquer naturezas decorrentes da execução do contrato, sendo os valores fixos e irreajustáveis.

10.3 O CONTRATANTE poderá promover alterações contratuais, observada as limitações constantes na Lei n. 8.666/1993, art. 65, §1º.

CLÁUSULA DÉCIMA PRIMEIRA – DA DOTAÇÃO ORÇAMENTÁRIA

11.1 As despesas com a execução correrão à conta de recursos orçamentários da União destinados ao CONTRATANTE, consignados no Programa de Trabalho Resumido - PTRES: 085322, Natureza de Despesa - ND: 449052, 449040 e 339030, Nota de Empenho n.os 2019NE000588, 2019NE000589 e 2019NE000590.

CLÁUSULA DÉCIMA SEGUNDA – DO PAGAMENTO

12.1 O pagamento será efetuado, por ordem bancária, mediante a apresentação de nota fiscal eletrônica emitida com número raiz do CNPJ qualificado no preâmbulo, conforme a seguir:

12.1.1 O pagamento referente aos serviços de suporte técnico por 60 (sessenta) meses será realizado mensalmente, já descontadas as glosas eventualmente aplicadas em função do não atendimento dos níveis de qualidade definidos no contrato, determinando o valor total do serviço para o mês, iniciando quando da emissão do Termo de Recebimento Definitivo - TRD da Etapa 2, conforme previsto no Anexo II Cronograma de Implantação.

12.1.2 Os pagamentos referentes aos equipamentos e softwares incluindo a garantia, bem como os serviços de instalação (instalação, configuração, migração e organização do cabeamento), bem como a transferência de conhecimento da solução serão realizados em única parcela.

12.2 As notas fiscais deverão ser encaminhadas ao gestor do contrato pelo e-mail: sesinf@cjf.jus.br ou sutec@cjf.jus.br .

12.2.1 A CONTRATADA deverá emitir as notas fiscais relativas aos valores dos equipamentos e softwares incluindo a garantia, após receber cópia do Termo de Recebimento Definitivo - TRD da Etapa 1, conforme previsto no Anexo II Cronograma de Implantação.

12.2.2 A CONTRATADA deverá emitir a nota fiscal relativa ao valor dos serviços de instalação (instalação, configuração, migração e organização do cabeamento), bem como a transferência de conhecimento da solução após receber cópia do Termo de Recebimento Definitivo – TRD da Etapa 2, conforme previsto no Anexo II Cronograma de Implantação.

12.2.3 No corpo da nota fiscal deverá ser especificado o serviço fornecido, o número do contrato e o período de fornecimento.

12.3 A nota fiscal emitida pela CONTRATADA deverá ser atestada pelo gestor do contrato em até 10 (dez) dias, contados do recebimento definitivo e, encaminhada à área financeira, que efetuará o pagamento no prazo de 10 (dez) dias úteis, contados do atesto.

12.3.1 Esse prazo pode ser estendido nos termos da alínea a do inciso XIV do art. 40 da Lei n. 8.666/1993).

12.4 Deverá ser apresentada, concomitante à nota fiscal, a seguinte documentação:

a) Certificado de Regularidade do FGTS - CRF, comprovando regularidade com o FGTS;

b) Certidão Conjunta Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal;

c) Certidão Negativa de Débitos Trabalhistas - CNDT, expedida pela Justiça do Trabalho;

d) Prova de regularidade com as Fazendas Estadual e Municipal do domicílio ou sede da CONTRATADA.

12.5 Dos valores a serem pagos à CONTRATADA, serão abatidos, na fonte, os tributos federais, estaduais e municipais, na forma da lei.

12.5.1 Caso a CONTRATADA goze de algum benefício fiscal, deverá, juntamente com a nota fiscal, encaminhar documentação hábil, ou, no caso de optante pelo Simples Nacional deverá apresentar declaração relativa à sua opção por tal regime tributário.

12.6 Poderá o CONTRATANTE, após efetuar a análise das notas fiscais, realizar glosas dos valores cobrados indevidamente. Neste caso, a CONTRATADA será informada das razões que motivaram a recusa dos valores.

12.6.1 A CONTRATADA poderá apresentar impugnação à glosa, no prazo de 3 (três) dias úteis, contados da data do recebimento da notificação.

12.6.2 Caso a CONTRATADA não apresente a impugnação, ou caso o CONTRATANTE não acolha as razões da impugnação, o valor será deduzido da respectiva nota fiscal.

12.7 O prazo de pagamento será interrompido nos casos em que haja necessidade de regularização do documento fiscal, o que será devidamente apontado pelo CONTRATANTE.

12.7.1 A contagem do prazo previsto para pagamento será iniciada a partir da respectiva regularização.

12.8 Nenhum pagamento será efetuado enquanto pendente o cumprimento de qualquer obrigação imposta à CONTRATADA, inclusive em virtude de penalidade ou inadimplência.

12.9 O depósito bancário produzirá os efeitos jurídicos da quitação da prestação devida.

CLÁUSULA DÉCIMA TERCEIRA - DA ATUALIZAÇÃO MONETÁRIA

13.1 No caso de eventual atraso no pagamento e, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, haverá incidência de atualização monetária, sobre o valor devido, pro rata temporis, ocorrida entre a data limite estipulada

para pagamento e a da efetiva realização.

13.1.1 Para esse fim, será utilizada a variação acumulada do Índice Nacional de Preços ao Consumidor Amplo/IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE.

13.2 O mesmo critério de correção será adotado em relação à devolução dos valores recebidos indevidamente pela CONTRATADA.

CLÁUSULA DÉCIMA QUARTA - DAS PENALIDADES

14.1 Pela inexecução total ou parcial das obrigações assumidas a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as seguintes sanções:

14.1.1 Advertência.

14.1.2 Multa no percentual correspondente a 0,1% (um décimo por cento), calculada sobre o valor total da contratação, **por dia de atraso na entrega de todos os equipamentos, softwares e acessórios da solução**, além do prazo máximo definido no Anexo II – Cronograma de Implantação, até o limite de 30 (trinta) dias corridos, caracterizando inexecução total do contrato.

14.1.3 Multa no percentual correspondente a 0,5% (zero vírgula cinco por cento), calculada sobre o valor total do serviço de instalação, **por dia de atraso na entrega do Plano de Instalação**, além do prazo máximo definido no Anexo II - Cronograma de Implantação, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

14.1.4 Multa no percentual correspondente a 0,5% (zero vírgula cinco por cento), calculada sobre o valor total do serviço de instalação, **por dia de atraso na conclusão da etapa de instalação e configuração da solução**, além dos prazos máximos definidos no Anexo II - Cronograma de Implantação, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

14.1.5 Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total do serviço de instalação, **por dia de atraso na conclusão da etapa de instalação e configuração da solução**, além dos prazos máximos definidos no Anexo II - Cronograma de Implantação), até o limite de 30 (trinta) dias corridos, caracterizando inexecução total do contrato.

14.1.6 Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total do serviço de transferência de conhecimento, **por dia de atraso na conclusão do serviço de transferência de conhecimento**, além do prazo máximo definido no Anexo II - Cronograma de Implantação, até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

14.1.7 Multa no percentual correspondente a 1% (um por cento), calculada sobre o valor total da contratação, **no caso de aplicação de glosa referente ao mesmo indicador de nível mínimo de serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses**, caracterizando inexecução parcial do contrato.

14.2 A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da multa, no percentual de 20% (vinte por cento) sobre o valor da parte não entregue ou não executada.

14.3 Multa no valor de 5% (cinco por cento), sobre o valor total da contratação, **no caso de inexecução total do contrato**.

14.4 O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos artigos 87 e 88 da Lei n. 8.666/1993.

14.5 Suspensão temporária;

14.6 Declaração de inidoneidade.

14.7 Nos termos da Lei n. 10.520/2002, art. 7º, o CONTRATANTE poderá aplicar impedimento de licitar àquele que:

Ocorrência	Pena
a) fizer declaração falsa ou apresentar documentação falsa:	Impedimento do direito de licitar e contratar com a União e descredenciamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, pelo período de 24 (vinte e quatro) meses;
b) falhar na execução da contrato:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 12 (doze) meses;
c) fraudar na execução do contrato:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 30 (trinta) meses;
d) comportar-se de modo inidôneo:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 24 (vinte e quatro) meses;
e) cometer fraude fiscal:	Impedimento do direito de licitar e contratar com a União e descredenciamento do SICAF pelo período de 40 (quarenta) meses;

14.7.1 O CONTRATANTE, para aplicação da penalidade prevista no item

14.7, adotará os critérios previstos na Instrução Normativa n. 1, de 13/10/2017, da Presidência da República, publicada no DOU, em 16/10/2017 (n. 198, Seção 1, pág. 5).

14.8 A critério da autoridade competente do CONTRATANTE, com fundamento nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser relevadas ou atenuadas, em razão de circunstâncias fundamentadas, mediante comprovação dos fatos e, desde que formuladas por escrito, no prazo máximo de 5 (cinco) dias úteis, contados da data da notificação.

14.9 A aplicação das sanções previstas nesta cláusula será realizada mediante processo administrativo específico, mediante comunicação à CONTRATADA da penalidade, sendo assegurado, em todos os casos, o contraditório e a ampla defesa, no prazo de 5 (cinco) dias, contados do recebimento da comunicação.

14.10 Em caso de aplicação de multa, o valor poderá ser descontado da garantia prestada, dos pagamentos eventualmente devidos à CONTRATADA, ser recolhido ao Tesouro por meio Guia de Recolhimento da União - GRU, ou cobrado judicialmente, nos termos do § 3º do art. 86 da Lei n. 8.666/1993.

14.11 O atraso no recolhimento de multas será corrigido monetariamente pela variação acumulada do Índice Nacional de Preços ao Consumidor Amplo/IPCA, calculado e divulgado pelo Instituto Brasileiro de Geografia e Estatística/IBGE.

14.12 O CONTRATANTE promoverá o registro no Sistema de Cadastramento Unificado de Fornecedores - SICAF de toda e qualquer penalidade imposta à CONTRATADA.

CLÁUSULA DÉCIMA QUINTA - DA GARANTIA CONTRATUAL

15.1 A CONTRATADA apresentará, nos termos do art. 56 da Lei n. 8.666/1993, em até 20 (vinte) dias úteis, contados da assinatura deste instrumento, garantia de execução do contrato no valor de **R$ 154.422,95 (cento e cinquenta e quatro mil, quatrocentos e vinte e dois reais e noventa e cinco centavos)**, correspondente a 5% (cinco por cento) do valor total estimado da contratação, tendo como beneficiário o CONTRATANTE.

15.1.1 A CONTRATADA, caso opte pela modalidade de garantia caução, declara que manterá conta de caução específica para o depósito de valores oferecidos em garantia/caução referentes exclusivamente a contratos firmados com o CONTRATANTE.

15.1.2 No caso de a CONTRATADA optar pela caução em dinheiro, esta deverá ser feita na Caixa Econômica Federal, conforme Decreto-lei n. 1.737, de 21/12/1979.

15.2 A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do contrato;

b) prejuízos diretos causados ao CONTRATANTE, decorrentes de culpa ou dolo durante a execução do contrato;

c) multas moratórias e punitivas aplicadas à CONTRATADA;

d) obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber;

15.3 Caso o valor da garantia venha a ser utilizado em pagamento de qualquer obrigação atribuída à CONTRATADA, esta se obriga a efetuar a respectiva reposição no prazo máximo de 10 (dez) dias úteis, a contar da data do recebimento da comunicação pelo CONTRATANTE.

15.4 A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expirar o vencimento, alteração por aumento no valor do Contrato ou outra necessidade indispensável, em até 20 (vinte) dias úteis, contados da data de assinatura do respectivo instrumento contratual.

15.5 A garantia apresentada em desacordo com os requisitos e coberturas previstos neste instrumento será devolvida à CONTRATADA, que disporá do prazo improrrogável de 10 (dez) dias úteis para a regularização da pendência.

15.6 O CONTRATANTE poderá executar a garantia para ressarcimento dos valores que a CONTRATADA passe a lhe dever em virtude da ocorrência de qualquer das situações expressamente previstas neste contrato e na legislação pertinente, após a instauração de procedimento administrativo específico.

15.7 Na ocorrência de qualquer inadimplemento das obrigações contratadas, o CONTRATANTE notificará a empresa seguradora da expectativa de sinistro com vistas a resguardar a administração de possíveis prejuízos, mediante provocação da unidade gestora responsável pelo acompanhamento da execução contratual, durante a vigência da apólice.

15.8 A garantia deverá ser prestada com validade de 3 (três) meses após o término da vigência do contrato e será liberada ante a comprovação do adimplemento total das obrigações contratuais.

15.9 O termo da garantia será restituído à CONTRATADA após o cumprimento integral de todas as obrigações contratuais.

CLÁUSULA DÉCIMA SEXTA - DA RESCISÃO

16.1 Este contrato poderá ser rescindido a juízo do CONTRATANTE, com base nos arts. 77 a 80 da Lei n. 8.666/1993, especialmente quando entender que a CONTRATADA não está cumprindo de forma satisfatória as avenças estabelecidas, independentemente da aplicação das penalidades estabelecidas.

CLÁUSULA DÉCIMA SÉTIMA - DA PUBLICAÇÃO

17.1 Em conformidade com o disposto na Lei n. 8.666/1993, art. 61, parágrafo único, o contrato será publicado no Diário Oficial da União, em forma de extrato.

CLÁUSULA DÉCIMA OITAVA - DO DESENVOLVIMENTO NACIONAL SUSTENTÁVEL

18.1 Os equipamentos e peças fornecidos não deverão conter substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenilpolibromados (PBDEs) em concentração acima da recomendada pela diretiva da Comunidade Econômica Europeia Restriction of Certain Hazardous Substances - RoHS (Restriction of Certain Hazardous Substances).

18.2 Considerando que a indústria de material elétrico, eletrônico e comunicações se enquadra entre as atividades potencialmente poluidoras ou utilizadoras de recursos ambientais listadas no Anexo I da Instrução Normativa Ibama n. 6 de 15 de março de 2013, sujeitando a fabricante ao devido registro no Cadastro Técnico Federal.

18.3 A CONTRATADA deverá realizar o recolhimento de todos os componentes eletroeletrônicos substituídos nos equipamentos, responsabilizando-se pelo tratamento/descarte desses materiais/resíduos, para fins de devolução ao fabricante ou importador, responsáveis pela sua destinação final ambientalmente adequada, conforme normas e regras dos institutos ambientais e legislações vigentes no País, em especial a Lei n. 12.305/2010, que institui a Política Nacional de Resíduos Sólidos, regulamentada pelo Decreto n. 7.404/2010.

CLÁUSULA DÉCIMA NONA - DO FORO

19.1 Para dirimir quaisquer conflitos oriundos deste contrato, é competente o foro do Juízo da Seção Judiciária do Distrito Federal, com expressa renúncia a qualquer outro, por mais privilegiado que seja, no que se refere a qualquer ação ou medida judicial originada ou referente ao instrumento contratual.

CLÁUSULA VIGÉSIMA - DAS DISPOSIÇÕES FINAIS

20.1 As partes contratantes ficarão exoneradas do cumprimento das obrigações assumidas neste instrumento, quando ocorrerem motivos de força maior ou caso fortuito, assim definidos no parágrafo único do art. 393 do Código Civil.

20.2 Os casos omissos serão resolvidos à luz das disposições contidas na Lei n. 8.666/1993, bem como dos princípios de direito público.

20.3 É defeso à CONTRATADA utilizar-se deste contrato para caucionar qualquer dívida ou títulos por ela emitidos, seja qual for a natureza.

20.4 A CONTRATADA assumirá, de forma exclusiva, todas as dívidas que venha a contrair com vistas ao cumprimento das obrigações oriundas deste contrato, ficando certo, desde já, que o CONTRATANTE não será responsável solidário.

20.5 A documentação necessária para pagamento, pedido de prorrogação de prazo, recursos, defesa prévia e outros inerentes à contratação deverão ser encaminhados diretamente ao gestor do contrato pelos e-mails: sesinf@cjf.jus.br ou sutec@cjf.jus.br .

20.5.1 Alterações nos e-mails apresentados no item anterior, serão comunicados, por escrito, pelo gestor, não acarretando a necessidade de alteração contratual.

E por estarem assim de pleno acordo, assinam as partes este instrumento, na forma eletrônica, para todos os fins de direito.

JUÍZA FEDERAL SIMONE DOS SANTOS LEMOS FERNANDES

Secretária-Geral do Conselho da Justiça Federal

FREDERICO SAMARTINI QUEIROZ ALVES

Diretor Presidente da empresa Mtel Solução S.A

GABRIELLY ANDRESSA NAGY

Diretora de Contabilidade e Controladoria da empresa Mtel Solução S.A

/

/

/

/

ANEXO I - ESPECIFICAÇÃO TÉCNICA

1.0 TOPOLOGIA DE REFERÊNCIA

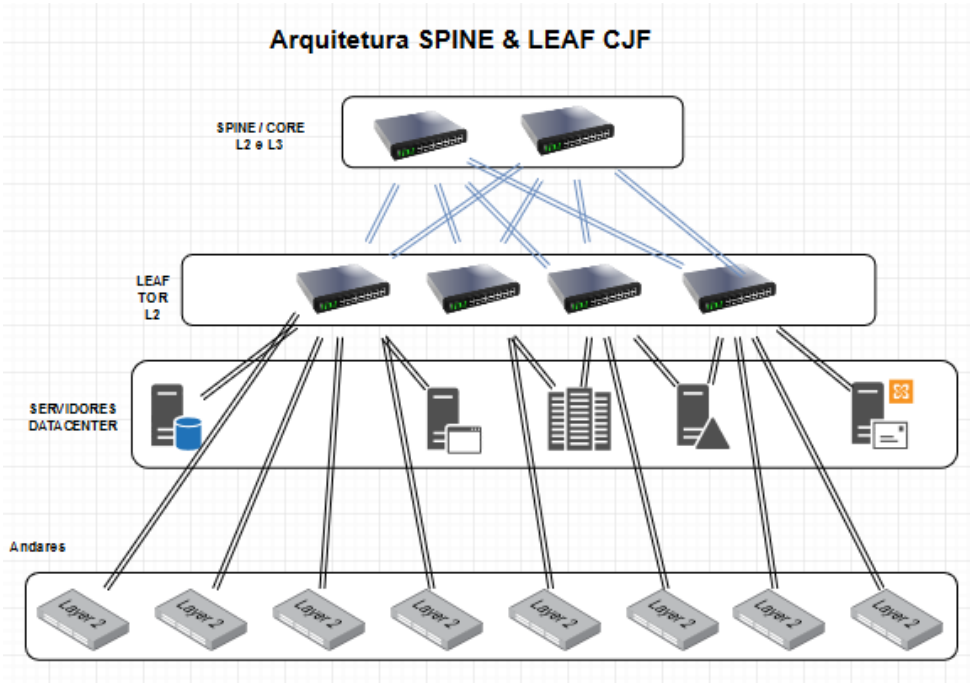

Figura 1 - Arquitetura Spine-Leaf CJF

1.1 A solução a ser fornecida no Lote 1 deverá para prover uma arquitetura de rede de datacenter (fabric de rede de datacenter) que também funcione como LAN, em topologia de duas camadas de switches físicos denominados SPINE e LEAF.

1.2 A solução SPINE and LEAF deverá também atender aos uplinks dos SWITCHES DE ACESSO através de dois links redundantes ativos em camada 2 (LACP), sendo cada link conectado em LEAFs distintos.

1.3 A solução deverá prover gateway VXLAN conforme arquitetura NSX da VMware. Deverá ser comprovada a compatibilidade com o NSX da VMware.

1.4 Os switches LEAF devem ser equipamentos com baixas latências, responsáveis pelas conexões de diferentes tipos de endpoints (servidores, roteadores, firewalls, balanceadores de carga e similares).

1.5 Deve implementar mecanismos de segurança para evitar a entrada de equipamentos e/ou controladores sem autorização no FABRIC;

1.6 A solução deve prover a abstração da rede física (UNDERLAY NETWORK) em uma rede virtual (OVERLAY NETWORK), utilizando o protocolo Virtual eXtensible Local Area Network (VXLAN).

1.7 Camada de Plano de Controle (“underlay network”) com, no mínimo, as seguintes características:

1. Baseada em protocolo IP (camada 3 do modelo OSI).
2. Que permita a criação de uma topologia full-mesh sem loops e sem utilização do protocolo Spanning-Tree.
3. Com balanceamento de tráfego baseado em ECMP (“equal-cost multipath”).

1.8 A proposta de fornecimento do LOTE 1 deverá contemplar todos os componentes, incluindo switches, transceivers, licenças, módulos, acessórios, conectores, cabos e adaptadores, bem como qualquer outro elemento de hardware ou software adicionais, de forma a atender plenamente os seguintes requisitos:

1. CAMADA SPINE.
2. CAMADA LEAF.
3. CAMADA ACESSO LAN.
4. REDE SAN.
5. RACK DE REDE.
6. SOLUÇÃO DE GERENCIAMENTO DE REDES.
7. SERVIÇOS DE INSTALAÇÃO E ORGANIZAÇÃO DO CABEAMENTO DE REDE.

2. SWITCH DE ACESSO – TIPO 1

Deverão ser fornecidos switches, a serem agrupados em, no mínimo, 7 (sete) pilhas, distribuídas nos andares do Edifício Sede do CJF e na sua unidade gráfica no SAAN, compondo a camada de acesso da rede local.

Os switches a serem fornecidos deverão atender integralmente aos seguintes requisitos:

2.1 QUANTIDADE DE INTERFACES E TRANSCEIVERS

2.2 Cada switch deverá possuir:

2.2.3 48 (quarenta e oito) portas 10/100/1000, suportando o padrão 802.3af (15,4W PoE) e 802.3at (30W PoE+) em todas portas com, pelo menos, 720W disponíveis para PoE/PoE+, sendo 15,4W para 48 portas simultaneamente ou 30W em 24 (vinte e quatro) portas simultaneamente.

2.2.4 4 (quatro) portas SFP+, além das 48 portas UTP solicitadas anteriormente.

2.3 As portas SFP+ devem suportar transceivers dos padrões SFP+ 10GBase-SR e 10GBase-LR.

2.4 Deverão ser fornecidos 28 (vinte e oito) transceivers do tipo SFP+, padrão 10Base-SR para fibra óptica multimodo com conectores tipo LC, para conexão com os switches LEAF, permitindo a implementação de, pelo menos, 7 (sete) pilhas de switches.

2.5 REQUISITOS DE CAPACIDADE

2.6 Deve possuir capacidade de encaminhamento de, no mínimo,100 Mpps (cem milhões de pacotes por segundo).

2.7 Deve possuir capacidade de comutação de, no mínimo, 160 Gbps (cento e sessenta gigabit por segundo).

2.8 A fonte interna do switch deve disponibilizar 720W de potência para alimentação do conjunto de portas PoE+.

2.9 Deve implementar a tecnologia de empilhamento ou agregação com outra unidade switch de mesmo fabricante e modelo, com, no mínimo 8 (oito) switches, tornando esse empilhamento uma única unidade de encaminhamento L3 e L2 ininterrupto e gerenciamento de múltiplos dispositivos por um único IP.

2.10 O empilhamento dos switches deverá ser feito através de, pelo menos, 2 (duas) portas, podendo ser utilizadas interfaces SFP+ ou portas e módulos dedicados para empilhamento. Deverão ser fornecidos todos os cabos necessários para o empilhamento.

2.11 Deve possuir buffers de, no mínimo, 4 MB de memória DRAM ou SDRAM.

2.12 Deve possuir memória RAM de, no mínimo, 512 MB de memória DRAM ou SDRAM.

2.13 Deve suportar 32.000 endereços MAC.

2.14 Deve implementar 1.000 VLANs simultaneamente.

2.15 Deve suportar agregação de link através de LACP com suporte a 60 grupos distribuídos através da pilha, com cada grupo permitindo até 8 portas.

2.16 Deve possuir tabela de roteamento com 2.000 rotas IPv4 e 1.000 rotas IPv6.

2.17 Deve possuir latência máxima de 4 μs, considerando pacotes de 64 bytes.

2.18 Deve possuir interface de Console Serial.

2.19 Deve possui, no mínimo, 1 (uma) porta para gerenciamento out-of-band com conector RJ-45.

2.20 Deverá operar nas temperaturas de 0 a 40 °C.

2.21 Deve possuir fontes de alimentação redundantes. A falha de uma das fontes não deve impactar no funcionamento de nenhum switch da pilha, inclusive na potência das portas PoE+.

2.22 REQUISITOS FUNCIONAIS

2.23 Compatível com protocolo 802.1X, Autenticação MAC, AAA, TACACS+ (ou similar) ou RADIUS e RPVST+.

2.24 Os switches de acesso deverão ser conectados por meio de dois links redundantes ativos em camada 2 (LACP), sendo cada link conectado em LEAFs distintos.

2.25 Deve suportar espelhamento de porta baseado em fluxo.

2.26 Deve armazenar imagem de firmware com no mínimo duas versões.

2.27 O conjunto deve atuar como uma única entidade lógica e gerenciável.

2.28 Deve implementar Jumbo Frames de até 9000 bytes em todas as portas.

2.29 Todos os switches membros da pilha devem ser do mesmo modelo e devem possuir a mesma configuração.

2.30 O equipamento deve ser novo, sem uso anterior e o modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta, não sendo aceita solução em roadmap.

2.31 Deve ser fornecido com a versão mais recente (última versão comercial disponível) do software interno instalado.

2.32 O equipamento deve ser do mesmo fabricante dos demais equipamentos da solução, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

2.33 Deve implementar IEEE 802.3az para as portas 10/100/1000.

2.34 Deve suportar a agregação de links entre diferentes membros da pilha.

2.35 Deve implementar funcionalidade que permita a detecção de links unidirecionais.

2.36 Deve implementar funcionalidade que permita a detecção de falhas de uplink.

2.37 Deve implementar MVRP (Multiple VLAN Registration Protocol) ou similar.

2.38 Deve implementar LLDP (IEEE 802.1ab).

2.39 Deve implementar LLDP-MED.

2.40 Deve implementar Q-in-Q (IEEE 802.1ad).

2.41 Deve implementar PVST+, RPVST+ ou protocolo compatível.

2.42 Deve implementar MSTP (IEEE 802.1s).

2.43 Deve implementar roteamento estático.

2.44 Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2).

2.45 Deve implementar RIPng.

2.46 Deve implementar Policy-based Routing.

2.47 Deve implementar VRRP.

2.48 Deve implementar VRRPv3.

2.49 Deve implementar roteamento baseado em políticas (PBR).

2.50 Deve implementar servidor DHCP.

2.51 Deve implementar DHCP snooping (IPv4 e IPv6).

2.52 Deve implementar DHCP relay (IPv4 e IPv6).

2.53 Deve implementar PIM-SM.

2.54 Deve implementar MLD snooping.

2.55 Deve implementar IGMP v3.

2.56 Deve implementar controle de broadcast.

2.57 Deve implementar rate limiting para tráfego broadcast e multicast.

2.58 Deve implementar rate limiting baseado em tráfego classificado por uma ACL.

2.59 Deve suportar espelhamento de portas.

2.60 Deve suportar espelhamento de tráfego para um switch remoto.

2.61 Deve implementar controle de acesso baseado em perfis (Role Based Access Control).

2.62 Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua).

2.63 Deve implementar autenticação baseada em web.

2.64 Deve implementar autenticação baseada em endereço MAC.

2.65 Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta.

2.66 Deve implementar TACACS+ ou similar.

2.67 Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas.

2.68 Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos.

2.69 Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows e Linux.

2.70 Deve implementar NTP com autenticação MD5.

2.71 Deve implementar Time Domain Reflectometry (TDR) ou similar, para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo.

2.72 Deve suportar duas imagens de software na flash.

2.73 Deve suportar múltiplos arquivos de configuração na flash.

2.74 Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos.

2.75 Deve implementar sFlow (IPv4 e IPv6) ou Netflow ou similar sem a necessidade de probes externas.

2.76 Deve possuir interface web para configuração.

2.77 Deve implementar SNMP v1/v2/v3.

2.78 Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como, debug, trace e log de eventos.

2.79 Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável), Jitter UDP e Jitter UDP para voz.

2.80 Deve implementar QoS (Quality of Service) nas seguintes funcionalidades: IEEE 802.1p, CoS, DSCP e Rate Limit.

2.81 Deve ter estrutura adequada para instalação em rack padrão EIA 19 polegadas e vir acompanhado de 1 (um) conjunto (kit) para montagem em rack de 19 polegadas.

2.82 Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento, permitindo que os equipamentos continuem operacionais com todas as funcionalidades descritas neste objeto, mesmo após o término do período de suporte ou garantia.

3. SWITCH LEAF - TIPO 2

Deverão ser fornecidos switches a serem instalados no Datacenter do CJF, compondo a camada LEAF.

Os switches a serem fornecidos deverão atender integralmente aos seguintes requisitos:

3.1 O equipamento deve ser específico para o ambiente de Datacenter, com capacidade de operação em camada 3 do modelo OSI, de baixa latência, com comutação de pacotes de alto desempenho arquitetura “non blocking”.

3.2 Instalável em rack padrão de 19”, ocupando no máximo 1 (uma) unidade de rack (RU), devendo ser fornecidos os respectivos acessórios de fixação.

3.3 Suportar a funcionalidade de “Leaf”, na arquitetura “Spine-and-Leaf”.

3.4 QUANTIDADE DE INTERFACES E TRANSCEIVERS

3.5 Cada switch deverá possuir:

3.5.1 48 (quarenta e oito) portas Ethernet SFP+ sem bloqueio (non-blocking), totalmente licenciadas.

3.5.2 4 (quatro) portas Ethernet QSFP28, sem bloqueio (non-blocking), totalmente licenciadas.

3.6 As portas SFP+ devem suportar transceivers dos padrões 10GBase-SR e 10GBase-LR, 1000Base-SX, 1000Base-LX e 1000Base-T, compatíveis com cabos SFP+ Direct Attach Cable (DAC) ou Twinax.

3.7 As portas QSFP+ devem suportar transceivers nos padrões 40GBASE-LR4 e 40GBASE-SR4.

3.8 Cada switch deverá ser fornecido com:

3.8.1 32 (trinta e dois) transceivers do tipo SFP+, 10GbE-SR para Fibra Óptica MultiModo, 850nm/50µ, OM3 ou OM4, com alcance de até 300m, em conectores tipo LC.

3.8.2 12 (doze) cabos do SFP+ to SFP+ (10Gbps), com comprimento de, no mínimo 5 (cinco) metros, do tipo DAC (Direct Attach Copper Cable) para conexão de servidores.

3.8.3 4 (quatro) transceivers do tipo SFP, 1000Base-T.

3.8.4 2 (dois) transceivers do tipo QSFP+, 40Base-SR4 SR para fibra óptica multimodo, 850nm/50µ, OM3 ou OM4, com alcance de até 300m, para conexão aos switches SPINE.

3.9 Deverão ser fornecidos os cabos UTP Cat6 e cordões ópticos multimodo OM3 ou OM4, com comprimento mínimo de 5 (cinco) metros, compatíveis com as interfaces cobre e fibra que compõem os dispositivos adquiridos e em quantidade suficiente para a conexão dessas interfaces, bem como com os equipamentos Tipo “SPINE” (uplink).

3.10 REQUISITOS DE CAPACIDADE

3.11 Possuir matriz de comutação com capacidade de, no mínimo, 1.7Tbps (um vírgula sete terabits por segundo).

3.12 Possuir capacidade de processamento de, no mínimo, 700 Mpps (setecentos milhões de pacotes por segundo).

3.13 Possuir capacidade de associação das portas de mesma capacidade, no mínimo, em grupo de 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.

3.14 Deve implementar, no mínimo, 4.000 (quatro mil) VLANs, conforme padrão IEEE 802.1q.

3.15 Deve implementar 802.3ad Agregação de links com mínimo de 54 grupos de 8 portas.

3.16 Suportar tabela de endereços MAC com capacidade para, no mínimo, 64.000 endereços MAC.

3.17 Deve possuir tabela de roteamento com 90.000 rotas IPv4 e 27.000 rotas IPv6.

3.18 Deve suportar no mínimo 1.000 Access Control Entries (Egress).

3.19 Deve suportar no mínimo 8.000 Access Control Entries (Ingress).

3.20 Deve implementar roteamento estático.

3.21 Deve possuir interface de Console Serial.

3.22 Deve possui, no mínimo, 1 (uma) porta para gerenciamento out-of-band com conector RJ-45.

3.23 Deverá operar nas temperaturas de 0 a 40 °C.

3.24 Deverá possuir fontes de alimentação internas com alimentação através de circuitos elétricos de entrada distintos, para tensão de 110/220 VAC a 60 Hz, com capacidade para implementar a configuração máxima e redundância n+1 instalada, ou seja, 1 (uma) fonte extra de redundância.

3.25 Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento.

3.26 REQUISITOS FUNCIONAIS

3.27 Suporte à OVERLAY NETWORK através de protocolos de encapsulamento como VXLAN ou GENEVE (Generic Network Virtualization Encapsulation).

3.28 Deverá prover gateway VXLAN conforme arquitetura do Software Defined Network (SDN) NSX da VMware. Deverá ser comprovado a compatibilidade.

3.29 A solução LEAF deverá também receber os UPLINKs dos SWITCHES DE ACESSO, por meio de dois links redundantes ativos em camada 2 (LACP).

3.30 Deve implementar funcionalidade que permita a detecção de links unidirecionais.

3.31 Deve implementar funcionalidade que permita a detecção de falhas de uplink.

3.32 Deve implementar os seguintes padrões IEEE 802.1D, 802.1W, 802.1S, 802.1P.

3.33 Deve suportar JUMBO FRAME (mínimo de 9000 bytes) em todas as interfaces Gigabit Ethernet.

3.34 Deve implementar LLDP (IEEE 802.1ab).

3.35 Deve implementar PVST+, RPVST+ ou protocolo compatível.

3.36 Deve implementar MSTP (IEEE 802.1s) com suporte a 64 instâncias.

3.37 Deve Implementar roteamento OSPFv2 e OSPFv3.

3.38 Deve implementar roteamento OSPFv2 NSSA.

3.39 Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro.

3.40 Deve implementar roteamento OSPF com ECMP (Equal Cost Multi Path) de no mínimo, 8 grupos.

3.41 Deve implementar OSPF com “Graceful Restart”, que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado.

3.42 Deve implementar BGP.

3.43 Deve implementar BGP-4.

3.44 Deve implementar PRB (Policy Based Routing).

3.45 Deve implementar VRRP (Virtual Router Redundancy Protocol).

3.46 Deve implementar DHCP Client e DHCP Relay.

3.47 Deve suportar VRF ((Virtual Routing and Forwarding) até 3 VRFs Routing

3.48 Deve implementar VRF Ipv4 e Ipv6.

3.49 Deve implementar PIM-SM.

3.50 Deve implementar IGMP nas versões v1 e v2 e Snooping.

3.51 Deve implementar MLD Snooping.

3.52 Deve implementar funcionalidade de proteção contra frames de BPDUs (spanning tree), no caso de recebimento de BPDUs, a porta deve ser colocada no estado de “down”.

3.53 Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso devão ser fornecidas.

3.54 Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado.

3.55 Deve suportar espelhamento de portas.

3.56 Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ ou CBWFQ.

3.57 Deve suportar no mínimo, 8 (oito) filas de prioridade por porta.

3.58 Deve implementar ACL´s Ipv4 e Ipv6.

3.59 Deve possuir RADIUS e TACACS+ para controle de gerenciamento do switch.

3.60 Deve suportar RADIUS/TACACS+ servers até 1 servidor.

3.61 Deve suportar duas imagens de software na memória flash (firmware).

3.62 Deve possuir capacidade de armazenar múltiplos arquivos de configuração.

3.63 Deve implementar sFlow (IPv4 e IPv6) ou similar.

3.64 Deve implementar TFTP, SFTP ou SCP para gerenciamento de software e configuração.

3.65 Deve implementar SNMP v1, v2c e v3.

3.66 Deve possuir sincronização de horário (clock) do equipamento com servidor de tempo através do protocolo NTP ou SNTP.

3.67 Deve suportar SSH v2.

3.68 Deve suportar AAA (TACACS+ & RADIUS).

3.69 Deve implementar CLI com gerência por meio de linhas de comando.

3.70 Deve ser fornecido com a versão de software mais completa disponível para o equipamento.

3.71 Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

3.72 Os equipamentos, materiais e produtos a serem fornecidos deverão atender a todas as Normas e Resoluções da Agência Nacional de Telecomunicações - ANATEL de acordo com a Resolução nº 242 ou superior.

3.73 Todas as versões de sistema operacional ou software armazenado no equipamento deverão ser fornecidos nos releases mais atualizados, adequadas às necessidades requeridas nesta especificação, fornecidas em mídia física. Durante a vigência da garantia / suporte técnico será prevista a atualização do Sistema Operacional do equipamento dentro da mesma versão por outra mais atualizada visando manter o equipamento atualizado e livre de bugs e falhas de segurança.

3.74 Deverão ser fornecidos todos os softwares, cabos de força e lógicos, conectores, adaptadores, acessórios de fixação, necessários para o pleno funcionamento do equipamento.

3.75 Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante) e estar nas condições originais de fabricação, ou seja, sem modificação, retirada ou acréscimo de componentes externos e / ou internos à montagem original do fabricante.

3.76 Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento, sem prazo para expirar, permitindo que os equipamentos continuem operacionais com todas as funcionalidades descritas neste objeto, mesmo após o término do período de suporte ou garantia.

3.77 Deve acompanhar todos os componentes necessários para sua fixação no rack.

4. SWITCH SPINE - TIPO 3

Deverão ser fornecidos switches a serem instalados no Datacenter do CJF, compondo a camada SPINE.

Os switches a serem fornecidos deverão atender integralmente aos seguintes requisitos:

4.1 O equipamento deve ser específico para o ambiente de Datacenter, com capacidade de operação em camada 3 do modelo OSI, de baixa latência, com comutação de pacotes de alto desempenho arquitetura “non blocking”.

4.2 Instalável em rack padrão de 19”, ocupando no máximo 1 (uma) unidade de rack (RU), devendo ser fornecidos os respectivos acessórios de fixação.

4.3 Suportar a funcionalidade de “SPINE”, na arquitetura “Spine-and-Leaf”.

4.4 QUANTIDADE DE INTERFACES E TRANSCEIVERS

4.5 Cada switch deverá possuir, no mínimo:

4.5.1 32 (trinta e duas) portas Ethernet SFP28 sem bloqueio (non-blocking), totalmente licenciadas.

4.5.2 5 (cinco) portas Ethernet QSFP28 para UPLINK, sem bloqueio (non-blocking), totalmente licenciadas.

4.6 As portas SFP28 devem suportar transceivers nos padrões 10GBASE-SR, 10GBASE-LR, 10GBASE-LRM, 25GBASE-SR, 25GBASE-LR, 25GBASE-LRM.

4.7 As portas QSFP28 devem suportar transceivers nos padrões 40GBASE-LR4, 40GBASE-SR4, 100GBASE-SR e 100GBASE-LR.

4.8 Cada switch deverá ser fornecido com:

4.8.1 16 (dezesseis) transceivers do tipo SFP+, 10GbE-SR para Fibra Óptica MultiModo, 850nm/50µ, OM3 ou OM4, com alcance de até 300m, em conectores tipo LC.

4.8.2 8 (oito) transceivers do tipo SFP28, 25GbE-SR para Fibra Óptica MultiModo, 850nm/50µ, OM3 ou OM4, com alcance de até 300m, em conectores tipo LC.

4.8.3 6 (seis) cabos QSFP+ para QSFP+, com comprimento de, no mínimo 5 (cinco) metros, do tipo DAC (Direct Attach Copper Cable) para conexão aos switches LEAF.

4.8.4 2 (dois) cabos QSFP28 para QSFP28 (100Gbps), com comprimento de, no mínimo 3 (três) metros, do tipo DAC (Direct Attach Copper Cable) para UPLINK com outro módulo SPINE.

4.9 Deverão ser fornecidos os cordões ópticos multimodo OM3 ou OM4, com comprimento mínimo de 5 (cinco) metros, compatíveis com as fibras que compõem os dispositivos adquiridos e em quantidade suficiente para a conexão dessas interfaces, bem como com os equipamentos Tipo "LEAF".

4.10 REQUISITOS DE CAPACIDADE

4.11 Possuir matriz de comutação com capacidade de pelo menos 3,6Tbps (três vírgula seis terabits por segundo).

4.12 Possuir capacidade de processamento de pelo menos 1200Mpps (um mil e duzentos milhões de pacotes por segundo).

4.13 Deve possuir buffers de, no mínimo, 24 MB (vinte e quatro megabytes).

4.14 Deve implementar, no mínimo, 4.000 (quatro mil) VLANs, conforme padrão IEEE 802.1q.

4.15 Deve implementar 802.3ad Agregação de Links com mínimo de 54 grupos de 8 portas.

4.16 Deve implementar MSTP (IEEE 802.1s) com suporte a 64 instâncias.

4.17 Deve suportar no mínimo, 8 (oito) filas de prioridade por porta.

4.18 Suportar tabela de endereços MAC com capacidade para, no mínimo, 64.000 endereços MAC.

4.19 Deve possuir interface de Console Serial.

4.20 Deve possui, no mínimo, 1 (uma) porta para gerenciamento out-of-band com conector RJ-45.

4.21 Deverá operar nas temperaturas de 0 a 40 °C.

4.22 Deverá possuir fontes de alimentação internas com alimentação através de circuitos elétricos de entrada distintos, para tensão de 110/220 VAC a 60 Hz, com capacidade para implementar a configuração máxima e redundância n+1 instalada e 1 (uma) fonte extra de redundância.

4.23 Deve suportar no mínimo 2 (duas) fontes de alimentação operando em redundância e em modo load-sharing. Estas Fontes devem operar entre 110 a 220VAC. Devem também operar em 50/60Hz de frequência.

4.24 Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento.

4.25 REQUISITOS FUNCIONAIS

4.26 Deve permitir a agregação de links com LACP entre dois equipamentos autônomos (MC-LAG).

4.27 Implementar SSH para acesso à interface de linha de comando.

4.28 Deve implementar funcionalidade que permita a detecção de links unidirecionais.

4.29 Deve implementar funcionalidade que permita a detecção de falhas de uplink.

4.30 Suportar simultaneamente em sua memória flash (ou semelhante), duas imagens do sistema operacional.

4.31 Permitir o acesso via GUI (graphical user interface) e CLI (command line interface). Podendo ser atendido através do software de gerenciamento.

4.32 Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um servidor de autenticação/autorização do tipo TACACS ou RADIUS ou similar.

4.33 Deve implementar os seguintes padrões IEEE 802.1D, 802.1W, 802.1S, 802.1P.

4.34 Deve implementar JUMBO FRAME (mínimo de 9000 bytes) em todas as interfaces Gigabit Ethernet.

4.35 Deve implementar LLDP (IEEE 802.1ab).

4.36 Deve implementar PVST+, RPVST+ ou protocolo compatível.

4.37 Deve implementar roteamento estático.

4.38 Deve Implementar roteamento OSPFv2 e OSPFv3.

4.39 Deve implementar roteamento OSPF com suporte NSSA.

4.40 Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro.

4.41 Deve implementar roteamento OSPF com ECMP (Equal Cost Multi Path) de no mínimo, 4 grupos.

4.42 Deve implementar OSPF com "Graceful Restart", que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado.

4.43 Deve implementar BGP.

4.44 Deve implementar BGP-4.

4.45 Deve implementar PRB (Policy Based Routing).

4.46 Deve implementar VRRP (Virtual Router Redundancy Protocol).

4.47 Deve implementar DHCP Client e DHCP Relay.

4.48 Deve suportar VRF (Virtual Routing and Forwarding) até 32 VRFs Routing

4.49 Deve implementar VRF Ipv4 e Ipv6.

4.50 Deve implementar PIM-SM.

4.51 Deve implementar IGMP nas versões v1 e v2 e v3.

4.52 Deve implementar MLD Snooping.

4.53 Deve implementar funcionalidade de proteção contra frames de BPDUs (spanning tree), no caso de recebimento de BPDUs, a porta deve ser colocada no estado de "down".

4.54 Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas.

4.55 Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado.

4.56 Deve implementar rate-limiting.

4.57 Deve suportar espelhamento de portas.

4.58 Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ ou CBWFQ.

4.59 Deve implementar ACL´s Ipv4 e Ipv6.

4.60 Deve possuir RADIUS e TACACS+ para controle de gerenciamento do switch.

4.61 Deve suportar RADIUS/TACACS+ servers até 3 server.

4.62 Deve possuir capacidade de armazenar múltiplos arquivos de configuração.

4.63 Deve implementar sFlow (IPv4 e IPv6) ou similar.

4.64 Deve implementar TFTP, SFTP ou SCP para gerenciamento de software e configuração.

4.65 Deve implementar SNMP v1, v2c e v3.

4.66 Deve possuir sincronização de horário (clock) do equipamento com servidor de tempo através do protocolo NTP ou SNTP.

4.67 Deve implementar CLI com gerência por meio de linhas de comando.

4.68 Deve ser fornecido com a versão de software mais completa disponível para o equipamento.

4.69 Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

4.70 Os equipamentos, materiais e produtos a serem fornecidos deverão atender a todas as Normas e Resoluções da Agência Nacional de Telecomunicações - ANATEL de acordo com a Resolução nº 242 ou superior.

4.71 Todas as versões de sistema operacional ou software armazenado no equipamento deverão ser fornecidos nos releases mais atualizados, adequadas às necessidades requeridas nesta especificação, fornecidas e disponíveis na mídia digital DVD ou Pendrive. Durante a vigência da garantia/suporte técnico será prevista a atualização do Sistema Operacional do equipamento dentro da mesma versão por outra mais atualizada visando manter o equipamento atualizado e livre de bugs e de falhas de segurança.

4.72 Deverão ser fornecidos todos os softwares, cabos de força e lógicos, conectores, adaptadores, acessórios de fixação, necessários para o pleno funcionamento do equipamento.

4.73 Os equipamentos fornecidos deverão ser novos, estar em produção (não serão aceitos equipamentos já descontinuados pelo fabricante) e estar nas condições originais de fabricação, ou seja, sem modificação, retirada ou acréscimo de componentes externos e / ou internos à montagem original do fabricante.

4.74 Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento, sem prazo para expirar, permitindo que os equipamentos continuem operacionais com todas as funcionalidades descritas neste objeto, mesmo após o término do período de suporte ou garantia.

5. SWITCH SAN - TIPO 4

Deverão ser fornecidos switches SAN a serem instalados no Datacenter do CJF, compondo uma rede de comunicação de armazenamento em protocolo FC (Fiber Channel).

Os switches a serem fornecidos deverão atender integralmente aos seguintes requisitos:

5.1 O equipamento deve ser específico para o ambiente de Datacenter.

5.2 O switch deve ser do tipo standalone, com altura máxima de 1RU e instalação em rack (19"). Deve acompanhar todos os componentes necessários para sua fixação no rack.

5.3 QUANTIDADE DE INTERFACES E TRANSCEIVERS

5.4 Cada switch deverá possuir, no mínimo:

5.4.1 36 (trinta e seis) portas SFP+, sem bloqueio (non-blocking), totalmente licenciadas.

5.5 As portas SFP+ devem suportar transceivers nos padrões FC ou FCoE que implementem as velocidades de 4, 8 e 16 Gbps.

5.6 Caso o equipamento não possua porta ou suporte a transceivers 16Gb nativo, deverá permitir a função SAN AGGREGATION TRUNK, utilizando duas portas de 8 Gbps.

5.7 Todas as portas deverão funcionar em modo FULL-DUPLEX e deverão suportar negociação automática de velocidade e permitir a configuração de velocidade fixa.

5.8 Cada porta FC, deverá suportar os seguintes tipos de “transceivers” ópticos SFP+ (Enhanced Small Form-factor Pluggable Transceiver): SHORT WAVELENGTH (SWL) e LONG WAVELENGTH (LWL).

5.9 Cada switch deverá ser fornecido com:

5.9.1 36 (trinta e seis) transceivers do tipo SFP+ SHORT WAVELENGTH (SWL) FC ou FCoE que implementem as velocidades de 4, 8 e 16 Gbps, fibra óptica multimodo, em conectores tipo LC para interconexão com as interfaces FC dos equipamentos em produção do CJF.

5.10 Todos os transceivers ópticos do tipo SFP+, devem ser de um mesmo modelo e fabricante.

5.11 Deverão ser fornecidos as fibras ópticas multimodo OM3 ou OM4, com comprimento mínimo de 3 (três) metros, compatíveis com os padrões dos transceivers que compõem os dispositivos adquiridos e em quantidade suficiente para a conexão dessas interfaces.

5.12 REQUISITOS FUNCIONAIS E DE CAPACIDADE

5.13 Deverá possuir, no mínimo, 768 Gbps (setecentos e sessenta e oito gigabit por segundo) de largura de banda agregada (full duplex).

5.14 Deve ser fornecido com configuração de CPU e memórias (RAM e Flash) suficientes para implementação de todas as funcionalidades descritas nesta especificação.

5.15 Deve ser instalada a versão mais recente do software interno do switch.

5.16 Deve permitir a atualização de firmware de forma não disruptiva (In Service Software Upgrade – ISSU).

5.17 Implementar isolamento total de múltiplos fabrics através de SANs Virtuais.

5.18 Possui a funcionalidade que permita criar TRUNKING entre os switches.

5.19 Deverá suportar os seguintes serviços "Fabric": Simple Name Server (SNS) e Registered State Change Notification (RSCN).

5.20 Deverá possuir funcionalidade que permita virtualizar portas de servidores conectados (NPIV).

5.21 Suporte a "Virtual Fabric".

5.22 Deve possui, no mínimo, 1 (uma) porta para gerenciamento out-of-band com conector RJ-45.

5.23 Deverá possuir funcionalidade de zonas a nível de porta.

5.24 Implementar, pelo menos, os protocolos: FC-AL-2, FC-GS-7, FC-GS-6, FC-GS-5, FC-GS-4, FC-IFR, FC-SP-2, FC-SP, FC-SW-6, FC-SW-5, FC-SW-4, FC-SW-3, FC-VI, FC-TAPE, FC-DA-2, FC-DA, FC-FLA, FC-PLDA, FC-MI-3, FC-MI-2, FC-PI-5, FC-PI-4,FC-PI-3, FC-PI-2, FC-PI, FC-FS-4, FC-FS-3, FC-FS-2, FC-FS, FC-LS-3, FC-LS-2, FCLS,FC-BB-6, FC-BB-5, FC-BB-4, FC-BB-3, FC-BB-2, FC-SB-4, FC-SB-3, FC-SB-2,FC-SB, FCP-4, FCP-3, FCP-2, FCP.

5.25 Deverá suportar os tipos de porta: F_Port, E_Port, EX_Port, D_Port e M_Port (porta de espelhamento).

5.26 Implementar canais virtuais para priorização de trafego dentro dos ISLs.

5.27 Deve implementar o protocolo NTP (Network Time Protocol).

5.28 Deve ser gerenciável via SNMP versões 1, 2 e 3.

5.29 Deve implementar SSH versão 2.

5.30 Possuir gerenciamento MIB, MIB SNMP II, MIB bridging (RFC 1493). Deve possuir a descrição completa das MIBs implementadas no equipamento e as extensões privadas se as mesmas existirem.

5.31 Cabos para todas as fontes de alimentação de energia elétrica, padrão ABNT 14136 (2P+T).

5.32 Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento, sem prazo para expirar, permitindo que os equipamentos continuem operacionais com todas as funcionalidades descritas neste objeto, mesmo após o término do período de suporte ou garantia.

5.33 Os equipamentos ofertados deverão ser novos e com embalagem do fabricante. Não serão aceitos switches vindos de reparos, recondicionados e/ou outra forma que demonstre que os switches tiveram uso anterior.

5.34 Deverá possuir fontes de alimentação internas com alimentação através de circuitos elétricos de entrada distintos, para tensão de 110/220 VAC a 60 Hz, com capacidade para implementar a configuração máxima e redundância n+1 instalada e 1 (uma) fonte extra de redundância.

5.35 Deve suportar no mínimo 2 (duas) fontes de alimentação operando em redundância e em modo load-sharing. Estas Fontes devem operar entre 110 a 220VAC. Devem também operar em 50/60Hz de frequência.

5.36 Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento.

5.37 O fornecimento deve contemplar todos os hardwares e softwares necessários para a implementação da função de agregação dos switches, de maneira a atender as especificações constantes neste documento.

6. SOFTWARE GERÊNCIA DE REDE CABEADA

6.1 A Contratada do LOTE 01 deverá fornecer Solução para Gerenciamento de Redes, com capacidade para prover monitoramento e gerenciamento fim-a-fim dos recursos da infraestrutura de ativos de rede e outros equipamentos a ela conectados, realizando também a gerência dos switches que irão compor a rede LAN do CJF.

6.2 A solução deve permitir o gerenciamento de capacidade, estado, configuração e uso dos recursos de rede, bem como dos serviços utilizados na rede, bem como os usuários que têm permissão para se utilizar da infraestrutura.

6.3 Deve ser uma solução de software modular, que permita a adição futura de licenças e funcionalidades sem que seja necessária a troca, ou atualização do software principal (framework).

6.4 A solução para gerenciamento de redes deve ser do mesmo fabricante dos switches ofertados.

6.5 As licenças da solução para gerenciamento de redes deverão ser fornecidas em quantidade suficiente para atender a necessidade de gerenciamento de todos os elementos fornecidos no Lote 1.

6.6 A solução para gerenciamento de redes deverá possuir as seguintes funcionalidades:

6.6.1 Os controladores deverão possuir licença e capacidade para operar, controlar e gerenciar o total de dispositivos fornecidos.

6.6.2 Os controladores de rede poderão ser fornecidos através de um conjunto de dispositivos físicos e software.

6.6.3 Deverá realizar a ativação do plano de controle (“underlay network”) e do plano de dados (“overlay network”) nos switches pertencentes à arquitetura “Spine and Leaf” de forma automatizada.

6.6.4 Deverá realizar automação, configuração, gerenciamento e monitoração da saúde física dos equipamentos, via GUI (graphical user interface).

6.6.5 Possibilidade de criação de versões de configuração dos equipamentos pertencentes à topologia “Spine-and-Leaf” e suporte a “rollback” da configuração para versões anteriores.

6.6.6 Deverá expor como serviço, via API (Application Programming Interface) REST, todas as configurações de rede, tanto da camada “underlay” quanto da camada “overlay”, permitindo configuração da infraestrutura de rede por orquestradores externos.

6.6.7 Implementar o protocolo SSH para acesso à interface de linha de comando, protegido por senha.

6.6.8 Implementar mecanismo de autenticação e autorização para acesso local ou remoto à solução, baseado em TACACS, RADIUS ou grupos LDAP.

6.6.9 Permitir, controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em determinados elementos de rede.

6.6.10 Deve possuir arquitetura WEB, de forma a poder ser acessado por browser padrão, sem necessidade de qualquer cliente específico.

6.6.11 Deve permitir instalação diretamente sobre o sistema operacional de servidor (Windows Server ou Linux), em caso necessário utilização de framework de terceiros, o mesmo deve ser fornecido juntamente com a solução.

6.6.12 Deve ter a funcionalidade de auto-descobrimento de equipamentos na rede, exibindo a rede através de várias opções de visualização dos elementos descobertos: por topologia, por VLAN, por tipo de elementos, por uma visualização customizada com base na organização física dos equipamentos e por organização lógica dos mesmos.

6.6.13 Deve permitir o agendamento de auto-descobrimento periódico.

6.6.14 Deve permitir a definição de múltiplos usuários de gerenciamento, definindo, inclusive, a atribuição de funções de gerência de cada um dos usuários, e a limitação sobre quais equipamentos esses usuários têm qual tipo de permissão de acesso.

6.6.15 O Administrador deve ter o controle sobre quais usuários do sistema de gerência que terão permissão de gerência sobre os equipamentos e grupos de equipamentos, bem como deve ter o poder de restringir quais comandos podem ser implementados pelos usuários.

6.6.16 O Administrador deve ter acesso a todas as ferramentas de auditoria, que possam identificar as alterações efetuadas na rede, mesmo as que tenham sido programadas na rede, bem como quem foram os autores das alterações.

6.6.17 Deve oferecer um gerenciamento completo dos processos de tolerância a falhas através de análise e correlação de eventos, alarmes em tempo real, e avaliação de problemas.

6.6.18 Deve permitir o monitoramento de performance, detecção de gargalos e outros problemas da rede, incluindo aqueles relacionados com a carga da CPU, uso da memória, e utilização de banda, tempo de resposta e disponibilidade dos equipamentos.

6.6.19 Deve permitir habilitar e/ou desabilitar sensores que estejam disponíveis no equipamento.

6.6.20 Deve permitir a rápida identificação das áreas mais carregadas da rede através de estatísticas sobre os maiores consumidores de recursos.

6.6.21 Deve possuir a possibilidade de definir limites de parâmetros que gerem alarmes em qualquer monitor, alertando rapidamente os operadores sobre qualquer questão considerada anormal.

6.6.22 Deve possibilitar a customização tanto dos eventos como das regras dos filtros de alarmes, para evitar que os operadores não recebam alarmes desnecessários.

6.6.23 Deve possuir gerenciamento centralizado de relatórios para simplificar o acesso dos operadores e administradores aos dados gerados pelo uso da rede.

6.6.24 Deve oferecer a possibilidade de uso de relatórios pré-definidos, além de permitir que os administradores definam os parâmetros de seus próprios relatórios.

6.6.25 Deve possibilitar a geração de relatórios em diversos formatos, incluindo arquivos com extensões "pdf" ou "xls".

6.6.26 A licença adequada do SGDB para uso neste Sistema de Gerenciamento também deve ser fornecida, se necessário.

6.6.27 Deve simplificar a distribuição e gerenciamento de VLANs através da infraestrutura de rede, incluindo a habilidade de verificar as topologias de VLAN vigentes, e fazer a distribuição em bloco das novas VLANs pela rede.

6.6.28 Deve permitir fazer o inventário das versões de sistema operacional e configuração gravados em cada equipamento, bem como controlar o backup e o restore dos ativos de rede gerenciados.

6.6.29 Deve permitir a integração com as bases de usuários da rede, para gerenciamento da autenticação desses usuários.

6.6.30 Deve implementar recursos de gerenciamento para redes SAN e específicos para Datacenter.

7. SERVIÇO DE ORGANIZAÇÃO DOS ATIVOS DE REDE E RACKS DE COMUNICAÇÃO QUE COMPÕE O SISTEMA DE CABEAMENTO ESTRUTURA E A INFRAESTRUTURA DE REDE DO CJF USANDO CABOS UTP E FC (SALAS DE DISTRIBUIÇÃO DOS ANDARES E DATACENTER)

7.1 Em instalações aparentes, a fixação dos cabos será feita por braçadeiras espaçadas de 50 cm. Em trechos curvos, as braçadeiras serão fixadas no início e no fim de cada curva. Em trechos curvos serão adotados os raios mínimos de curvatura recomendados pela Norma NBR 5410.

7.2 Os lances de cabos em par trançado, devem estar limitados a 100 m, obrigatoriamente, e não conter emendas.

7.3 Todas conexões em Painéis de Distribuição, “Hub’s”, devem ser providas de meios de proteção dos terminais, tais como tampa plástica, evitando contatos ou choques, que possam causar distúrbios elétricos.

7.4 Na instalação dos cabos, respeitar sempre os raios de curvatura mínimo dos cabos, conforme especificado pelos fabricantes.

7.5 Nos cabos do cabeamento primário, não são permitidas derivações em paralelo e emendas.

7.6 Todos os cabos devem estar perfeitamente identificados, através de anilhas plásticas.

8. RACK DE REDE – PADRÃO 19 POLEGADAS

8.1 A mudança do RACK atual para o novo será de responsabilidade da CONTRATADA bem como a sua organização no padrão de cabeamento estruturado seguindo as normas ANSI/TIA, como a ANSI/TIA-568-C.1, ANSI/TIA-568-C.2, a ANSI/TIA-569-C, ANSI/TIA-942-A, ANSI/TIA-568-C.3 e pela ISO, como a ISO/IEC 11801 e ISO/IEC 24764, ABNT NBR 14565:2013.

8.2 A Contratada do LOTE 1 deverá fornecer e realizar a troca do RACK atual onde localiza o nosso chassi Switch CORE, por um RACK de distribuição com as seguintes características:

8.2.1 Possuir, no mínimo, 40U.

8.2.2 Deve possuir porta nas laterais de distribuição dos cabos e para os equipamentos de conectividade que serão instalados.

8.2.3 Possuir unidades de distribuição de potência (PDU) com, no mínimo, 10 tomadas 2P+T.

8.2.4 Possuir estrutura com perfis de aço.

8.2.5 Possuir tampas laterais perfuradas e removíveis.

8.2.6 Possuir abertura na base inferior para passagem de cabos.

8.2.7 Possuir porta frontal e traseira, removíveis, com chaves.

8.2.8 Deve possuir fingers de acomodação e distribuição horizontal para saída de cabos a cada 1U, acomodando a cada finger 58 cabos Cat. 5E, 48 cabos Cat. 6 ou 35 cabos Cat.6a

8.2.9 Possuir porta frontal e traseira, removíveis, com chaves.

8.2.10 Deve suportar os equipamentos do LOTE 1.

8.3 Os cabos utilizados nesses subsistemas devem ser de par trançado ou de fibra ótica e devem estar de acordo com as normas ABNT NBR 14565 e ABNT NBR 1470.

9. PATCH CORDS 1,5M

9.1 Deverão ser confeccionados e testados em fábrica.

9.2 O acessório deve ser confeccionado em cabo par trançado, U/UTP (Unshielded Twisted Pair), 24 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento em poliolefina e capa externa em PVC classe CM não propagante a chama impressa na capa.

9.3 Os conectores RJ-45 macho, devem atender às especificações para Categoria 6, consistirão de uma carcaça em policarbonato transparente, deverão ser banhados com um mínimo de 50 micropolegadas de ouro na área do contato, sobre um banho-baixo mínimo de 100 micropolegadas de níquel e os contatos devem ser de bronze fosforoso estanhado.

9.4 Os conectores RJ-45 macho devem possuir protetores sobre os conectores (Boots) na cor do cabo, para evitar desconexões acidentais.

9.5 Deverá ter uma etiqueta colada no cabo contendo o código de comercialização do fabricante do produto para fácil identificação, ter identificado o número do lote, ano e semana que o produto foi produzido.

9.6 Possuir impresso na capa do cabo a marca do fabricante e sua respectiva categoria (cat6).

9.7 O componente deve ser acompanhado de velcro, fitas auto colantes, e demais acessórios necessários para a correta fixação e identificação.

10. PATCH CORDS 2,5M

10.1 Deverão ser confeccionados e testados em fábrica.

10.2 O acessório deve ser confeccionado em cabo par trançado, U/UTP (Unshielded Twisted Pair), 24 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento em poliolefina e capa externa em PVC classe CM não propagante a chama impressa na capa.

10.3 Os conectores RJ-45 macho, devem atender às especificações para Categoria 6, consistirão de uma carcaça em policarbonato transparente, deverão ser banhados com um mínimo de 50 micropolegadas de ouro na área do contato, sobre um banho-baixo mínimo de 100 micropolegadas de níquel e os contatos devem ser de bronze fosforoso estanhado.

10.4 Os conectores RJ-45 macho devem possuir protetores sobre os conectores (Boots) na cor do cabo, para evitar desconexões acidentais.

10.5 Deverá ter uma etiqueta colada no cabo contendo o código de comercialização do fabricante do produto para fácil identificação, ter identificado o número do lote, ano e semana que o produto foi produzido.

10.6 Possuir impresso na capa do cabo a marca do fabricante e sua respectiva categoria (cat6).

10.7 O componente deve ser acompanhado de velcro, fitas auto colantes, e demais acessórios necessários para a correta fixação e identificação.

LOTE 2

LOTE 2 - SOLUÇÃO REDE SEM FIO

Para solução sem fio, novos protocolos de distribuição de sinal foram desenvolvidos pelas empresa onde a substituição do atual cenário existente no CJF, irá proporcionar um novo modo de navegação mais seguro, integrado, criptografado com trilhas de auditoria e fechamento de acesso por meio do Network Access Control (NAC), protocolos como 802.1x, sinal 5 GHZ AC MIMO Wave 2 e mapeamento dos laptops por meio de tags de segurança interligadas a nossa rede sem fio com a nossa planta baixa do prédio, evitando furtos e movimentações não autorizadas.

Assim os novos Pontos de Acesso (APs) serão instalados para dar uma nova experiência para os usuários que participam de eventos, trabalham e prestam serviço ao CJF.

Deve ser realizado um site survey pela CONTRATADA com o acompanhamento e validação da equipe técnica da SUTEC/SESINF, será responsável pela análise e determinação da quantidade exata dos equipamentos a serem adquiridos e instalados.

Serão substituídos todos os pontos de acesso controlador wireless existente no CJF.

Os APs de cada andar deverão estar conectados no rack do respectivo andar em switches com portas PoE+ (Power Over Ethernet Plus).

Os APs serão configurados para operarem no padrão IEEE 802.11 a/b/g/n/ac MIMO Wave 2.

A infraestrutura para fixação dos APs e passagem dos cabos UTP para conexão entre os APs e os switches é de responsabilidade da CONTRATADA.

A implementação da solução Wireless será feita por analista de redes da CONTRATADA acompanhada pelos técnicos do CJF.

Os equipamentos deverão possuir certificado válido referente à homologação da Agência Nacional de Telecomunicações (ANATEL). Não serão aceitos documentos provisórios ou de entrada para obtenção da certificação.

Os equipamentos fornecidos deverão estar habilitados para total integração com a rede de dados local do CONTRATANTE, apresentando compatibilidade de protocolos, configurações, energização elétrica e demais funcionalidades necessárias para o acoplamento entre as Soluções de rede sem fio e cabeada.

As licenças ofertadas deverão ser permanentes, fornecidas em versões atualizadas e estáveis, e suscetíveis às constantes atualizações de versões durante o período de garantia da Solução.

A proposta de fornecimento do LOTE 2 deverão ser contemplar todos os componentes, incluindo controladora, pontos de acesso, softwares, licenças, subscrições, módulos, acessórios, conectores, cabos e adaptadores, bem como qualquer outro elemento de hardware ou software adicionais, de forma a atender plenamente os seguintes requisitos:

i. CONTROLADORA DE MOBILIDADE WIRELESS
ii. ACCESS POINT (PONTO DE ACESSO) TIPO 1
iii. ACCESS POINT (PONTO DE ACESSO) TIPO 2
iv. TAGS DE LOCALIZAÇÃO BLE
v. SOFTWARE DE MONITORAMENTO E GERÊNCIA SEM FIO
vi. SOFTWARE DE CONTROLE DE ACESSO DE USUÁRIO

1. CONTROLADORA WIRELESS

1.1 Não será aceita solução baseada em nuvem (cloud).

1.2 Possuir tecnologia baseada em appliance virtual ou appliance físico.

1.3 REQUISITOS DE CAPACIDADE

1.4 Cada controladora deve suportar, no mínimo, 150 (cento e cinquenta) pontos de acesso simultâneos, com objetivo de suportar expansões futuras.

1.5 Permitir a conexão simultânea de, no mínimo, 1.000 (hum mil) clientes wireless, mesmo em caso de indisponibilidade da controladora ou controller.

1.6 A controladora, física ou virtual, deverá ser capaz de gerenciar a totalidade de pontos de acesso especificados no LOTE 02.

1.7 Permitir, em conjunto com o software de gerenciamento, o cadastramento de, no mínimo, 100 (cem) usuários visitantes.

1.8 Caso seja fornecido appliance físico, deve possuir fonte de alimentação interna com seleção automática de tensão (100-240V AC).

1.9 Caso seja fornecido appliance físico, deve suportar temperatura de operação entre 5°C a 40°C.

1.10 Para o caso de appliance físico, a controladora deverá vir acompanhada de 1 (um) transceiver óptico padrão 10GBase-SR SFP+ e 1 (um) transceiver óptico padrão 10GBase-LR SFP+, plenamente compatível com suas portas SFP+, para operação em fibras multimodo e monomodo com conectores padrão LC.

1.11 Caso seja fornecido appliance físico, deve possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45 ou conector padrão RS-232 ou USB.

1.12 Caso seja fornecido appliance físico, deve possuir LED para a indicação do status de atividade do equipamento e das portas Ethernet.

1.13 REQUISITOS FUNCIONAIS

1.14 Implementar agregação de links seguindo o protocolo LACP ou protocolo compatível com o switch existente.

1.15 Permitir armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

1.16 Possuir capacidade de centralização, manutenção, gerência e distribuição das configurações da solução de rede sem fio, inclusive das configurações e atualizações dos pontos de acesso.

1.17 Deverá realizar a gerência das configurações de segurança da rede sem fio e parâmetros de Radio Frequência (RF).

1.18 Permitir que os SSIDs operem em modo de tunelamento de tráfego remoto ou comutação de tráfego local.

1.19 Permitir, em conjunto com o software de gerenciamento, a criação de páginas personalizadas para o captive portal, com a inclusão de imagens, instruções em texto e campos de texto que possam ser preenchidos pelos clientes.

1.20 Permitir, em conjunto com o software de gerenciamento, a criação de SSID para visitantes, que terão seu acesso controlado através de criação de usuário e senha cadastrados internamente, sendo que este deverá possuir tempo pré-determinado de acesso à rede wireless.

1.21 O controlador wireless deverá permitir a criação de múltiplos usuários visitantes (guests).

1.22 Deve permitir que, após o processo de autenticação de usuários visitantes, os mesmos sejam redirecionados para uma página de navegação específica.

1.23 Deverá permitir o direcionamento do tráfego de saída de usuários visitantes (guests) para uma rede isolada do tráfego da rede corporativa.

1.24 Deve permitir que o portal interno para usuários visitantes (guest) seja customizável.

1.25 Deve permitir que múltiplos usuários visitantes (guest) compartilhem a mesma senha de acesso à rede.

1.26 Possibilitar a configuração de envio dos eventos do Controlador wireless para um servidor de Syslog remoto, assim como a gravação de eventos em log interno e externo.

1.27 Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

1.28 Possibilitar obtenção, via SNMP, de informações sobre a configuração do equipamento, assim como informações de capacidade, desempenho, CPU, memória e portas.

1.29 Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento e disponibilizar descrição completa da mesma.

1.30 Possibilitar níveis de acesso administrativo ao equipamento para apenas leitura, leitura/escrita, criação de contas de usuários do tipo guest (visitante), entre outros.

1.31 Permitir a configuração e gerenciamento através de browser padrão (HTTPS), SSH, quando aplicável.

1.32 Permitir que o processo de atualização de versão seja realizado através de browser padrão (HTTPS) e FTP ou TFTP.

1.33 Deverá programar a ativação ou desativação de SSID baseado em dia/hora, permitindo ao administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia determinados.

1.34 Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível (ping, trace e logs).

1.35 Possibilitar cópia “backup” da configuração, bem como a funcionalidade “restore” da configuração através de browser padrão (HTTPS) ou FTP ou TFTP.

1.36 O gerenciamento dos controladores em redundância deverá ser realizado através de um único endereço IP.

1.37 Em caso de falha, a redundância deverá ser realizada de forma automática sem nenhuma ação do administrador de rede.

1.38 Implementar os protocolos NTP com autenticação entre peers.

1.39 O protocolo de comunicação entre a controladora wireless e o ponto de acesso gerenciável e entre os pontos de acesso deve implementar criptografia.

1.40 Deverá implementar suporte ao protocolo IPv4 e IPv6.

1.41 Suportar atribuição dinâmica de endereços IPv6 tais como, IPv6 Stateless AutoConfiguration (SLAAC), Stateless DHCPv6, Statefull DHCPv6 e configuração manual de endereços IPv6.

1.42 Permitir associação de clientes IPv4 e IPv6 no mesmo SSID.

1.43 Permitir roaming transparente sem troca de endereçamento para o cliente móvel tanto em Layer 2 quanto em Layer 3.

1.44 Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x.

1.45 Implementar, pelo menos, os seguintes padrões de segurança wireless:

i. Wired Equivalent Privacy (WEP) com chaves estáticas e dinâmicas (64 e 128 bits).

ii. Wi-Fi Protected Access (WPA) com algoritmo de criptografia TKIP (Temporal Key Integrity Protocol).

iii. Wi-Fi Protected Access2 (WPA2) com os seguintes algoritmos:

a) Advanced Encryption Standard (WPA2-AES), AES – 128 bits

b) IEEE 802.1x

c) IEEE 802.11i

1.46 Implementar os seguintes controles/filtros:

i. L2 - Baseado em MAC Address e Client Isolation por VLAN.

ii. L3 - Baseado em Endrereço IP.

iii. L4 - Baseado em Portas TCP/UDP.

1.47 Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

i. MAC Address.

ii. Base Interna do equipamento.

iii. Portal de Autenticação.

iv. RADIUS.

v. IEEE 802.1x.

vi. LDAP.

1.48 Implementar IEEE 802.1X, com pelo menos os seguintes métodos EAP:

i. EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) ou EAP TTLS.

ii. PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP- MSCHAPv2).

iii. EAP-Transport Layer Security (EAP-TLS), suportando terminação do túnel EAP.

1.49 Implementar, pelo menos, mecanismos para detecção e identificação de pontos de acesso:

i. MAC Address-Spoofing.

ii. Adhoc.

1.50 Deve implementar varredura de RF nas bandas IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues).

1.51 Deve permitir criação de grupos de Pontos de Acesso para prevenção e contenção de intrusos não autorizados (rogues).

1.52 Deve possibilitar a utilização de pontos de acesso como ”sensores” de RF para fazer a monitoração do ambiente Wireless.

1.53 Ajustar automaticamente a potência dos pontos de acesso para eliminar lacunas de cobertura e otimizar o desempenho de RF.

1.54 Deve classificar automaticamente Pontos de Acesso válidos e os não autorizados (rogues).

1.55 Deve ser possível a inserção de mecanismos de firewall entre a comunicação da controladora e do Ponto de Acesso.

1.56 Implementar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.

1.57 Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e endereços MAC.

1.58 Implementar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação.

1.59 Implementar em conjunto com o software de gerenciamento o rastreamento e localização de usuário.

1.60 Permitir o controle da utilização de banda individual de cada usuário.

1.61 Implementar o snooping de pacotes multicast IGMP.

1.62 O sistema deverá permitir que seja configurado um perfil para o qual será direcionado o usuário que não consiga se autenticar (acesso guest) de forma nativa ou por meio de software externo fornecido pela CONTRATADA.

1.63 Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.

1.64 Possuir mecanismo de autenticação entre cliente móvel e ponto de acesso para evitar ataques de camada 2 com foco em pacotes de gerenciamento como association e disassociation.

1.65 Implementar varredura de RF contínua, programada ou sob demanda, com identificação de pontos de acesso ou clientes irregulares.

1.66 Na ocorrência de inoperância de um ponto de acesso, o controlador WLAN deverá ajustar automaticamente a potência dos pontos de acesso adjacentes, de modo a prover a cobertura da área não assistida.

1.67 Ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance.

1.68 Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF de forma automática.

1.69 Implementar monitoração das interferências não Wi-Fi (telefones sem fio, dispositivos bluetooth, microondas), com classificação e localização das fontes de interferência.

1.70 Suportar mecanismos “Air Time Fairness” para otimização da utilização do meio físico “ar” e desta forma, suportar melhoria de performance (throughput), entre usuários com velocidades e tecnologias mais lentas para usuários com velocidades e tecnologias mais rápidas.

1.71 Deve possuir recursos instalados para implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar a performance durante elevada utilização da rede.

1.72 Permitir que o serviço wireless seja desabilitado em determinado ponto de acesso.

1.73 Deve permitir o uso de voz e dados em cima de um mesmo SSID.

1.74 Deve possuir mecanismo automático de QoS para protocolos de voz, utilizando inspeção automática de pacotes, sem a necessidade de fazer a marcação prévia (tagging) de pacotes ou por prioridades baseado na porta TCP com protocolo SVP.

1.75 Suportar 802.11e com WMM e U-APSD.

1.76 Implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede.

1.77 Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN e videoconferência.

1.78 Implementar mecanismo de Call Admission Control (CAC) para chamadas de Voz ou mecanismos similares.

1.79 Deve permitir visibilidade e controle das aplicações, permitindo a priorização de aplicações críticas, redução na prioridade de aplicações menos críticas e o bloqueio de aplicações não permitidas já na camada de acesso.

1.80 Deve implementar técnica de inspeção de pacotes para controle de aplicações que não utilizam portas fixas ou que utilizam protocolo TCP porta 80 ou 443.

1.81 As controladoras deverão atender aos seguintes padrões, protocolos e funcionalidades:

i. IEEE 802.11a.
ii. IEEE 802.11b.
iii. IEEE 802.11g.
iv. IEEE 802.11n.
v. IEEE 802.11ac Wave1 e Wave 2.
vi. IEEE 802.11d.
vii. WPA® Enterprise/Personal.
viii. WPA2® Enterprise/Personal.
ix. EAP-TLS.
x. EAP-TTLS/MSCHAPv2.
xi. PEAPv0/EAP-MSCHAPv2.
xii. PEAPv1/EAP-GTC.
xiii. EAP-SIM.
xiv. EAP-FAST.
xv. Short Guard Interval (SGI).
xvi. Packet Aggregation (A-MPDU).

1.82 Implementar QoS específico por SSID para priorização de tráfego de um SSID sobre outro SSID.

1.83 Implementar assinaturas de ataques de RF e prevenção de intrusão para ajudar o administrador a detectar rapidamente ataques de RF “Denial of Service (DoS)” no mínimo dos seguintes tipos: “Association flood or storm”, “Authentication flood or storm” e “EAPOL Start”.

1.84 Deve ser compatível com as TAGS DE LOCALIZAÇÃO fornecida no Lote 02.

1.85 Deve permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

1.86 Deve permitir gravação de múltiplas configurações.

1.87 Deve permitir a gravação de eventos por meio do protocolo syslog.

1.88 Deve possuir capacidade de gerenciamento hierárquico, com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do grupo sem a necessidade de configuração individual de cada equipamento.

1.89 Deve permitir acesso ao sistema através de cliente com browser padrão (http, https).

1.90 Deve permitir operação em modo mesh e permitir a utilização de mesh com os pontos de acesso apresentados na proposta comercial sem restrições.

1.91 Deve permitir o uso de múltiplos SSIDs simultaneamente.

1.92 Deve permitir implementar varredura de RF contínua, programada ou sob demanda, com identificação de APs ou clientes irregulares.

1.93 Na ocorrência de inoperância de um AP, o controlador WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a prover a cobertura da área não assistida.

1.94 Deve ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance.

1.95 Deve detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura e controle da propagação indesejada de RF.

1.96 Deve permitir implementar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance.

1.97 Deve permitir implementar balanceamento entre APs, fornecendo todas as licenças necessárias.

1.98 Deve detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção, automaticamente.

1.99 Deve ajustar, dinamicamente, o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade.

1.100 Deve permitir o uso de voz e dados sobre um mesmo SSID.

1.101 Deve permitir conexão entre APs sem a necessidade de conexão cabeada, implementando assim uma rede padrão mesh, utilizando o modelo dos APs ofertados na proposta.

1.102 Deve suportar 802.11e com WMM, U-APSD e T-SPEC.

1.103 Deve otimizar o desempenho e a cobertura da radiofrequência.

1.104 Deve possuir base de dados de usuários interna para autenticação de usuários convidados / temporários (acesso guest).

1.104 Deve permitir autenticação em no mínimo os seguintes sistemas de base de dados de usuários: Microsoft Active Diretor, FreeRadius, entre outros.

1.105 Deve realizar o provisionamento de usuários convidados (guests) através de interface Web por meio de um usuário administrativo com permissões mínimas, exclusivas para este fim.

1.106 Deve possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos EAP: EAP-MD5, PEAP/EAP-GTC, PEAP/EAP-MSCHAPv2, EAP-TLS com utilização de base de usuários interna ou servidor RADIUS externo.

1.107 Deve suportar as especificações abaixo:

i. RFC 2716 PPP EAP-TLS
ii. RFC 2865 RADIUS Authentication
iii. RFC 2548.
iv. RFC 3579 RADIUS Support for EAP
v. RFC 3580 IEEE 802.1X RADIUS Guidelines
vi. RFC 3748 Extensible Authentication Protocol (EAP)
vii. Web-based authentication
viii. RFC 768 UDP
ix. RFC 791 IP
x. RFC 2460 IPv6
xi. RFC 792 ICMP
xii. RFC 793 TCP
xiii. RFC 826 ARP
xiv. RFC 1122 Requirements for Internet Hosts
xv. RFC 1519 CIDR
xvi. RFC 1542 BOOTP

xvii. RFC 2131 DHCP
xviii. Wi-Fi Protected Access (WPA)
xix. IEEE 802.11i (WPA2, RSN)
xx. RFC 2104 Keyed-Hashing for Message Authentication (HMAC)
xxi. RFC 2246 The TLS Protocol (SSL)
xxii. RFC 2401 Security Architecture for the Internet Protocol
xxiii. RFC 2403 The Use of HMAC-MD5-96 within ESP and AH
xxiv. RFC 2404 HMAC-SHA-1-96 within ESP and AH
xxv. RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV
xxvi. RFC 2407 Interpretation for ISAKMP
xxvii. RFC 2408 ISAKMP
xxviii. RFC 2409 IKE
xxix. RFC 2451 The ESP CBC-Mode Cipher Algorithms
xxx. RFC 5246 TLS1.2
xxxi. Simple Network Management Protocol (SNMP) v1, v2c, v3
xxxii. RFC 854 Telnet client and server
xxxiii. RFC 1157 SNMPv1
xxxiv. RFC 1213 MIB Base for Network Management of TCP/IP-based internets - MIB-II
xxxv. RFC 1350 The TFTP Protocol (Revision 2)
xxxvi. RFC 2030 SNTP, Simple Network Time Protocol v4
xxxvii. RFC 2863 The Interfaces Group MIB
xxxviii. RFC 3164 BSD System Logging Protocol (syslog)
xxxix. RFC 3414 User-based Security Model (USM) for v.3 of the Simple Network Management
xl. RFC 3418 Management Information Base (MIB) for SNMP

1.109 Deve possuir suporte a autenticação IEEE 802.1X, com o método PEAP/EAP-GTC, e com utilização de base de usuários LDAP externa.

1.110 Deve suportar utilização de Portal Captivo externo ao controlador.

1.111 Deve permitir a autenticação (através de endereço MAC, Portal Captivo ou IEEE 802.1X) de usuários conectados à rede WLAN.

1.112 Deve suportar implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação.

1.113 Deve permitir o bloqueio de comunicação entre clientes wireless – L2 bridging.

1.114 Deve suportar implementar listas de controle de acesso (ACLs).

1.115 Deve oferecer detecção e proteção integrada de ataques de negação de serviços TCP, ICMP.

1.116 Deve suportar implementar Qualidade de Serviço com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede.

1.117 Deve possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras.

1.118 Deve possuir mecanismo de controle de admissão de chamadas nos pontos de acesso (CAC).

1.119 Deve implementar a tecnologia de “Channel load balancing”, permitindo que clientes sejam automaticamente distribuídos entre Pontos de Acesso adjacentes operando em canais distintos, com o objetivo de balancear a carga entre os Pontos de Acesso.

1.120 Deve implementar a tecnologia de “Band Steering/Select”, permitindo que clientes com suporte a faixa de frequência de 5GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5GHz.

1.121 Deve possuir funcionalidade de conexão Site to Site VPN utilizando padrão Ipsec. Caso a solução fornecida não possua a funcionalidade, será aceita solução de VPN adicional do mesmo fabricante.

1.122 Deve permitir implementar segurança IEEE 802.11i.

1.123 Deve suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP e TKIP.

1.124 Deve realizar a varredura no canal de operação do AP sem impacto na performance da rede WLAN.

1.125 Deve permitir a varredura em todos os canais possíveis de RF para detecção e contenção de ameaças na rede WLAN.

1.126 Deve fazer a varredura dos espectros de 2,4 GHz e 5 GHz para localização e classificação de interferências não 802.11 e evita-las automaticamente.

1.127 Deve possuir funcionalidade de analisador gráfico de espectro para detecção de interferências nas faixas de frequência de 2.4 e 5 GHz, sejam elas IEEE 802.11 ou não.

1.128 Deve disponibilizar interface gráfica com, pelo menos, gráficos de Fast Fourier Transform (FFT) e espectrograma. Caso a funcionalidade não possa ser apresentada pela controladora, deve ser fornecido um equipamento ou software, do mesmo fabricante, que o faça.

1.129 Deve possibilitar utilizar os APs como ”sensores” de RF para fazer a monitoração do ambiente Wireless.

1.130 Deve classificar automaticamente APs válidos, os que interferem e os não autorizados (rogues).

1.131 Deve realizar a identificação e contenção de redes “ad-hoc”.

1.132 Deve detectar e bloquear o bridging entre estações da rede WLAN.

2.0 PONTO DE ACESSO - TIPO 1

2.1 Equipamento deve possuir Rádio Bluetooth Low Energy (BLE) (Bluetooth de baixa energia) integrado que simplifica a gestão remota de uma rede alimentada por bateria em grande escala, enquanto também fornece localização avançada e sinalização interna, bem como capacidades de notificação push baseadas na proximidade.

2.2 Não serão aceitas plataformas de gerenciamento em nuvem.

2.3 O equipamento deve ser novo, sem uso anterior e o modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta, não sendo aceita solução em roadmap.

2.4 Deve ser fornecido com a versão mais recente (última versão comercial disponível) do software interno instalado.

2.5 O equipamento deve ser do mesmo fabricante dos demais equipamentos da solução, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

2.6 Deve permitir funcionamento em modo auto gerenciado, sem a necessidade de uma controladora de mobilidade, onde o próprio Ponto de Acesso pode operar como uma Controladora Virtual, seguindo no mínimo as seguintes características:

i. Deve suportar o agrupamento dos pontos de acesso, para operar em modo distribuído/colaborativo com suporte a, pelo menos, 60 (sessenta) Pontos de Acesso do mesmo modelo em um mesmo conjunto.

2.7 Deve suportar o atendimento de, no mínimo, 1.500 (um mil e quinhentos) dispositivos associados simultaneamente.

2.8 Deve permitir que o conjunto de pontos de acesso sejam atualizados de forma centralizada pela interface gráfica.

2.9 Deverá ser entregue todo o hardware e software necessário para suportar todas as quantidades e funcionalidades descritas.

2.10 Deve disponibilizar uma interface gráfica única e centralizada, acessível por browser padrão em página https, para configuração do conjunto de Pontos de Acesso (cluster).

2.11 Deve permitir funcionamento em modo gerenciado por controlador de mobilidade, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF.

2.12 Em modo gerenciado por controladora de mobilidade, o Ponto de Acesso deve ser capaz de criar tuneis distintos para encaminhando de trafego de gerência e encaminhamento de trafego dos dispositivos (Dados).

2.13 O túnel onde é encaminhado o trafego de gerência entre o Ponto de Acesso e a Controladora, deve suportar conexão segura IPSEC ou similar, garantindo integridade dos dados trafegados. Esta funcionalidade pode ser feita pelo Ponto de Acesso ou pela controladora fornecida no Lote 2.

2.14 Equipamento de Ponto de Acesso para rede local sem fio com dois rádios, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac, 5GHz, e IEEE 802.11b/g/n, 2.4GHz.

2.15 Deve implementar a tecnologia 802.11ac Wave 2 MU-MIMO (Multi-User, Multiple Input, Multiple Output).

2.16 Os pontos de acesso deverão atender aos seguintes padrões, protocolos e funcionalidades:

i. IEEE 802.11a.
ii. IEEE 802.11b.
iii. IEEE 802.11g.
iv. IEEE 802.11n.
v. IEEE 802.11ac
vi. IEEE 802.11d.
vii. IEEE 802.3az.
viii. WPA® Enterprise/Personal.
ix. WPA2® Enterprise/Personal.
x. EAP-TLS.
xi. EAP-TTLS/MSCHAPv2.
xii. PEAPv0/EAP-MSCHAPv2.
xiii. PEAPv1/EAP-GTC.
xiv. EAP-SIM.
xv. EAP-FAST.
xvi. WMM® e WMM® Power Save.
xvii. Short Guard Interval (SGI) para canais de 20Mhz, 40Mhz, 80Mhz

2.17 Operar com canais de 20/40/80 para a frequência de 5GHz.

2.18 Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n e 801.11ac.

2.19 Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:

i. 802.11b: 1, 2, 5.5, 11
ii. 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
iii. 802.11n (2.4GHz): 6.5 to 300 (MCS0 até MCS15)
iv. 802.11n (5GHz): 6.5 to 450 (MCS0 to até MCS23)
v. 802.11ac: 6.5 to 1.300 (MCS0 to MCS9, NSS = 1 até 3 para VHT20/40/80)

vi. 802.11n high-throughput (HT) suportar: HT20/40
vii. 802.11n/ agregação de pacotes: A-MPDU, A-MSDU

2.20 Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão.

2.21 Operar nas seguintes tecnologias de rádio:

i. 802.11b: Direct-sequence spread-spectrum (DSSS)
ii. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)

2.22 Operar nos seguintes tipos de modulação:

i. 802.11b: BPSK, QPSK, CCK
ii. 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

2.23 Possuir capacidade de selecionar automaticamente o canal de transmissão - DFS.

2.24 Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.

2.25 Suportar até 255 clientes associados por rádio.

2.26 Possuir suporte a, pelo menos, 16 (dezesseis) SSIDs.

2.27 Permitir habilitar e desabilitar a divulgação do SSID.

2.28 Implementar diferentes tipos de combinações encriptação/autenticação por SSID.

2.29 Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras.

2.30 Deve ser capaz de classificar aplicações através de deep-packet inspection e bloquear acesso as aplicações identificadas.

2.31 Não deve haver licença restringindo o número de usuários por ponto de acesso.

2.32 Deve possuir antenas integradas ao equipamento, compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac com ganho de, pelo menos, 5 dBi e IEEE 802.11/b/g/n com ganho de, pelo menos, 3,5 dBi, com padrão de irradiação omnidirecional.

2.33 Deve suportar operação em 2x2:2 MIMO com diversidade espacial na frequência de 2.4Ghz.

2.34 Deve suportar operação em 3x3:3 MIMO com diversidade espacial na frequência de 5.0Ghz.

2.35 Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas.

2.36 Possuir potência máxima de transmissão de, no mínimo, +21 dBm para frequências de 2.4GHz.

2.37 Possuir potência máxima de transmissão de, no mínimo, +21 dBm para frequências de 5GHz.

2.38 Implementar a pilha de protocolos TCP/IP.

2.39 Suporte a IPv6.

2.40 Possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas.

2.41 Possuir LEDs multicoloridos indicativos do estado de operação, da atividade do rádio e da interface Ethernet.

2.42 Possuir ao menos uma interface de rede 10/100/1000BASE-T Ethernet (RJ-45) com as seguintes características:

i. Auto-sensing link speed and MDI/MDX.
ii. 802.3az Energy Efficient Ethernet (EEE).
iii. PoE-PD: 48 Vdc (nominal) 802.3af ou 802.3at.

2.43 Implementar VLANs conforme padrão IEEE 802.1Q.

2.44 Possuir botão que permita reset de fábrica do equipamento.

2.45 Possuir porta de console para gerenciamento e configuração via linha de comando CLI. Esta porta deverá ser dedicada e não será aceito o uso da interface de rede do item 2.44 acima, para o uso desta função.

2.46 Possuir trava padrão "Kensington security lock point" ou similar.

2.47 Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono).

2.48 Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível.

2.49 Implementar cliente DHCP para configuração automática de rede.

2.50 Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior.

2.51 Deve configurar-se automaticamente ao ser conectado na rede.

2.52 Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação.

2.53 Possuir kits de montagem opcionais para instalar o AP em variedade de superfícies.

2.54 Possuir mecanismo de reconhecimento de aplicações através de DPI (Deep Packet Inspection) permitindo a classificação para mais de 1400 aplicações.

2.55 Permitir o bloqueio da configuração do Ponto de Acesso via rede wireless.

2.56 Deve permitir controle de acesso e priorização de tráfego baseado em aplicações, tais como, Facebook, Office 365 e Skype.

2.57 Possuir mecanismo de prevenção a intrusão em redes WiFi (WIPS) oferecendo proteção contra ameaças e eliminando assim a necessidade de sensores dedicados a esse fim.

2.58 Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso, sem impacto no seu desempenho.

2.59 Deve possuir uma base de usuários interna que diferencie usuários visitantes de funcionários, para ser usada em autenticação 802.1x ou portal captivo.

2.60 Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através: MAC Address, 802.1x em base Local, Captive Portal, 802.1x em base externa RADIUS ou 802.1x em base externa LDAP.

2.61 Deve permitir a seleção/uso de servidor de autenticação específico com base no SSID.

2.62 Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS e PEAP-MSCHAPv2.

2.63 Permitir a integração com RADIUS Server com suporte aos métodos EAP citados.

2.64 Permitir a integração com LDAP.

2.65 Implementar WPA com algoritmo de criptografia TKIP e MIC.

2.66 Implementar WPA2 com algoritmo de criptografia AES 128, IEEE 802.11i.

2.67 Equipamento deverá possuir registro na ANATEL.

2.68 O certificado da ANATEL deverá ser apresentado no momento da habilitação.

2.69 Deve vir acompanhado de todas as licenças e softwares necessários, para atender a especificação deste documento, sem prazo para expirar, permitindo que os equipamentos continuem operacionais com todas as funcionalidades descritas neste objeto, mesmo após o término do período de suporte ou garantia.

2.70 Deve vir acompanhado com todas as licenças necessárias para total funcionamento com a controladora especificada no Lote 2 deste Termo.

2.71 Deve vir acompanhado com todas as licenças necessárias para total funcionamento com a solução de gerência especificada no Lote 2 deste Termo.

2.72 Não deve haver restrição de licença que limite o número de usuários por Ponto de Acesso.

2.73 Permitir a captura dos pacotes transmitidos na rede sem fio atuando como um “wireless sniffer” para fins de debug. Os pacotes capturados poderão ser armazenados no Ponto de Acesso ou exportados diretamente para softwares de terceiros que suporte arquivos com padrão “pcap”.

2.74 O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI.

2.75 O ponto de acesso deverá conectar-se ao controlador WLAN através de túnel seguro padrão IPsec ou através de protocolo de comunicação que ofereça controle total do equipamento.

2.76 Permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF.

2.77 Capacidade de selecionar faixas de frequências diferentes (2.4Ghz e 5Ghz) de acordo com as requisições dos clientes da rede sem fio se associem ao Ponto de Acesso.

3. PONTO DE ACESSO - TIPO 2

3.1 Equipamento deve possuir Rádio Bluetooth Low Energy (BLE) (Bluetooth de baixa energia) integrado que simplifica a gestão remota de uma rede alimentada por bateria em grande escala, enquanto também fornece localização avançada e sinalização interna, bem como capacidades de notificação push baseadas na proximidade.

3.2 O equipamento deve ser novo, sem uso anterior e o modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta, não sendo aceita solução em roadmap.

3.3 Não serão aceitas plataformas de gerenciamento em nuvem.

3.4 Deve ser fornecido com a versão mais recente (última versão comercial disponível) do software interno instalado.

3.5 O equipamento deve ser do mesmo fabricante dos demais equipamentos da solução, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

3.6 Deve permitir funcionamento em modo auto gerenciado, sem a necessidade de uma controladora de mobilidade, onde o próprio Ponto de Acesso pode operar como uma Controladora Virtual, seguindo no mínimo as seguintes características:

3.7 Deve suportar o agrupamento dos pontos de acesso, para operar em modo distribuído/colaborativo com suporte a pelo menos 60 (sessenta) Pontos de Acesso do mesmo modelo em um mesmo conjunto.

3.8 Deve suportar o atendimento de, no mínimo, 1.500 (um mil e quinhentos) dispositivos associados simultaneamente.

3.9 Deve permitir que o conjunto de pontos de acesso sejam atualizados de forma centralizada pela interface gráfica.

3.10 Deverá ser entregue todo o hardware e software necessário para suportar todas as quantidades e funcionalidades descritas.

3.11 Deve disponibilizar uma interface gráfica única e centralizada, acessível por browser padrão em página https, para configuração do conjunto de Pontos de Acesso (cluster).

3.12 Deve permitir funcionamento em modo gerenciado por controlador de mobilidade, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF.

3.13 Em modo gerenciado por controladora de mobilidade, o Ponto de Acesso deve ser capaz de criar tuneis distintos para encaminhando de trafego de gerência e encaminhamento de trafego dos dispositivos (Dados).

3.14 O túnel onde é encaminhado o trafego de gerência entre o Ponto de Acesso e a Controladora, deve suportar conexão segura IPSEC ou similar, garantindo integridade dos dados trafegados. Esta funcionalidade pode ser feita pelo Ponto de Acesso ou pelo controlador fornecido no Lote 2.

3.15 Equipamento de Ponto de Acesso para rede local sem fio com dois rádios, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac, 5GHz, e IEEE 802.11b/g/n, 2.4GHz.

3.16 Deve implementar a tecnologia 802.11ac Wave 2 MU-MIMO (Multi-User, Multiple Input, Multiple Output).

3.17 Os pontos de acesso deverão atender aos seguintes padrões, protocolos e funcionalidades:

i. IEEE 802.11a.
ii. IEEE 802.11b.
iii. IEEE 802.11g.
iv. IEEE 802.11n.
v. IEEE 802.11ac
vi. IEEE 802.11d.
vii. IEEE 802.3az.
viii. WPA® Enterprise/Personal.
ix. WPA2® Enterprise/Personal.
x. EAP-TLS.
xi. EAP-TTLS/MSCHAPv2.
xii. PEAPv0/EAP-MSCHAPv2.
xiii. PEAPv1/EAP-GTC.
xiv. EAP-SIM.
xv. EAP-FAST.
xvi. WMM® e WMM® Power Save.
xvii. Short Guard Interval (SGI) para canais de 20Mhz, 40Mhz, 80Mhz

3.18 Operar com canais de 20/40/80/160 para a frequência de 5GHz.

3.19 Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n e 801.11ac.

3.20 Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:

i. 802.11b: 1, 2, 5.5, 11
ii. 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
iii. 802.11n (2.4GHz): 6.5 to 300 (MCS0 até MCS15)
iv. 802.11n (5GHz): 6.5 to 600 (MCS0 to até MCS31)
v. 802.11ac: 6.5 to 1.700 (MCS0 to MCS9, NSS = 1 até 4 para VHT20/40/80)
vi. 802.11n high-throughput (HT) suportar: HT20/40/80/160
vii. 802.11n/ agregação de pacotes: A-MPDU, A-MSDU

3.21 Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão.

3.22 Operar nas seguintes tecnologias de rádio:

i. 802.11b: Direct-sequence spread-spectrum (DSSS)
ii. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)

3.23 Operar nos seguintes tipos de modulação:

i. 802.11b: BPSK, QPSK, CCK
ii. 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM

3.24 Possuir capacidade de selecionar automaticamente o canal de transmissão - DFS.

3.25 Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.

3.26 Suportar até 255 clientes associados por rádio.

3.27 Possuir suporte a pelo menos 16 SSIDs.

3.28 Permitir habilitar e desabilitar a divulgação do SSID.

3.29 Implementar diferentes tipos de combinações encriptação/autenticação por SSID.

3.30 Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras.

3.31 Deve ser capaz de classificar aplicações através de deep-packet inspection e bloquear acesso as aplicações identificadas.

3.32 Não deve haver licença restringindo o número de usuários por ponto de acesso.

3.33 Deve possuir antenas integradas ao equipamento, compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac com ganho de, pelo menos, 6 dBi e IEEE 802.11/b/g/n com ganho de, pelo menos, 3,5 dBi, com padrão de irradiação omnidirecional.

3.34 Deve suportar operação em 2x2:2 MIMO com diversidade espacial na frequência de 2.4Ghz.

3.35 Deve suportar operação em 4x4:4 MIMO com diversidade espacial na frequência de 5.0Ghz.

3.36 Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas.

3.37 Possuir potência máxima de transmissão de, no mínimo, +21 dBm para frequências de 2.4GHz.

3.38 Possuir potência máxima de transmissão de, no mínimo, +21 dBm para frequências de 5GHz.

3.39 Implementar a pilha de protocolos TCP/IP.

3.40 Possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas.

3.41 Possuir LEDs multicoloridos indicativos do estado de operação, da atividade do rádio e da interface Ethernet.

3.42 Possuir ao menos uma interface de rede 10/100/1000BASE-T Ethernet (RJ-45) com as seguintes características:

i. Auto-sensing link speed and MDI/MDX.
ii. 802.3az Energy Efficient Ethernet (EEE).
iii. PoE-PD: 48 Vdc (nominal) 802.3af ou 802.3at.

3.43 Implementar VLANs conforme padrão IEEE 802.1Q.

3.44 Possuir botão que permita reset de fábrica do equipamento.

3.45 Possuir porta de console para gerenciamento e configuração via linha de comando CLI. Esta porta deverá ser dedicada e não será aceito o uso da interface de rede do item 3.43 acima, para o uso desta função.

3.46 Possuir trava padrão "Kensington security lock point" ou similar.

3.47 Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono).

3.48 Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível.

3.49 Implementar cliente DHCP para configuração automática de rede.

3.50 Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior.

3.51 Deve configurar-se automaticamente ao ser conectado na rede.

3.52 Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação.

3.53 Possuir kits de montagem opcionais para instalar o AP em variedade de superfícies.

3.54 Possuir mecanismo de reconhecimento de aplicações através de DPI (Deep Packet Inspection) permitindo a classificação para mais de 1400 aplicações.

3.55 Permitir o bloqueio da configuração do Ponto de Acesso via rede wireless.

3.56 Possuir mecanismo de prevenção a intrusão em redes WiFi (WIPS) oferecendo proteção contra ameaças e eliminando assim a necessidade de sensores dedicados a esse fim.

3.57 Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n e 802.11ac para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso, sem impacto no seu desempenho.

3.58 Deve possuir uma base de usuários interna que diferencie usuários visitantes de funcionários, para ser usada em autenticação 802.1x ou portal captivo.

3.59 Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através: MAC Address, 802.1x em base Local, Captive Portal, 802.1x em base externa RADIUS ou 802.1x em base externa LDAP.

3.60 Deve permitir a seleção/uso de servidor de autenticação específico com base no SSID.

3.61 Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2.

3.62 Permitir a integração com RADIUS Server com suporte aos métodos EAP citados.

3.63 Permitir a integração com LDAP.

3.64 Implementar WPA com algoritmo de criptografia TKIP e MIC.

3.65 Implementar WPA2 com algoritmo de criptografia AES 128, IEEE 802.11i.

3.66 Equipamento deverá possuir registro na ANATEL.

3.67 O certificado da ANATEL deverá ser apresentado no momento da habilitação.

3.68 Deve vir acompanhado de todas as licenças e softwares necessários, para atender a especificação deste documento, sem prazo para expirar, permitindo que os equipamentos continuem operacionais com todas as funcionalidades descritas neste objeto, mesmo após o término do período de suporte ou garantia.

3.69 Deve vir acompanhado com todas as licenças necessárias para total funcionamento com a controladora especificada neste Termo.

3.70 Deve vir acompanhado com todas as licenças necessárias para total funcionamento com a solução de gerência especificada.

3.71 Não deve haver restrição de licença que limite o número de usuários por Ponto de Acesso.

3.72 Permitir a captura dos pacotes transmitidos na rede sem fio atuando como um “wireless sniffer” para fins de debug. Os pacotes capturados poderão ser armazenados no Ponto de Acesso ou exportados diretamente para softwares de terceiros que suporte arquivos com padrão “pcap”.

3.73 O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI.

3.74 O ponto de acesso deverá conectar-se ao controlador WLAN através de túnel seguro padrão IPsec ou através de protocolo de comunicação que ofereça controle total do equipamento.

3.75 Permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF.

3.76 Capacidade de selecionar faixas de frequências diferentes (2.4Ghz e 5Ghz) de acordo com as requisições dos clientes da rede sem fio se associem ao Ponto de Acesso.

4. SOFTWARE DE MONITORAMENTO E GERÊNCIA DA REDE SEM FIO

4.1 Deverá gerenciar todos os Pontos de Acesso especificados neste Termo no Lote 02 - Rede sem fio, de maneira centralizada.

4.2 Para adequada instalação da plataforma, compete à CONTRATADA, fornecer todos os acessórios necessários para completa operacionalização da ferramenta, tais como: licenças, mídias, kits/arquivos de instalação, documentações e manuais técnicos.

4.3 Deverá incluir todas as licenças necessárias para que a plataforma de gerência possa atender aos requisitos e funcionalidades técnicas.

4.4 Incluir, além das licenças específicas da plataforma de gerência, as licenças requeridas neste termo, de caráter permanente, por tempo indeterminado, permitindo que todas as funcionalidades e características da solução estejam operantes mesmo após a vigência do contrato ou garantia.

4.5 O software deverá permitir expansão gradual ou modular dos recursos de gerenciamento, mediante adição de novas licenças, tanto para gerência de um número maior de pontos de acessos quanto para incremento de usuários/clientes, visitantes e dispositivos.

4.6 Permitir o direcionamento de eventos e logs para um servidor de syslog.

4.7 Permitir acesso ao sistema de gerenciamento através de browser padrão por protocolo HTTPS.

4.8 Implementar SSH, HTTP/HTTPS e SSL.

4.9 Permitir a criação e distribuição dos arquivos de configuração dos equipamentos gerenciados na solução de rede sem fio.

4.10 Possibilitar configuração de templates para replicação das configurações entre equipamentos, permitindo realizar agendamento para aplicação do mesmo.

4.11 Realizar gerência das configurações, com armazenamento de versões e suporte a “rollback” das configurações.

4.12 Capacidade de configuração por interface gráfica completa dos recursos das controladoras e pontos de acesso.

4.13 Comparar as configurações das controladoras e as versões gravadas no sistema, identificando prováveis discrepâncias nos itens de configuração.

4.14 Armazenando pelo menos 5 perfis de configurações distintos.

4.15 Armazenar, por no mínimo 60 dias, os logs gerados pela solução.

4.16 Possibilidade de criação de grupos de equipamentos para realização de configurações específicas para cada grupo.

4.17 Capacidade de organização e gerenciamento hierárquico dos recursos, permitindo uma configuração em lotes e não de maneira individual.

4.18 Organização hierárquica de equipamentos em plantas, por andares, por prédios e por projetos.

4.19 Permitir a importação de plantas baixas nos seguintes formatos DWG, CAD, GIF e JPEG.

4.20 Permitir gerar projeto automatizado de redes sem fio nos padrões 802.11 ac, 802.11n, 802.11 a, 802.11b e 802.11g, utilizando as plantas baixas dos prédios, e os parâmetros de atenuação de cada item da planta. O software deverá considerar a área de cobertura e a banda por usuário desejada.

4.21 Permitir o cálculo e planejamento de rádio frequência (RF) para o adequado ajuste das quantidades e distribuições geográficas dos pontos de acesso na rede sem fio, levando em consideração a cobertura do sinal, qualidade, desempenho e banda por usuário.

4.22 Além da geração de projeto de cobertura de rede sem fio em planta baixa, permitir ainda, exibir planta de cobertura real (pós-ativação) com indicação gráfica da potência média para cada localização da planta e a distribuição física dos pontos de acesso.

4.23 Implementar recursos de descoberta automática dos dispositivos individuais da infraestrutura de rede sem fio.

4.24 Monitorar o desempenho da rede sem fio, consolidando informações de desempenho, tais como:

i. níveis de ruído
ii. relação sinal-ruído
iii. interferência e potência de sinal.

4.25 Representar o mapa lógico da rede sem fio, identificando e monitorando equipamentos, realizando o relacionamento dos eventos e estado operacional, com sinalização por cores.

4.26 Identificar eventos e alertas em tempo real, com indicação da severidade e separação por cores.

4.27 Possibilitar a configuração de alarmes.

4.28 Permitir o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede.

4.29 Identificação de áreas sem cobertura de sinal (coverage holes) com capacidade para efetuar os devidos ajustes para a correção automática das áreas de sombras.

4.30 Possibilitar a visualização de informações de clientes conectados à rede sem fio, tais como:

i. endereço IP.
ii. endereço MAC.
iii. nome do usuário.
iv. características das sessões (data, horário, duração da sessão, ponto de acesso associado).
v. SSID.
vi. canais utilizados.
vii. ponto de acesso.
viii. controladores aos quais está associado.
ix. dados de associação e de autenticação 802.1x.

4.31 Capacidade de listagem on-line da relação sinal-ruído de cada usuário, sua localização (tracking), endereço IP, endereço MAC e nível de potência de recepção.

4.32 Permitir a identificação de falhas no processo de autenticação/associação dos clientes na rede sem fio, para possibilitar a identificação de forma ágil na autorização de acesso dos usuários/clientes da rede sem fio.

4.33 Armazenar informações históricas sobre autenticação de usuários da rede sem fio, tanto da rede coorporativa (802.1x) como da rede visitante.

4.34 Deve implementar solução para localização dos elementos irradiantes presentes na área de cobertura da rede sem fio.

4.35 Capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID.

4.36 Detecção e localização e bloqueio de pontos de acesso não autorizados (rogues) e redes ad-hoc.

4.37 Identificação e geração de alertas para eventos indicativos de ataques na rede sem fio.

4.38 Capacidade de visualização em tela, elaboração de gráficos sumarizados das seguintes informações:

i. Listagem de clientes da rede sem fio.
ii. Listagem de pontos de acesso.
iii. Inventário.
iv. Informações de configuração das controladoras wireless.
v. Utilização da rede.
vi. Detalhes dos pontos de acesso estranhos detectados.

4.39 Criação de relatórios com as ameaças de segurança detectadas na rede sem fio.

4.40 Criação de relatórios que permitam filtrar as informações gerais da solução de rede sem fio, identificando e classificando dados relativos aos pontos de acessos, tais como:

i. Equipamentos.
ii. Usuários.
iii. Cobertura do sinal.
iv. Interferências.
v. Qualidade de sinal.
vi. Densidade de usuários por ponto de acesso.
vii. Clientes por SSID/ponto de acesso/região geográfica/protocolo de autenticação

4.41 Fornecimento de modelos de relatórios para geração automática ou possibilidade de criação específica de relatórios e filtros.

4.42 Deve implementar ferramentas de troubleshooting para análise de falhas nas conexões de clientes ou dispositivos com dificuldade de se conectarem à rede WiFi.

4.43 Permitir a estimativa sobre a localização geográfica, na planta baixa, de cliente/usuário/dispositivo conectado à rede sem fio.

4.44 Capacidade de desativação e reativação de determinada rede sem fio.

4.45 Permitir a configuração de administradores de recursos da rede sem fio com diferentes visões administrativas.

4.46 Deve permitir a criação de “Perfis” para os administradores da rede.

4.47 Deve ser possível que determinados usuários e administradores sejam associados a estes “Perfis” de forma que apenas tenham acesso ao gerenciamento e visualização dos elementos pertencentes ao “Domínio Virtual”.

4.48 Monitorar o desempenho da rede wireless, consolidando informações de cada ponto de acesso, tais como:

i. Níveis de sinal.
ii. Potência de sinal.
iii. Topologia da rede.
iv. Tempo de conexão.
v. VLAN utilizada.
vi. MAC Address.
vii. Endereço IP.
viii. Quantidade de clientes conectados e
ix. SSID/BSSID configuradas.

4.49 Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3.

4.50 A solução deve ser capaz de suportar sistemas MDM (Mobile Device Management).

4.51 Implementar protocolo de autenticação para controle do acesso administrativo à solução utilizando servidor Radius e auditoria de comandos com mecanismos de AAA.

4.52 Detectar, em conjunto com a controladora wireless e com o ponto de acesso, pelo menos, os seguintes ataques:

i. flood de frames de gerenciamento dos clientes da rede sem fio.
ii. flood de autenticação.
iii. ataque de deauthentication.
iv. Broadcast Disassociation.
v. Broadcast deauthentication.
vi. Spoofed MAC.

4.53 Gerenciar, de forma centralizada, a autenticação de usuários e dispositivos, permitindo a autenticação através dos seguintes métodos:

i. Local por tipo de usuário.
i. Local por tipo de dispositivo.
ii. Externa via RADIUS.
iii. Externa via LDAP.
iv. Externa via Windows Active Directory.
v. Certificado Digital.

4.54 A solução deverá implementar autenticação de dispositivos e usuários utilizando o padrão IEEE 802.1x, suportando pelo menos os seguintes métodos:

i. EAP.
ii. EAP-MD5.
iii. EAP-TLS.
iv. PEAP.

4.55 A solução deverá oferecer autenticação de usuários através de portal web seguro HTTPS com redirecionamento automático.

4.56 A solução deverá implementar autenticação específica para dispositivos por seu endereço MAC.

4.57 A solução deverá implementar validação de certificados digitais atendendo as seguintes caraterísticas:

i. Suportar o cadastramento de pelo menos duas CA (Certificate Authority) externos.
ii. Suportar consulta periódica da lista de revogados CRL (Certificate Revogation List) via HTTP.
iii. Suportar o protocolo OCSP para verificação do estado do certificado.

4.58 O sistema deverá permitir a criação de múltiplos usuários visitantes (guests), podendo atribuir privilégios de acesso distintos à rede sem fio.

4.59 A solução deverá permitir, durante a criação da conta de usuário visitante, a definição da validade temporal da conta e níveis de acesso.

4.60 Deverá permitir a customização do formulário com os campos e informações necessários para criação da conta de usuário visitante, tais como:

i. Nome.
ii. Sobrenome.
iii. E-mail.
iv. Empresa ou Órgão.
v. Telefone.
vi. Cargo.

4.61 A solução deverá fornecer, no mínimo, os seguintes modelos de criação de usuários visitantes (guest):

i. Criação de contas locais, através de usuário administrator específico da controladora wireless, com os seguintes requisitos.

ii. Criar conta individual.

iii. Criar contas em modo batch.

iv. Importar contas de arquivo ".csv".

v. Enviar senha via e-mail.

vi. Enviar senha via SMS.

vii. Definir a senha do visitante.

viii. Imprimir detalhes da senha.

4.62 Ver, editar ou suspender contas criadas pelo próprio autorizador, pelo mesmo grupo autorizador e por outros grupos autorizadores.

4.63 Estabelecer duração máxima da conta visitante.

4.64 Especificar o perfil de acesso à rede que será atribuído a conta visitante.

4.65 Permitir que grupos de usuários corporativos autorizados possam criar contas de usuários visitantes.

4.66 Permitir o direcionamento para página web, em servidor distinto, que forneça funcionalidade de criação de usuários visitantes (portal web e servidor AAA).

4.67 Plataforma de autocadastramento ou "Self-registration" que permita que o próprio usuário crie sua conta de visitante na rede sem fio, sem necessidade de autorizador, através dos seguintes procedimentos:

i. Envio da senha criada por e-mail.
ii. Envio da senha criada por SMS.
iii. Cadastramento através de contas pessoais das redes/mídias sociais.
iv. Cadastramento sem a necessidade de geração de senhas, apenas com o fornecimento de informações pessoais.

4.68 Deverá implementar um portal WEB seguro SSL a ser apresentado automaticamente aos usuários temporários (visitantes) durante a sua conexão com a rede (hotspot).

4.69 Deverá implementar as seguintes funções no Portal Web (hotspot):

i. Permitir a troca de senha do usuário visitante diretamente pelo portal seguro.
ii. Exigir somente no primeiro login o aceito do "Termo de uso dos recursos de rede do CJF".
iii. Customização da página de "Termo de uso dos recursos de rede do CJF".

4.70 Deverá implementar mecanismo de descobrimento automático e transparente de dispositivos que se conectam à rede wireless e cabeada, classificando-os em categorias, por exemplo:

i. Dispositivo Apple.
ii. Dispositivo Android.
iii. Impressora.

iv. Telefone IP.
v. Desktop.

4.71 Deverá implementar os seguintes mecanismos para coleta de informações do dispositivo a ser utilizada na classificação:

i. Coleta do tráfego DHCP.
ii. Coleta dos atributos RADIUS referente a sessão 802.1x do dispositivo.

4.72 Deverá possuir uma base de regras e categorias de políticas de dispositivos pré-configuradas.

4.73 Deverá possuir mecanismo de atualização da base de regras e políticas de dispositivos.

4.74 Deverá permitir que a classificação do dispositivo descoberto seja utilizada como parâmetro de autorização nas regras de admissão de dispositivos.

4.75 A solução deverá permitir a verificação da postura da estação/dispositivo através das seguintes formas:

i. Agente Instalado: Agente a ser instalado na estação do usuário para coleta das informações referentes à postura.
ii. Agente a ser carregado na estação, no momento de verificação, para coleta das informações referentes à postura.
iii. O agente deverá ser responsável somente pela verificação da postura da estação.
iv. O Agente (instalado ou temporário) deverá permitir a verificação dos seguintes itens:
a. Sistema Operacional Instalado.
b. Verificação do Service Pack Instalado.
c. Chaves do Registro do Windows.
d. Arquivos existentes na estação do usuário.
e. Status dos serviços que estão rodando na máquina.
f. Existência de Software Antivírus e AntiSpyware instalado.
g. Data da última atualização do Antivírus.
h. Status do software Antivírus (habilitado ou desabilitado).
i. Verificação do Hotfix do Windows instalado.

4.76 A solução deverá permitir a verificação da última versão de antivírus fornecida e sua respectiva data. Devem ser suportados os seguintes fabricantes de antivírus:

i. F-Secure.
ii. Symantec.
iii. Trend Micro.
iv. McAfee.

4.77 A solução deverá possuir base de dados com as informações de assinaturas de antivírus e Antispyware.

4.78 A solução deverá permitir o isolamento das estações mesmo sem a presença de agente instalado.

4.79 A solução deverá permitir o isolamento das estações que utilizem endereço IP estático.

4.80 Deve implementar funcionalidades de autenticação de visitantes suportando as seguintes características:

i. Deve possuir portal (Captive Portal) para acesso de visitantes em plataformas via web e específicas para smartfones e tablets.
ii. Deve permitir a customização (logos e banners) destes portais para prover interfaces amigáveis de acesso.
iii. Permitir realização de login por meio de redes sociais (social login) de pelo menos as seguintes redes: Facebook e Twitter.
iv. Permitir a configuração de credenciais de acesso de visitantes oriundos de texto SMS, e-mail e impressão.

4.81 Possuir mecanismos de se realizar o auto cadastro (self-registration) para criação de credenciais de acesso por parte do próprio visitante sem a utilização do sistema autenticação.

4.82 Caso tenha licenciamento específico, deverão ser fornecidas licenças de visitantes para 500 (quinhentos) dispositivos conectados simultaneamente.

4.83 Deve suportar integração com, no mínimo, uma das seguintes soluções de MDM: MobileIron e/ou Airwatch.

4.84 Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro.

4.85 Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes.

4.86 Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil.

4.87 Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas.

4.88 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv.

4.89 Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta.

4.90 Deve permitir que o visitante crie sua própria credencial temporária (“self-service”) através da portal web, sem a necessidade de um autorizador.

4.91 Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante.

4.92 Para a função de autosserviço, deve ser possível inserir e remover campos especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais de preenchimento.

4.93 Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha.

4.94 Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login.

4.95 Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail e impressão local.

4.96 Deve suportar integração com, no mínimo, uma das seguintes soluções de Firewall: FortiGate, Cisco Firepower, Check Point, Palo Alto, SonicWALL.

5. TAGS DE LOCALIZAÇÃO BLE (BLUETOOTH LOW ENERGY)

5.1 As tags de localização deverão suportar a tecnologia Bluetooth Low Energy (BLE) (Bluetooth 4.0 ou superior), fornecendo dados de localização para cada equipamento móvel do CJF móvel, dentro do alcance dos APs habilitados para BLE.

5.2 A solução deverá ser compatível com os Pontos de Acessos Tipo 1 e Tipo 2 fornecidos no Lote 2.

5.3 Deve ser fornecida bateria, tipo moeda, para cada tag de localização, suficiente para 3 (três) anos de uso, no mínimo.

5.4 Deve trabalhar na frequência 2.4 Ghz.

5.5 Deve possuir adesivo externo de alta resistência.

5.6 Deve possuir peso máximo de 15g.

5.7 Deve funcionar numa temperatura entre 0ºC a 45ºC.

5.8 Deve suportar umidade relativa de 5% a 90% sem condensação.

5.9 Deve ser conforme com os regulamentos CE, R&TTE 1995/5/EC, diretiva de baixa tensão 72/23/EEC.

6. SOFTWARE DE CONTROLE DE ACESSO DE USUÁRIO

No que se refere a proteção contra acessos não autorizados, a solução de controle de acesso deve implementar políticas que garantam que cada perfil de usuário e dispositivo tenha acesso somente aos recursos necessários a sua operação, bloqueando qualquer outro tipo de acesso não relacionado com sua atividade, de forma a minimizar possibilidade a ocorrência de vazamentos devido à acessos não autorizados, situações acidentais ou ilícitas. Além disso, todos os acessos à rede deverão ser registrados, permitindo identificar o usuário e dispositivo associados à uma conexão, auxiliando em processos de investigação de incidentes.

A lei geral de proteção de dados (LGPD) requer também, dentro das boas práticas de segurança e da governança, que a organização conte com planos de resposta a incidentes e remediação. A solução de controle de acesso deverá interagir com as demais ferramentas de segurança para proporcionar resposta rápida a incidentes de segurança detectados por estas ferramentas, agindo diretamente na camada de acesso da rede para minimizar a probabilidade de disseminação de ameaças na rede.

6.1 Deverá ser fornecida uma solução de autenticação de usuários e dispositivos para controle de acesso a rede, baseada em appliance físico ou virtual, do mesmo fabricante dos demais equipamentos da solução do Lote 2, compondo uma solução única de rede, para assegurar a compatibilidade funcional de todos os recursos e permitir o gerenciamento unificado.

6.2 Não será aceita solução baseada em nuvem (cloud).

6.3 Deve ser fornecido com a versão mais recente (última versão comercial disponível) do software interno instalado.

6.4 Deve ser totalmente compatível com os Pontos de Acesso e Controladora especificados neste Termo.

6.5 Deve fornecer todos os softwares operacionais e de apoio que sejam necessários para a solução de controle de acesso.

6.6 Todos os softwares (gerenciamento, operacional e de apoio) devem ser fornecidos devidamente licenciados e com a chave de ativação.

6.7 Deve fornecer licenças de uso permanente (perpétua) de todos os softwares que compõem a solução proposta, em suas versões mais recentes, sem previsão de descontinuidade, na data de entrega da proposta.

6.8 Deverão ser fornecidas licenças para 1.000 (mil) dispositivos conectados simultaneamente.

6.9 O licenciamento da solução completa deve permitir a continuidade do uso pela CONTRATANTE, em caráter permanente, mesmo após o término do contrato, inclusive sem restrições à futura utilização para atendimento a eventuais novas demandas.

6.10 Deve suportar a configuração redundante em alta disponibilidade utilizando um outro appliance virtual do mesmo modelo ofertado.

6.11 Deve implementar funcionalidade de classificação automática de dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede.

6.12 Deve classificar, no mínimo, por categoria (Ex. Computador, Smartdevice, Impressora e Câmera), por sistema operacional e tipo de dispositivo (Ex. Android, Apple).

6.13 Deve suportar coleta de informações para classificação usando, no mínimo, DHCP, HTTP User-Agent, MAC OUI, SNMP, Sflow, Netflow, IF-MAP e TCP Fingerprinting.

6.14 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com, no mínimo, as seguintes informações:

i. Atributos do usuário autenticado.
ii. Hora do dia, dia da semana.
iii. Tipo de dispositivo utilizado.
iv. Localização do usuário.
v. Tipo de autenticação utilizado.

6.15 Deve possuir interface para construção de regras e categorias customizadas de classificação de dispositivos.

6.16 Deve permitir que o administrador cadastre manualmente um determinado dispositivo em uma categoria.

6.17 Deve possuir base de regras e categorias de dispositivos pré-configurada.

6.18 Deve suportar mecanismo de atualização das regras e categorias pré-configuradas.

6.19 Possuir recursos integrados de AAA, permitindo que a solução possa ser utilizada como plataforma de autenticação (RADIUS).

6.20 Deve possuir suporte a TACACS+

6.21 Possuir Autoridade Certificadora (CA – Certification Authority) integrada, para geração de certificados para os dispositivos que forem se autenticar na rede.

6.22 Deve suportar integração com bases de dados de usuários do tipo LDAP, Active Directory e SQL.

6.23 Deve possuir suporte à “Single Sign-On” (SSO) através de SAML v2.0.

6.24 Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários.

6.25 Suportar administração através de IPv6.

6.26 Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única dashboard, tais quais:

i. Data e Hora.
ii. Mac Address e classificação do dispositivo.
iii. Usuário.
iv. Equipamento que requisitou a autenticação (origem), método de autenticação utilizado (meio) e entidade de autenticação utilizada para validação (destino).
v. Perfil de acesso aplicado.

6.27 Todos os atributos de entrada do protocolo utilizados na requisição (ex. RADIUS).

6.28 Informações de resposta da solução para o elemento de rede requisitante e alertas em caso de falha.

6.29 Deve possuir dashboard customizável, permitindo a visualização de, no mínimo, as seguintes informações:

i. Listagem dos últimos alertas do sistema.
ii. Listagem das últimas tentativas de autenticação e autenticações com sucesso.
iii. Gráfico com categorização dos dispositivos classificados, divididos de acordo com as categorias classificativas.

6.30 Deve implementar funcionalidades de NAC (network Access Control), suportando as seguintes características:

i. Suporte de agente persistente para no mínimo, versões operacionais em Windows 10, Windows 7 e Mac OS.
ii. Suporte a checagem de “saúde” dos dispositivos.
iii. Suporte a controle de aplicativos nos dispositivos com agente persistente como: Aplicações instaladas, checagem de antivírus, checagem de status do firewall e habilitar e desabilitar portas USB.
iv. Suporte a remediar ou mover os dispositivos para a quarentena com base nas informações de checagem de postura dos dispositivos.

6.31 Caso exija licenciamento específico, deverão ser fornecidas licenças de NAC para 1.000 (mil) dispositivos conectados simultaneamente.

6.32 Todas licenças deverão ser permanentes e perpétuas.

6.33 Deve ser fornecido, no mínimo, 1.000 (mil) licenças que suporte as funções de autenticação via 802.1x e acesso guest.

ANEXO II DO CONTRATO - CRONOGRAMA DE IMPLANTAÇÃO DA SOLUÇÃO

LOTE 1 E LOTE 2

ETAPA 1 - ENTREGA DOS EQUIPAMENTOS E SOFTWARES DA SOLUÇÃO

Prazo Máximo (em dias corridos)	**Descrição**	**Responsável**
D	Assinatura do Contrato.	CJF
D + 3	Reunião de Planejamento.	CJF e CONTRATADA
D + 30	Concluir a entrega dos equipamentos, softwares e acessórios e demais documentos.	CONTRATADA
TRP	Emitir o **Termo de Recebimento Provisório (TRP)** após a entrega dos equipamentos, softwares e acessórios da solução. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE.	CJF
Data de Emissão do TRP + 10	Conferência da entrega dos equipamentos, softwares e acessórios e demais documentos.	CONTRATADA
TRD	Emitir o **Termo de Recebimento Definitivo (TRD),** desde que não haja pendências a cargo da CONTRATADA.	CJF

Observações:

- D = data da assinatura do contrato contratual.
- TRP = Emissão do Termo de Recebimento Provisório pelo CJF, se não houverem pendências a cargo da CONTRATADA.
- TRD = Data de emissão do Termo de Recebimento Definitivo pelo CJF, se não houverem pendências a cargo da CONTRATADA.

ETAPA 2 – INSTALAÇÃO, CONFIGURAÇÃO, MIGRAÇÃO E TRANSFERÊNCIA DE CONHECIMENTO DA SOLUÇÃO

Prazo Máximo (em dias corridos)	**Descrição**	**Responsável**
D	Data de emissão de ordem de serviço – OS para início do serviço de instalação e configuração da solução	CJF e CONTRATADA
D + 10	Entregar o Plano de Instalação contendo o planejamento detalhado das atividades necessárias para a instalação, configuração, migração, organização do cabeamento e transferência de conhecimento da solução.	CONTRATADA
D + 15	Comprovar que os técnicos que executarão as atividades	CONTRATADA

	de instalação, configuração, migração e organização do cabeamento possuem as certificações exigidas.	
TRP	Emitir o **Termo de Recebimento Provisório (TRP)** após a entrega e aprovação do Plano de Instalação. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE.	CJF
Data de Emissão do TRP + 90	Concluir no prazo de 90 (noventa) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, o serviço de instalação, configuração, migração, organização do cabeamento e transferência de conhecimento da solução, realizando todas as atividades programadas para esta etapa.	CONTRATADA
TRD	Emitir o **Termo de Recebimento Definitivo (TRD)** após a finalização do serviço instalação, configuração, organização do cabeamento e transferência de conhecimento da solução, acompanhado da documentação técnica detalhada de todas as atividades executadas, desde que não haja pendências a cargo da CONTRATADA.	CJF
Data de Emissão do TRD + 30	Realizar o acompanhamento ON-SITE da operação da solução, esclarecendo dúvidas e realizando ajustes na configuração dos componentes de hardware e software, visando à melhor utilização dos recursos disponíveis na solução.	CONTRATADA

Observações:

- D = data da assinatura do contrato contratual.
- TRP = Emissão do Termo de Recebimento Provisório pelo CJF, se não houverem pendências a cargo da CONTRATADA.
- TRD = Data de emissão do Termo de Recebimento Definitivo pelo CJF, se não houverem pendências a cargo da CONTRATADA.

ANEXO III DO CONTRATO - PLANILHAS DE COMPOSIÇÃO DE CUSTOS

aquisição de solução de infraestrutura de redes de dados

Item	Descrição	Quantidade	Quantidade de meses	Preço unitário	Total
Lote 1					
1.1	Switch Acesso Tipo 1	27	-	R$ 20.631,61	R$ 557.053,47
1.2	Suporte SW Tipo 1	27	60	R$ 2.900,88	R$ 174.052,80
1.3	Switch LEAF Tipo 2	2	-	R$ 200.681,21	R$ 401.362,42
1.4	Suporte SW Tipo 2	2	60	R$ 2.389,48	R$ 143.368,80
1.5	Switch SPINE Tipo 3	2	-	R$ 177.582,42	R$ 355.164,84
1.6	Suporte SW Tipo 3	2	60	R$ 2.250,98	R$ 135.058,80

1.7	Switch SAN Tipo 4	2	-	R$ 122.039,19	R$ 244.078,38
1.8	Suporte SW Tipo 4	2	60	R$ 1.559,16	R$ 93.549,60
1.9	Serviço instalação lote 1	1	-	R$ 127.404,00	R$ 127.404,00
1.10	Rack de rede	1	-	R$ 6.712,90	R$ 6.712,90
1.11	Patch Cord 1,5m	500	-	R$ 47,15	R$ 23.575,00
1.12	Patch Cord 2,5m	500	-	R$ 63,66	R$ 31.830,00
1.13	Software de gerência de Rede LAN	1	-	R$ 140.404,34	R$ 140.404,34
1.14	Transferência de conhecimento lote 1	4	-	R$ 3.051,25	R$ 12.205,00
				Total Lote 1	**R$ 2.445.820,35**

Lote 2					
Item	**Descrição**	**Quantidade**	**Quantidade de meses**	**Preço unitário**	**Total**
2.1	Controladora rede sem fio	1	-	R$ 16.992,00	R$ 16.992,00
2.2	Suporte controladora	1	60	R$ 56,18	R$ 3.370,80
2.3	Ponto de Acesso Tipo 1	50	-	R$ 4.049,56	R$ 202.478,00
2.4	Suporte AP Tipo 1	50	60	R$ 535,00	R$ 32.100,00
2.5	Ponto de Acesso Tipo 2	5	-	R$ 4.117,31	R$ 20.586,55
2.6	Suporte AP Tipo 2	5	60	R$ 80,05	R$ 4.803,00
2.7	Serviço instalação lote 2	1	-	R$ 42.593,77	R$ 42.593,77
2.8	Software de gerência e controle de acesso	-	-	R$ 81.910,14	R$ 81.910,14
2.9	Tags bluetooth (BLE)	50	-	R$ 627,41	R$ 31.370,50
2.10	Software de gerência Tags BLE	1	-	R$ 197.440,32	R$ 197.440,32
2.11	Transferência de conhecimento lote 2	4	-	R$ 2.248,41	R$ 8.993,64
				Total Lote 2	**R$ 642.638,72**

Total Geral	**R$ 3.088.459,07**

Autenticado eletronicamente por **Frederico Samartini Queiroz Alves**, **Usuário Externo**, em 26/11/2019, às 15:55, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Autenticado eletronicamente por **Gabrielly Andressa Nagy**, **Usuário Externo**, em 26/11/2019, às 15:55, conforme art. 1º, §2º, III,

b, da Lei 11.419/2006.

Autenticado eletronicamente por **Juíza Federal SIMONE DOS SANTOS LEMOS FERNANDES**, **Secretária-Geral**, em 26/11/2019, às 19:48, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0081441** e o código CRC **338694EC**.