TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Praça Desembargador Edgard Nogueira. S/Nº - Centro Civico - Bairro Cabral - CEP 64000920 - Teresina - PI

ANÁLISE DE VIABILIDADE 32/2020 - SEINF

1. IDENTIFICAÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

SOLUÇÃO DE TI	
NOME DA SOLUÇÃO DE TI:	Aquisição de solução para rede sem fio
ÁREA DEMANDANTE:	CODIN
E-MAIL DO DEMANDANTE:	antonio.sousa@tre-pi.jus.br
TELEFONE DO DEMANDANTE:	86 2107 9762

2. DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

O Tribunal Regional Eleitoral do Piauí adquiriu, em 2016, solução de rede sem fio para implantação em sua Sede e Anexo, que veio a se mostrar bastante versátil e se tornou ferramenta de uso diário pelos servidores, colaboradores e visitantes.

Sua criação deu fim à prática disseminada de se conectar indiscriminadamente roteadores wi-fi na rede de computadores do TRE-PI para a criação de pequenas redes sem fio com áreas de alcance curtas. Na maioria dos casos, esses equipamentos eram utilizados sem qualquer conhecimento da Secretaria de Tecnologia da Informação e ofereciam um elevado risco à segurança da rede de computadores da Justiça Eleitoral.

Essa aquisição também permitiu a conformidade do Tribunal com a Resolução 211/2015 do Conselho Nacional de Justiça, quando esta determina em seu art. 24 que :

> Art. 24. O nivelamento da infraestrutura de TIC deverá obedecer aos seguintes requisitos mínimos:
> [...]
> XIII - rede sem fio para a promoção dos serviços ofertados aos usuários e respeitando a política da informação de cada órgão, sempre que possível.

A solução adquirida é composta por uma controladora física e 30 pontos de acesso (AP - *Access Points*), dos quais 19 (dezenove) foram instalados no edifício Sede e Anexo; 06 (seis) na Central de Atendimento ao Eleitor da capital; e outros 05 (cinco) foram implantados em cartórios eleitorais do interior do Estado em projeto piloto para verificar a viabilidade técnica de sua implantação nas Zonas Eleitorais.

No entanto, passados 04 anos desde sua implantação, os equipamentos adquiridos estão sem cobertura de suporte e garantia. A controladora da rede sem fio, por exemplo, já apresentou problemas, ficando alguns dias sem funcionar. Isso mostrou que o cenário atual é suscetível à incidentes por não possuir redundância.

A sua substituição por uma controladora virtual proverá à solução resiliência em relação a falhas, passando a depender unicamente da infraestrutura de virtualização do Tribunal, o que por si só já garantirá a alta disponibilidade almejada.

Também se faz necessária a aquisição de novos Pontos de Acesso. Como dito acima, os APs adquiridos foram todos utilizados e não possuem suporte/garantia vigentes, não sendo possível sua substituição em caso de falhas.

3. REQUISITOS DE NEGÓCIO

3.1 – Requisitos funcionais (Necessidades de negócio)

NECESSIDADE 1				
Possibilitar a criação de rede wi-fi com controladora virtual				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Permitir a centralização da manutenção, configuração e otimização dos pontos de acesso gerenciados otimizando o desempenho e a cobertura da radiofrequência (RF)	1	Integrante Demandante	CODIN
2	Possuir compatibilidade com VMware vSphere ESXi	1	Integrante Demandante	CODIN
3	Prover o gerenciamento centralizado dos Pontos de Acesso através de Endereço IP, Range de IPs e/ou Sub-Redes pré-configuradas	1	Integrante Demandante	CODIN
4	Deve permitir que as configurações sejam aplicadas em vários pontos de acesso selecionados simultaneamente, isto é, não será permitido soluções que necessitem configurar os pontos de acesso individualmente	1	Integrante Demandante	CODIN

NECESSIDADE 2

Garantir a segurança da comunicação sem fio				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP	1	Integrante Demandante	CODIN
2	Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento	1	Integrante Demandante	CODIN
3	Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa	1	Integrante Demandante	CODIN
4	Implementar os principais padrões de segurança wireless, como: WPA, WPA2, TKIP, AES, IEEE 802.1x, IEEE 802.11I, IEEE 802.11w	1	Integrante Demandante	CODIN
5	Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless)através: MAC Address, Autenticação Local, Captive Portal, Active Directory, RADIUS, IEEE 802.1x e LDAP	1	Integrante Demandante	CODIN
6	Deverá implementar tagging de VLANs através do protocolo 802.1q	1	Integrante Demandante	CODIN

NECESSIDADE 3				
Garantir flexibilidade na criação e manutenção de redes sem fio				
ID	**FUNCIONALIDADE**	**ID**	**RESPONSÁVEL**	**ÁREA**
1	Deverá implementar disponibilidade de SSID baseado em dia da semana/hora, permitindo ao administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia da semana determinados	1	Integrante Demandante	CODIN
2	Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x	1	Integrante Demandante	CODIN
3	Deverá suportar agrupamento de APs	1	Integrante Demandante	CODIN
4	A solução deverá suportar a criação de uma zona ou rede de visitantes	1	Integrante Demandante	CODIN

3.2 – Requisitos não-funcionais

ID	**TIPO**	**REQUISITO**
1	Requisitos de capacitação	Não se aplica.
2	Requisitos Legais	Devem-se observar as normas: 1. Lei n° 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública; 2. Lei n° 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação; 3. Decreto n° 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal e faz exigência contratual de comprovação da origem dos bens importados oferecidos pelos licitantes e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa 4. Resolução CNJ nº 182 de 17 de outubro de 2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ); 5. Resolução TSE nº 23.234, de 15 de abril de 2010, que dispõe sobre regras e diretrizes para a contratação de serviços no âmbito da Justiça Eleitoral; 6. Orientação Técnica n° 01 TiControle, de 12 de março de 2008, que dispõe sobre boas práticas para a estimativa de preços na contratação de bens e serviços de TI; 7. Resolução TRE-PI nº 356/2017, de 19 de dezembro de 2017, que estabelece a Política de Segurança da Informação (PSI) do Tribunal Regional Eleitoral do Piauí; 8. Lei nº 10.520/2002; 9. Instrução Normativa nº 5, de 27 de Junho de 2014 e demais normas pertinentes.
3	Requisitos de Manutenção	A manutenção em garantia poderá ser realizada pelo fabricante, porém, sendo responsabilidade subsidiaria da CONTRATADA. A CONTRATADA deverá informar o número do chamado e disponibilizar um meio de acompanhamento do seu estado. A manutenção deverá cobrir todas as peças e componentes mecânicos e eletrônicos substituídos, decorrentes de manutenção corretiva, deverá apresentar padrões de qualidade e desempenho iguais ou superiores aos

		utilizados na fabricação do equipamento, sendo sempre novos e de primeiro uso, durante todo o período de garantia técnica. O serviço de suporte técnico à solução fornecida e implementada se destina a correção de problemas e esclarecimento de dúvidas sobre configuração e utilização da solução ofertada. Os serviços serão solicitados pela equipe técnica do Tribunal mediante abertura de chamado junto à CONTRATADA, via chamada telefônica local ou gratuita, e-mail ou sítio web. As atualizações e upgrades de software e firmware devem ser disponibilizadas à CONTRATANTE para download no site da CONTRATADA ou do fabricante. Ocorrendo problemas técnicos ou físicos com os equipamentos cuja recuperação ao status operacional fique prejudicada, durante a vigência contratual, a contratada deverá substituir os equipamentos envolvidos. Todas as especificações técnicas a seguir devem estar plenamente disponíveis nos equipamentos a serem fornecidos pela empresa contratada, sem necessidade de quaisquer outras aquisições, tais como licenças, peças ou dispositivos complementares. As únicas exceções a essa prerrogativa são os itens em que estão claramente descritas capacidades de expansão da solução. Caso os equipamentos e softwares fornecidos requeiram licenciamento para atender aos requisitos deste termo de referência, todas as licenças necessárias deverão ser entregues, instaladas e ativadas em caráter permanente e contínuo, de forma que a solução funcione mesmo após o término da garantia exigida Todos os equipamentos, produtos, peças ou softwares necessários à contratação deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Já os softwares comerciais deverão, ainda, ser entregues em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço
4	Requisito Temporal	O prazo máximo para entrega dos produtos/equipamentos deverá ser de 30 (trinta) dias corridos, contados a partir do recebimento, pela Contratada, da ordem de fornecimento
5	Requisitos de Segurança da Informação	A CONTRATADA se obriga a conhecer e observar a Política de Segurança da Informação do TRE. A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços contratados ou da relação contratual mantida com o TRE-PI, abstendo-se de divulgá-los a terceiros sob qualquer pretexto, a menos que prévia e formalmente autorizado pelo TRE-PI. A solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações do TRE-PI por ela gerenciadas e armazenadas Os dispositivos de armazenamento substituídos em função de troca em garantia, ou ficarão retidos na Contratante até seu pagamento, ou somente serão devolvidos após sua inutilização completa. A devolução do componente inutilizado ou desmagnetizado ficará a critério exclusivo da CONTRATANTE, sem gerar direitos à CONTRATADA. A CONTRATADA não poderá armazenar consigo qualquer documento técnico que contemple configurações e regras de segurança aplicadas nos equipamentos implantados na rede da CONTRATANTE. A CONTRATADA responderá solidariamente com seus agentes empregados, prepostos, ou subcontratados, no caso de violação do compromisso de confidencialidade ora assumido. O TRE-PI terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação. Os equipamentos que vierem a ser substituídos deverão, sempre que possível, ter suas configurações apagadas.
6	Requisitos Sociais, Ambientais e Culturais	Os materiais, objetos deste Termo deverão seguir, no que couberem, a Instrução Normativa n° 1 de 19 de janeiro de 2010 do Ministério do Planejamento, Orçamento e Gestão e Decreto 7.746/2012), seguindo os seguintes critérios de sustentabilidade ambiental: a) Os materiais deverão ser, preferencialmente, acondicionados em embalagem individual adequada, preferencialmente a base de papel, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento. b) Não serão aceitos, em hipótese alguma, fardos, caixas ou frascos violados ou com outros danos que prejudiquem o acondicionamento e a qualidade do produto ou que causem vazamento e os lacres e selos de segurança das embalagens e frascos deverão estar de acordo com as normas pertinentes, inclusive contendo informações quanto as suas características na embalagem. c) O materiais não poderão conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenilpolibromados (PBDEs).

		Os equipamentos novos e de primeiro uso, deverão ser entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos; Os manuais devem estar em língua inglesa e/ou portuguesa. Os manuais poderão ser entregues em meio digital ou disponibilizados para *download*.
7	Requisitos de Desempenho	Definidos nas especificações dos requisitos tecnológicos

3.3 – Requisitos tecnológicos

ID	TIPO	REQUISITO
1	Requisitos da Arquitetura Tecnológica	**SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO (SGC)** **Características Gerais** 1. Deve ser na forma de appliance virtual; 2. Deve possibilitar a centralização da manutenção, configuração e otimização dos pontos de acesso gerenciados otimizando o desempenho e a cobertura da radiofrequência (RF); 3. Deve ser compatível com VMware vSphere ESXi; 4. Deverá ser compatível com sistema operacional CentOS versão 7 ou superior, caso contrário, deverão ser fornecidas as licenças do sistema operacional utilizado com suporte e atualizações por um período de 60 (sessenta) meses; 5. Deve ser compatível com banco de dados MySQL ou PostgreSQL, caso contrário, deverão ser fornecidas as licenças do sistema operacional utilizado com suporte e atualizações por um período de 60 (sessenta) meses; 6. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac, compatíveis com os demais itens desse termo; 7. Deve possuir suporte e atualizações por um período de 60 (sessenta) meses, para todos os itens que sejam fornecidos para compor a solução incluindo, mas não se limitando a servidores, sistemas operacionais, softwares de bancos de dados e qualquer componente ou software adicional que venha a fazer parte da solução oferecida **Gerenciamento** 1. Capacidade para gerenciar no mínimo 1000 (mil) Pontos de Acesso mediante adição de licenças; 2. Suportar 20.000 (Vinte mil) clientes wireless simultâneos; 3. Prover o gerenciamento centralizado dos Pontos de Acesso através de Endereço IP, Range de IPs e/ou Sub-Redes pré-configuradas. 4. Deve permitir que as configurações sejam aplicadas em vários pontos de acesso selecionados simultaneamente, isto é, não será permitido soluções que necessitem configurar os pontos de acesso individualmente; 5. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF); 6. A SGC poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento nível 3 da camada OSI; 7. Possibilitar a configuração de envio dos eventos dos Pontos de Acesso ou da SGC para um servidor de Syslog remoto; 8. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3,incluindo a geração de traps SNMP; 9. Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento; 10. Permitir a visualização de alertas da rede sem fio em tempo real; 11. Implementar no mínimo dois níveis de acesso administrativo à SGC (apenas leitura e leitura/escrita) protegidos por senhas independentes; 12. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador; 13. Permitir a configuração e gerenciamento através de browser padrão (HTTPS) ou porta console; 14. Gerenciar de forma centralizada a autenticação de usuários na integração com servidores AAA (Radius) ou LDAP; 15. Permitir o envio de notificações através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS); 16. Permitir que o processo de atualização de versão seja realizado através de browser padrão(HTTPS) ou SSH; 17. 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; 18. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa; 19. Deverá implementar disponibilidade de SSID baseado em dia da semana/hora, permitindo ao administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia da semana determinados; 20. Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível; 21. Possuir ferramenta que permita o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede da SGC ou dos Pontos de Acesso;

22. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de browser padrão (HTTPS) ou FTP ou TFTP;
23. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede wireless;
24. Monitorar o desempenho da rede wireless, permitindo a visualização de informações de cada ponto de acesso;
25. A falha de comunicação entre SGC e os Pontos de Acesso não devem interferir na operação dos Pontos de Acesso e o chaveamento entre instâncias deve ser automático entre os SGCs;
26. Deverá efetuar compartilhamento de recursos e licenças de pontos de acesso entre os SGCs participantes da solução;
27. Deverá em caso de falha realizar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede.
28. Deverá possuir a capacidade de geração de informações ou relatórios de no mínimo os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;
29. Deverá suportar a identificação de aplicações dos clientes conectados ao ponto de acesso, permitindo o controle de banda para estas aplicações;
30. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos;
31. Deverá possibilitar a importação de plantas baixas nos formatos dwg ou jpg ou png, devendo permitir a visualização dos Pontos de Acesso instalados, com seu estado de funcionamento;
32. Implementar funcionalidade de análise espectral, permitindo a detecção de interferências no ambiente de rede sem fio;
33. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando no mínimo os 5 itens mais usados;
34. Deverá suportar protocolo LLDP;
35. Deverá suportar a identificação de aplicações dos clientes conectados ao ponto de acesso;
36. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos;
37. Deverá permitir o acréscimo unitário de licenças para expansão da capacidade dos Pontos de Acesso ou cada Pontos de Acesso deve vir acompanhado de sua licença;
38. As licenças instaladas na SGC deverão ser livres e facilmente migradas para outra SGC da mesma solução em uma eventual troca;
39. As licenças devem ser compartilhadas entre os SGCs, sem a necessidade de adquirir uma licença para cada SGC;
40. Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;
41. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
42. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF deforma automática;
43. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos, para otimizar a performance;
44. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso;
45. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado;
46. Deve possuir funcionalidade que permita a utilização dos pontos de acesso em sites remotos, onde através de conexão pela internet este automaticamente estabeleça um túnel seguro até a SGC permitindo que os SSIDs corporativos sejam disponibilizados aos usuários;
47. Deve permitir a criação de um SSID local, que efetue a conexão direta via internet, sem a utilização do túnel seguro. Caso esta funcionalidade necessite de licenças adicionais, estas deverão estar contempladas para totalidade da capacidade da SGC;
48. Deve permitir o tunelamento seguro do tráfego de dados dos usuários da rede wi-fi na WLAN por meio de túneis seguros com suporte para NAT.

Rede

1. Deverá implementar suporte aos protocolos IPv4 e IPv6;
2. Deverá implementar tagging de VLANs através do protocolo 802.1q;
3. Suportar a configuração de no mínimo 4000 (quatro mil) VLANs;
4. Deverá oferecer os recursos de mobilidade para roaming de camada L2 ou L3;
5. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x;
6. Deverá suportar agrupamento de APs, e no mínimo, 512 (quinhentos e doze) grupos de APs simultâneos;
7. Deverá permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID;
8. Em caso de falha de comunicação entre os pontos de acesso e a SGC, os usuários associados à rede sem fios devem continuar conectados com acesso à rede. Também deve permitir que novos usuários se associem à rede sem fios utilizando autenticação do tipo 802.1xmesmo que os pontos de acesso estejam sem comunicação com a SGC;
9. Deve permitir o uso de voz e dados em cima de um mesmo SSID;
10. Suportar 802.11e;
11. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID;
12. Deverá permitir a configuração de prioridade de um determinado SSID sobre os outros SSID’s;
13. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de

autenticação;

Segurança

1. Deverá implementar, pelo menos, os seguintes padrões de segurança wireless:
   - (WPA) Wi-Fi Protected Access;
   - (WPA2) Wi-Fi Protected Access;
   - (TKIP) Temporal Key Integrity Protocol;
   - (AES) Advanced Encryption Standard;
   - IEEE 802.1x;
   - IEEE 802.11i;
   - IEEE 802.11w.
2. Deverá implementar, pelo menos, os seguintes controles/filtros:
   - L2 – Baseado em MAC Address e Client Isolation
   - L3 – Baseado em Endereço IP;
   - L4 – Baseado em Portas TCP/UDP
3. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:
   - MAC Address;
   - Autenticação Local;
   - Captive Portal;
   - Active Directory;
   - RADIUS;
   - IEEE 802.1x;
   - LDAP.
4. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID;
5. Deverá suportar servidor de autenticação RADIUS redundante, isto é, na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;
6. Deverá permitir o Accounting do servidor RADIUS, em conformidade com a RFC 2866, inclusive o pacote de Framed-IP-Address, permitindo a identificação de um usuário e seu respectivo endereço IP associado;
7. A solução deverá suportar a criação de uma zona ou rede de visitantes, que terão seu acesso controlado através de senha cadastrada internamente, sendo que este deverá possuir a configuração de tempo pré-determinado de acesso a rede wireless;
8. A SGC deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote);
9. Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável;
10. Deve permitir que o portal interno para usuários visitantes (guest) seja customizável;
11. Deverá permitir enviar a senha de usuários visitantes (guests), por e-mail ou por SMS;
12. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a internet, de forma totalmente separada do tráfego da rede corporativa;
13. Deverá permitir o isolamento da comunicação entre usuários visitantes (guests) em uma mesma VLAN/Subnet;
14. Deve implementar políticas de acesso com regras granulares com segmentação para grupos do domínio, usuário, localização, tipo de SO, status do certificado e VLAN;
15. As políticas de acesso devem incluir permitir, negar, e limitar a taxa de transmissão com base em VLAN e Listas de controle de Acesso (ACLs);
16. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0;
17. Implementar, mecanismos para detecção de pontos de acesso do tipo rogue com informações de no mínimo:
    a. SSID-Spoofing – APs não pertencentes à solução propagando a mesma SSID;
    b. MAC Spoofing – APs não pertencentes à solução propagando o mesmo MAC de um AP válido;
    c. Rogue APs – APs não pertencentes à solução;
    d. Same Network – APs não pertencentes à solução exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN;
18. Deve implementar varredura de RF nas bandas IEEE 802.11a, IEEE 802.11b, IEEE802.11g e 802.11n, para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogues);
19. Deve fazer a varredura no canal de operação do Ponto de Acessos em impacto na performance da rede WLAN;
20. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;
21. 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;
22. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance;
23. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática;
24. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos, para otimizar a performance;
25. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso;

26. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado

PONTO DE ACESSO SEM FIO INDOOR

Características Gerais

1. Equipamento ponto de acesso para rede local sem fios deverá atender aos padrões IEEE802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n e IEEE 802.11ac com operação nas frequências 2.4 GHz e 5 GHz de forma simultânea;
2. Deverá ser do mesmo fabricante da SGC;
3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a Resolução nº 242 da ANATEL. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras. O certificado será pesquisado em https://sistemas.anatel.gov.br/mosaico/sch/publicView/listarProdutosHomologados.xhtml.
4. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point, a ser verificado através do link:https://www.wi-fi.org/product-finder-results?subcategories=5;
5. Deverá possuir antenas internas e integradas com padrão de irradiação omni-direcional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE802.11g, IEEE 802.11n e IEEE 802.11ac e com ganhos de no mínimo 3 dBi;
6. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas;
7. Deve suportar potência de saída de no mínimo 20 dBm na frequência 5 GHz e de no mínimo20 dBm na frequência 2.4 GHz;
8. Deverá suportar canalização de 20 MHz, 40 MHz e 80 MHz;
9. Deverá possuir mecanismo de rádio com suporte a no mínimo o tipo MU-MIMO 3x3:3;
10. Deverá implementar a tecnologia Wave2;
11. Deverá suportar explicitamente TxBF ou Beamforming;
12. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de5GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência;
13. Deve suportar a identificação e controle de aplicações dos clientes conectados ao ponto de acesso;
14. Deve oferecer suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service);
15. Deverá possuir, no mínimo, 02 (duas) interface IEEE 802.3 10/100/1000 Mbps Base-TEthernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa;
16. Deverá suportar protocolo LACP;
17. Deverá possuir LEDs para a indicação do status, aceitando-se LED que emita mais de uma cor;
18. Possibilitar alimentação elétrica local via fonte de alimentação e/ou via padrão PoE (IEEE802.3af) ou PoE+ (IEEE 802.3at);
19. Deve suportar temperatura de operação entre 0°C a 40°C com PoE ativado;
20. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede;
21. Deverá ser fornecido com a versão mais recente do software interno dos Pontos de Acesso;
22. Deverá ser fornecido com todas as funcionalidades de segurança instaladas. Não deve haver licença restringindo itens de segurança do equipamento e nem a quantidade de usuários conectados;
23. Deverá ser fornecido com todas as licenças para seu completo funcionamento;
24. As licenças deverão ser perpétuas;
25. Deve vir acompanhado de sistema antifurto do tipo Kensington lock ou similar, incluindo cabo de segurança com a finalidade de evitar furto do equipamento, com no mínimo 1,5 metros e duas chaves;
26. Operar de tal forma que realize o chaveamento (switching) do tráfego de dados dos usuários sem que este tráfego tenha que passar através da(s) SGC(s);
27. Deve possuir garantia de 60 (sessenta) meses;

Gerenciamento

1. Permitir a configuração e gerenciamento direto através de browser padrão (HTTPS), SSH, SNMPv2c e SNMPv3, ou através da SGC, a fim de se garantir a segurança dos dados;
2. Permitir gerenciamento através de plataformas de softwareque sigam padrões SNMPv2c eSNMPv3, ou TR-069;
3. Implementar funcionamento em modo gerenciado pela SGC, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF;
4. Permitir que sua configuração seja automaticamente realizada quando este for conectado no ambiente de rede da SGC especificada neste documento;
5. O ponto de acesso poderá estar diretamente ou remotamente conectado à SGC, inclusive via roteamento da camada 3 de rede OSI;
6. O ponto de acesso deverá conectar-se à SGC através de túnel seguro padrão ou através de protocolo de comunicação seguro que ofereça controle total do equipamento;
7. Permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF;
8. Permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF;
9. Permitir que o processo de atualização de versão seja realizado manualmente através da WEB ou FTP ou TFTP ou automaticamente através da SGC descrito neste documento;

		Rede 1. Implementar cliente DHCP, para configuração automática deseu endereço IP e implementar também suporte à endereçamento IP estático; 2. Deve suportar VLAN seguindo a norma IEEE 802.1q; 3. Possuir suporte pelo menos 8 SSIDs por ponto de acesso; 4. Permitir habilitar e desabilitar a divulgação do SSID; 5. Possuir capacidade de selecionar automaticamente o canal de transmissão; 6. Suportar, no mínimo, 200 (duzentos) usuários wireless simultâneos por AP; 7. Deve suportar limitação de banda por grupo de usuários ou SSID; 8. Implementar, pelo menos, os seguintes padrões de segurança wireless: a. (WEP) Wired Equivalent Privacy; b. (WPA) Wi-Fi Protected Access; c. (WPA2) Wi-Fi Protected Access 2; d. (AES) Advanced Encryption Standard; e. (TKIP) Temporal Key Integrity Protocol; f. IEEE 802.1x; g. IEEE 802.11i; 9. Implementar as seguintes taxas de transmissão com fallback automático: a. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps; b. IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; c. IEEE 802.11n/ac: 6.5 até 800Mbps ou superior; 10. Deverá permitir a criação de filtros de MAC address de forma a restringir o acesso à rede wireless; 11. Funcionar via configuração do SGC no modo MESH (WiFi Mesh) sem adição de novo hardware ou alteração do sistema operacional; **INJETOR POE** 1. Injetor POE 10/100/1000 MBPS; 2. Injetor de Energia (PoE) que permite transmissão de energia elétrica juntamente com os dados para um dispositivo remoto, através do cabo de par trançado padrão em uma rede Ethernet; 3. Deve seguir o padrão do Ponto de acesso sem fio indoor, 802.3af ou 802.3at; 4. Suportar velocidades de conexão 10/100/1000 Mbps Base-T Ethernet, com conector RJ-45; 5. Capacidade de fornecer corrente elétrica em cabo UTP com comprimento de até 100 (cem) metros; 6. Possuir fonte de alimentação com seleção automática de tensão (100-240 VAC); 7. Deve ser acompanhado do respectivo cabo de força padrão ABNT e dos acessórios necessários para operacionalização do equipamento; 8. Deve ser compatível com os Pontos de Acesso sem fio indoor; 9. Deve possuir garantia de 60 (sessenta) meses.
2	Requisitos do Projeto de Implantação da solução de TI	A CONTRATADA deverá realizar a configuração inicial do ambiente virtual da rede sem fio e de, pelo menos, um ponto de acesso da Sede e outro de cartório de Zona Eleitoral do interior do Estado. A CONTRATADA deverá fornecer o conjunto de manuais técnicos oficiais, elaborados pelo fabricante de cada equipamento, contendo todas as informações sobre o produto como instruções para instalação, configuração, operação e gerenciamento. Os manuais técnicos do fabricante devem estar escritos em português e/ou inglês, e podem ser fornecidos em mídia digital (CD-ROM, DVD, PDF) ou disponibilizados para *download*.
3	Requisitos da Garantia e Manutenção	A empresa fornecedora do equipamento deverá: a) Garantir os equipamentos e serviços (suporte) pelo período mínimo de 60 (sessenta) meses diretamente com o fabricante do equipamento, contados a partir da data de emissão do Termo de Recebimento Definitivo; b) Prover assistência técnica no território brasileiro; c) Dispor de um número telefônico para suporte técnico e abertura de chamados técnicos, disponíveis 24 horas por dia e 7 dias por semana, inclusive feriados; d) possuir um sistema de atendimento de suporte via Chat, 0800, email ou através da Internet.
4	Requisitos de Capacitação	Não se aplica
5	Requisitos de Experiência Profissional da Equipe Técnica	Não se aplica
6	Requisitos de Formação da Equipe Técnica	Não se aplica
7	Requisitos da Metodologia de trabalho	Durante a implantação da solução, a CONTRATADA oferecerá treinamento Hands-On à equipe técnica do Tribunal.
8	Requisitos de Segurança sob o ponto de vista Técnico	Não se aplica

3.4 – Outros requisitos

ID	TIPO	REQUISITO
1	Não se aplica	

4. IDENTIFICAÇÃO DAS SOLUÇÕES DISPONÍVEIS

SOLUÇÃO 1	**NOME DA SOLUÇÃO:**	Aquisição de solução de rede sem fio com controladora física
	DESCRIÇÃO:	Essa alternativa trata da aquisição de solução com **controladora física**, a exemplo do que já existe no Tribunal. Devido à necessidade de **redundância**, essa alternativa exigiria a aquisição de **02 controladoras físicas** operando em modo ativo-ativo ou ativo-passivo para que incidentes não causem a indisponibilidade da rede sem fio, como já ocorreu anteriormente. Conforme explanado nos Estudos Técnicos 56 (SEI nº 1096590), a aquisição de equipamentos que permitiram a criação de um **ambiente de virtualização** robusto no Tribunal, nos possibilitam afirmar ser mais seguro manter uma aplicação nesse ambiente que tê-lo em hardware próprio. Como vantagens adicionais para a utilização de controladoras virtuais, ainda podemos citar: • economia de energia: por se tratar de máquinas virtuais, o consumo de energia elétrica será reduzido; • menor número de pontos de falha: com uma quantidade menor de hardware implantado na infraestrutura do Tribunal há uma redução na quantidade de itens que poderão apresentar falhas, como por exemplo: conexão de rede, memória, disco rígido, firmware, etc; • facilidade de backup: por se tratar de ambiente virtualizado, pode-se optar por realizar backup de toda a controladora virtual (*snapshot*); • recuperação de desastre: em caso de desastre que torne o serviço indisponível, pode-se apenas reiniciar a máquina virtual para reativar os serviços; • financeira: por se tratar de controladora virtual, não havendo, portanto, hardware envolvido, o curto de aquisição é menor. Assim, entendemos que esta solução, apesar de viável, **não é a mais adequada** para o atual ambiente do Tribunal.
	FORNECEDOR(ES):	Não se aplica
	ENTIDADE:	Não se aplica
	VALOR:	-
SOLUÇÃO 2	**NOME DA SOLUÇÃO:**	**Aquisição de solução de rede sem fio com controladora virtual de qualquer fabricante**
	DESCRIÇÃO:	Essa alternativa trata da aquisição de solução com **controladora virtual** de qualquer fabricante. Diante da dificuldade e complexidade que seria gerenciar duas soluções distintas funcionando concomitantemente, entendemos que a implantação desta solução provocaria a descontinuidade da solução atualmente utilizada. Diante disso, juntamente com a controladora, faz-se necessária a aquisição de, ao menos, **30 pontos de acesso** para substituir integralmente os que são utilizados atualmente e, assim, **manter a atual área de cobertura do serviço**. Com isso, a necessidade do Tribunal seria atendida, bem como a necessidade da Unidade Demandante em ter uma controladora virtual. Conforme Estudos Técnicos 56 (SEI nº 1096590), a aquisição da solução nos moldes adquiridos pelo TRE-AP (ARP nº 10/2020 - SEI 1097426), custaria R$ 200.308,00 (duzentos mil trezentos e oito reais) e seria composto por: • 01 Controladora wireless virtual; • 30 Licenças para controladora wireless virtual; • 30 Ponto de acesso wireless; • 30 Injetores PoE; • Serviço de instalação e configuração da controladora virtual; • Serviço de instalação e configuração dos pontos de acesso wireless indoor. Necessário deixar claro que, nesta solução, os serviços de instalação e configuração seriam adquiridos devido equipe técnica do Tribunal não possuir *know-how* necessário para implantação da mesma. Outro ponto importante é o fato de que nesta solução a área de cobertura do serviço permanecerá inalterada. Portanto, utilizando como parâmetro a ARP do TRE-AP, seriam gastos R$ 200.308,00 para a substituição dos equipamentos, sem qualquer modificação na área de cobertura do serviço.

	FORNECEDOR(ES):	Teltec Solutions LTDA
	ENTIDADE:	Tribunal Regional Eleitoral do Amapá
	VALOR:	R$ 200.308,00
SOLUÇÃO 3	**NOME DA SOLUÇÃO:**	Aquisição de solução de rede sem fio com controladora virtual do mesmo fabricante da solução já implantada no Tribunal
	DESCRIÇÃO:	Assim como a solução anterior, essa alternativa trata da aquisição de solução com **controladora virtual**. A diferença entre elas reside no fato de que nesta opção restringiremos a solução às oferecidas pela **Ruckus**, fabricante dos equipamentos atualmente em uso. Isso foi feito para que possamos analisar um cenário de **padronização** com uma solução já conhecida e implantada. Como dito anteriormente, a solução atual já está em funcionamento desde 2016, tendo como único incidente o fato de a controladora física já ter ficado indisponível por alguns dias devido problemas em seu hardware. Conforme ficou claro na comparação das propostas da empresa **Seger Technoloby**, é mais vantajoso ao Tribunal adquirir licenças/equipamentos com 05 anos de garantia e suporte. Outro detalhe importante é que a aquisição de solução **Ruckus** permitiria a utilização dos Access Points antigos em Zonas Eleitorais, expandindo a área de cobertura do serviço e atendendo a solicitação de muitas Zonas Eleitorais que, até então, eram negadas por falta de Pontos de Acesso. Nessa solução, seriam adquiridos: • 01 Controladora wireless virtual em substituição à controladora física existente que está sem garantia; • 01 licença do Virtual Data Plane, software necessário para o tunelamento da comunicação com os Access Points instalados nas Zonas Eleitorais do interior do Estado; • 30 Pontos de Acesso indoor com respectiva licença; • 30 Injetores PoE. Realizando o cálculo do preço médio da proposta da empresa (Proposta 02 - SEI 1097117) e as Atas de Registro de Preços encontradas e que forneceram equipamentos da marca Ruckus (**ARP TRE-SP 02/2020**, **ARP UFMG 04/2019** e **ARP UFRN 02/2020**), a solução teria um custo de total de **R$ 184.442,36** (cento e oitenta e quatro mil quatrocentos e quarenta e dois reais e trinta e seis centavos).
	FORNECEDOR(ES):	Seger Technology (Proposta 02 - SEI 1097117) ARP TRE-SP 08/2020 (SEI 1097137) ARP UFMG 04/2019 (SEI 1097179) ARP UFRN 02/2020 (SEI 1097596)
	ENTIDADE:	-
	VALOR:	R$ 184.442,36

5. DETALHAMENTO DAS SOLUÇÕES E ALTERNATIVAS EXISTENTES

REQUISITO	ID DA SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	x		
	2	x		
	3	x		
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Eleitoral?	1	x		
	2	x		
	3	x		
A Solução está disponível no Portal do Software Público Brasileiro?	1			x
	2			x
	3			x
A Solução é um software livre ou software público?	1			x
	2			x
	3			x
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1			x
	2			x
	3			x
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			x
	2			x
	3			x

A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?	1			x
	2			x
	3			x

6. ANÁLISE E COMPARAÇÃO DOS CUSTOS TOTAIS DA DEMANDA

A **Solução 1** não teve seu custo mencionado pois não atende um requisito da Unidade Demandante, qual seja, que a controladora seja virtual. Além disso, o fato de ter hardware envolvido eleva seu preço em relação à soluções virtuais.

A **Solução 2** tem seu valor orçado em **R$ 200.308,00** (duzentos mil trezentos e oito reais), conforme cotado em **ARP TRE-AP nº 10/2020** (SEI nº 1097426).

A **Solução 3** tem seu valor orçado em **R$ 184.442,36** (cento e oitenta e quatro mil quatrocentos e quarenta e dois reais e trinta e seis centavos), conforme preço médio calculado anteriormente.

A implantação da **Solução 2** **substituirá integralmente** a solução de rede sem fio implantada no Tribunal. Com isso, será necessária a aquisição da solução com todos os 30 Pontos de Acesso previstos. Após a substituição dos equipamentos, o Tribunal poderá contar com uma solução com 05 anos de garantia/suporte mas que terá área de cobertura inalterada.

A implantação da **Solução 3** permitirá que Tribunal conte com uma rede sem fio fornecida por equipamentos resguardados com contrato de suporte/garantia. Os Pontos de Acesso antigos, que hoje estão sem essa proteção, poderão ser utilizados em Zonas Eleitorais do interior, aumentando a área de cobertura do serviço e atendendo as solicitações de diversas Zonas Eleitorais. Futuramente, mais Pontos de Acesso poderão ser adquiridos aumentando ainda mais a área de cobertura do serviço.

7. SOLUÇÃO ESCOLHIDA

7.1 – Identificação

NOME:	Aquisição de solução de rede sem fio com controladora virtual do mesmo fabricante da solução já implantada no Tribunal		
JUSTIFICATIVA:	A utilização de equipamentos de mesma marca já utilizada no Tribunal proverá **padronização** à solução de rede sem fio ao mesmo tempo em que permitirá **aumentar a área de cobertura** do serviço com um **custo menor**. Isso será possível através da utilização dos pontos de acesso existentes que, após serem substituídos por novos, poderão ser implantados nos cartórios das Zonas Eleitorais do interior do Estado. Como se vê dos Estudos Técnicos realizados, esta opção foi a que se mostrou mais vantajosa financeiramente. Além disso, preservará o conhecimento adquirido acerca da solução ao longo de 04 anos e causando, inclusive, menor impacto aos usuários.		
DESCRIÇÃO:	01 Controladora Wireless Virtual com 05 anos de suporte 01 Licença do Virtual Data Plane com 05 anos de suporte 30 Pontos de acesso indoor com 05 anos de suporte e licença respectiva 30 Injetores PoE		
BENS E SERVIÇOS	**ID**	**BEM / SERVIÇO**	**VALOR ESTIMADO**
	1	01 Controladora Wireless Virtual com 05 anos de suporte	10.778,53
	2	01 Licença do Virtual Data Plane com 05 anos de suporte	10.778,53
	3	30 Pontos de acesso indoor com 05 anos de suporte e licença respectiva	154.195,80
	4	30 Injetores PoE	8.689,50
		TOTAL	**184.442,36**

7.2 – Alinhamento com as necessidades de negócio

ID	FUNÇÃO	NECESSIDADE DO NEGÓCIO
1	Utilização de controladora wi-fi compatível com VMware vShere ESXi	Possibilitar a criação de rede wi-fi com controladora virtual
2	Utilização dos principais protocolos de segurança wireless e de certificados digitais emitidos por autoridade certificadora externa	Garantir a segurança da comunicação sem fio
3	Possibilidade de criação de múltiplos SSIDs, agregação de APs, criação de rede para visitantes e permitir múltiplos meios de autenticação	Garantir flexibilidade na criação e manutenção de redes sem fio

7.3 – Benefícios esperados

ID	TIPO	BENEFÍCIOS
1	Confiabilidade	Equipamentos novos em garantia
2	Disponibilidade	Controladora virtual propiciando maior disponibilidade

3	Orçamentária	Possibilidade de aquisição da solução com melhor custo/benefício
4	Segurança	Utilização de túneis para interligar equipamentos do interior ao equipamento do Datacenter
5	Padronização	Utilização de solução de fornecedor único, facilitando gerenciamento e manutenção da solução
6	Ambiental	Utilização de Pontos de Acesso antigos nas Zonas Eleitorais de modo que não sejam descartados
7	Satisfação	Atendimento da solicitação realizada pelas Zonas Eleitorais pedindo a implantação do serviço

7.4 – Justificativa de não-conformidade

ID	SOLUÇÃO	JUSTIFICATIVA
1	Aquisição de solução de rede sem fio com controladora física	Maior custo pois envolve a aquisição de equipamento físico (hardware) Necessidade de que a controladora seja virtual de modo a propiciar maior disponibilidade do serviço
2	Aquisição de solução de rede sem fio com controladora virtual de qualquer fabricante	Não permitirá a padronização da solução Não permitirá o aumento na área de cobertura do serviço Custo de aquisição mais alto Maior impacto na implantação

8. AVALIAÇÃO DAS NECESSIDADES DE ADEQUAÇÃO PARA EXECUÇÃO CONTRATUAL

ID	TIPO DE NECESSIDADE	DESCRIÇÃO
1	Não se aplica	

9. ASSINATURAS

INTEGRANTE	NOME	ÁREA
Demandante:	ANTONIO MANOEL SILVEIRA DE SOUSA	CODIN
Técnico:	CARLOS ALBERTO RIBEIRO DO NASCIMENTO JR.	SEINF
Administrativo:	SIDNEI ANTUNES RIBEIRO	SELIC

Teresina, 26 de outubro de 2020.

Documento assinado eletronicamente por **Sidnei Antunes Ribeiro**, **Chefe de Seção**, em 03/11/2020, às 11:21, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Carlos Alberto Ribeiro do Nascimento Junior**, **Técnico Judiciário**, em 05/11/2020, às 00:37, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Antonio Manoel Silveira de Sousa**, **Coordenador de Desenvolvimento e Infraestrutura**, em 08/11/2020, às 17:00, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1099017** e o código CRC **C9935CCD**.