ANEXO IV – ESPECIFICAÇÕES TÉCNICAS – SOLUÇÃO WIFI

1. ACCESS POINT

1.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless.
1.2. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
1.3. Deve ser compatível e gerenciado pelo “Firewall de Próxima Geração (NGFW)”, modelo FortiGate-1800F, já existente na estrutura da CONTRATANTE;
1.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;
1.5. Deve permitir ser gerenciado remotamente através de links WAN;
1.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
1.7. Deve possuir capacidade de operar simultaneamente nas frequências de 2.4GHz, 5GHz e 6 GHz, além de permitir configurações independentes para cada rádio;
1.8. O ponto de acesso deve possuir rádio Wi-Fi adicional àqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;
1.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
1.10. Deve permitir a conexão de 500 (quinhentos) clientes wireless simultaneamente;
1.11. Deve possuir 2 (duas) interfaces Ethernet com conector RJ-45 para permitir a conexão com a rede LAN sendo uma delas padrão 10/100/1000 Base-T e a outra padrão 100/1000/2500 Base-T;
1.12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

1.13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;
1.14. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;
1.15. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;
1.16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
1.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
1.18. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
1.19. Deve permitir operação em modo Mesh;
1.20. Deve possuir potência de irradiação mínima de 23dBm em todos os rádios;
1.21. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
1.22. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
1.23. Deve suportar OFDMA;
1.24. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
1.25. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
1.26. Deve suportar BSS Coloring;
1.27. Deve suportar operação em 6GHz com canais de 20, 40, 80 e 160 MHz;
1.28. Deve possuir sensibilidade mínima de -93dBm quando operando em 6GHz com MCS0 (HT20);

1.29. Deve possuir antenas internas ao equipamento com ganho mínimo de 4.5dBi em 2.4GHz, 5GHz e 6GHz;
1.30. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
1.31. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem no mínimo nas frequências de 2.4GHz e 5GHz;
1.32. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem no mínimo nas frequências de 2.4GHz ou 5GHz;
1.33. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
1.34. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
1.35. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea;
1.36. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
1.37. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
1.38. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
1.39. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
1.40. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
1.41. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
1.42. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
1.43. Deve implementar o padrão IEEE 802.11e;

1.44. Deve implementar o padrão IEEE 802.11h;
1.45. Deve implementar o padrão IEEE 802.3az;
1.46. Deve suportar ser gerenciado via SNMP;
1.47. Deve suportar consultas via REST API;
1.48. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
1.49. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;
1.50. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
1.51. Deve possuir indicadores luminosos (LED) para indicação de status;
1.52. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
1.53. Deve possuir certificado emitido pela Wi-Fi Alliance;
1.54. Deve estar homologado pela ANATEL na data de execução do pregão.

2. LICENCIAMENTO, SUPORTE E GARANTIA DO FABRICANTE

2.1. Refere-se as características das licenças suporte técnico e garantia dos equipamentos access points e da solução de gerenciamento de portal de acesso, pelo período de 36 meses.
2.2. Quaisquer licenças necessárias para plena execução de todas as características descritas neste termo de referência entre hardware e software deverão ser fornecidas;
2.3. Deverá ser fornecido contrato garantia oficial do fabricante com duração de 36 meses.
2.4. A Garantia e Suporte compreendem todo o serviço de diagnóstico, reparo e/ou substituição de funcionalidade, recurso, componente ou módulo do equipamento que apresente sinais de alerta de troca de peças ou defeito por outro de mesmas características técnicas, ou superior.
2.5. O Suporte e garantia para os access points (item 1) deve ser realizado pelo Fabricante, no período de 36 (trinta e seis) meses contados a partir do recebimento definitivo do equipamento, sem prejuízo de qualquer política de garantia adicional oferecido pelo fabricante.
2.6. A CONTRATADA deve, no início da vigência do contrato, indicar os canais e requisitos necessários para a solicitação e acompanhamento dos serviços de garantia e suporte, conforme procedimentos padronizados pelo fabricante.

2.7. As solicitações de chamado técnico terão origem em decorrência de qualquer evento ou problema detectado pela Equipe Técnica do TCE-GO no tocante ao pleno estado de funcionamento da solução, incluindo problemas relacionados à instalação, configuração e atualização.
2.8. Deverá providenciar correção de problemas e esclarecimentos de dúvidas sobre configuração e utilização da solução ofertada.
2.9. Deverá providenciar manutenção e atualização de softwares que compõem a solução ofertada.
2.10. O serviço de suporte será solicitado pela equipe técnica do Tribunal mediante abertura de chamado junto à CONTRATADA, via chamada telefônica local ou gratuita, e-mail ou Internet, devendo o recebimento dos chamados ocorrer em período integral (24x7x365).
2.11. Deve permitir o acesso aos patches de correção e a atualização tecnológica sempre na versão mais recente disponível no mercado.
2.12. Os serviços deverão ser prestados pelo próprio Fabricante ou assistência técnica autorizada ou credenciada.
2.13. Deve oferecer atendimento em português.
2.14. A CONTRATANTE poderá abrir chamados de manutenção diretamente no fabricante do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software.
2.15. Deverá ser garantido à CONTRATANTE o pleno acesso ao site do fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.
2.16. A logística e os custos envolvidos para substituição e transporte de hardware são de responsabilidade da CONTRATADA.
2.17. O Suporte pode ser prestado na categoria remota, porém nos casos em que exista a necessidade de intervenção física aos equipamentos devem ser prestados na categoria on-site na cidade de Goiânia – GO.
2.18. Deve contemplar suporte do FABRICANTE pelo período vigente, com no mínimo, as seguintes características:
2.18.1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento funcionando 24 horas por dia e 7 dias por semana para atendimento telefônico.

2.18.2. Deve assegurar a utilização de novas versões de software da solução sem ônus ao CONTRATANTE, sempre que esta estiver disponível para o modelo ofertado.
2.18.3. Deve permitir o acesso à base de conhecimento da solução;
2.18.4. O CONTRATANTE poderá abrir chamados de manutenção diretamente no
2.18.5. Fabricante do item, através de chamada gratuita a número 0800 e por interface Web, sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.
2.18.6. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software.
2.18.7. Poderá ser solicitado ao fabricante acesso remoto aos equipamentos para ajuda na correção de problemas dos diversos tipos inclusive configuração.
2.18.8. Deverá ser garantido ao CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

3. INJETOR POE

3.1. Deve ser compatível com o padrão 802.3at.
3.2. Duas portas RJ-45 blindado (EIA 568A e 568B).
3.3. Possuir tensão de saída de 55 V.
3.4. Alimentação de 100 a 240 V AC.
3.5. Gigabit Ethernet (10/100/1000 Mbps).
3.6. Potência de saída (Output Power) 36 Watts.
3.7. MTBF 100.000 horas.

4. SOLUÇÃO DE GERENCIAMENTO DE PORTAL DE ACESSO

4.1. CARACTERÍSTICAS GERAIS PARA SOLUÇÃO DE GERENCIAMENTO DE PORTAL DE ACESSO

4.1.1. Deve ser do tipo appliance virtual, sendo de responsabilidade da CONTRATANTE a disponibilização dos recursos necessários para a implantação da solução: hardware e software (hypervisor), ou contratação de instâncias de computação em nuvem;
4.1.2. Em nuvens privadas, deverá ser compatível com pelo menos os Hypervisors: VMware, Microsoft Hyper-V, Xen, Linux KVM, Nutanix AHV;
4.1.3. Em nuvens públicas, deverá ser compatível com pelo menos as seguintes provedoras de nuvem: AWS, Azure e OCI;
4.1.4. Deve suportar número ilimitado de vCPUs em implementação em ambientes virtualizados;
4.1.5. Deve ser entregue licenciado e configurado para permitir Alta Disponibilidade (HA);
4.1.6. Deve ser compatível e integrável ao “Firewall de Próxima Geração (NGFW) **FG-1800F**” já existente na estrutura da CONTRATANTE;
4.1.7. Deve estar licenciado para permitir ao menos 1000 usuários locais ou remotos;
4.1.8. Deve estar licenciado para permitir ao menos 300 dispositivos (NAS);
4.1.9. Deve estar licenciado para permitir ao menos 100 grupos de usuários;
4.1.10. Deve estar licenciado para suportar ao menos 50 certificados de Autoridades Certificadoras;
4.1.11. Deve estar licenciado para suportar ao menos 5000 certificados de usuários;
4.1.12. Deverá possui suporte 24x7 com resposta em uma hora para problemas críticos e resposta no próximo dia útil para problemas não críticos.

4.2. REQUISITOS GERAIS

4.2.1. Deve suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS;
4.2.2. Deve suportar administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH;
4.2.3. Deve permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;

4.2.4. Deve possuir indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);
4.2.5. Deve suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo;
4.2.6. Deve suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa;
4.2.7. Deve suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção;
4.2.8. Deve suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas;
4.2.9. Deve permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HA;
4.2.10. Deve suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas;
4.2.11. Deve suportar a opção de backup criptografado;
4.2.12. Deve suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;
4.2.13. Deve suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on e etc. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;
4.2.14. Deve suportar NTP (Network Time Protocol), visando o sincronismo de hora/data;
4.2.15. Deve suportar roteamento estático;
4.2.16. Deve suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps;
4.2.17. Deve suportar nativamente Trap SNMP indicando mudança de status de HA;
4.2.18. Deve suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark);
4.2.19. Deve suportar o envio de e-mails atuando como servidor próprio (localhost) ou integrar-se com servidor(es) externo(s) para envio das mensagens aos usuários ou administradores;

4.2.20. Deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token);

4.2.21. Deve permitir o envio de mensagens SMS para os usuários através de gateways SMS de terceiros ou seu próprio serviço de envio de SMS, sendo este segundo licenciado ou não.;

4.2.22. Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais;

4.3. AUTENTICAÇÃO

4.3.1. A solução deve efetuar autenticação para a gerência de identidade dos usuários visitantes, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;

4.3.2. Suporta autenticação em dois fatores (two-factor authentication);

4.3.3. Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como softwares para dispositivos móveis, e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário.;

4.3.4. A solução deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais etc.;

4.3.5. A solução deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta;

4.3.6. A solução deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;

4.3.7. A solução deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;

4.3.8. A solução deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação do mesmo;

4.3.9. A solução deve permitir a criação de novos usuários na base de dados local de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário;

4.3.10. Remoção automática em massa de usuários desabilitados, baseado em critérios definidos;

4.3.11. A solução deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança;

4.3.12. Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade.;

4.3.13. Deve continuar permitindo a autenticação de dois fatores em clientes Windows mesmo com a máquina offline;

4.3.14. Deve prover um portal web para o auto-registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado;

4.3.15. O portal web deve ser personalizável de modo que seja possível definir, conforme as políticas do Tribunal, quais atributos e informações os usuários devem fornecer para efetuar o auto-registro.

4.3.16. A solução deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;

4.3.17. A solução deve suportar a integração com servidor RADIUS remoto;

4.3.18. A solução pode funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;

4.3.19. A solução deve possuir um servidor LDAP interno que permita ser configurado de forma hierárquica, para a correta administração por grupos ou unidades organizacionais dos usuários locais;

4.3.20. A solução deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);

4.3.21. A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google;

4.3.22. A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;

4.3.23. A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;

4.3.24. A solução deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes;

4.3.25. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

4.3.26. Deve permitir integração com bases do Azure Directory e GSuite;

4.3.27. Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365;

4.4. CONTROLE BASEADO EM PORTA

4.4.1. A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;

4.4.2. Deve nativamente (sem o redirecionamento para equipamentos de terceiros) proporcionar a integração de clientes finais para oferecer autenticação 802.1X, por exemplo um cliente que utilize Windows poderá configurar seu equipamento para o suporte 802.1X;

4.4.3. Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC;

4.4.4. Suportar interoperabilidade com equipamentos de acesso (switches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X;

4.4.5. Deve suportar bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X, a liberação deverá ser feita baseada no endereço MAC dos equipamentos previamente

cadastrados, estes terão acesso a rede sem necessidade de autenticação ou ação do usuário ou dispositivo;

4.5. CERTIFICADOS

4.5.1. A solução deve atuar como Autoridade Certificadora (CA);
4.5.2. Deve permitir a administração de certificados digitais, com emissão e revogação;
4.5.3. Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas;
4.5.4. Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL);
4.5.5. Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados;
4.5.6. Deve suportar SCEP server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador;
4.5.7. Deve criar e assinar certificados X.509 para utilização em servidores HTTPS e SSH, assim como para os clientes de serviços HTTPS, SSH e VPNs IPSec;
4.5.8. Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados;
4.5.9. Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários;

4.6. SERVIÇO DE AUTENTICAÇÃO ÚNICA (SINGLE SIGN-ON)

4.6.1. A solução deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis;
4.6.2. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade se SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio;
4.6.3. Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO;
4.6.4. Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO;

4.6.5. Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Indentity Providers - IDP's) de terceiros;
4.6.6. Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On);
4.6.7. Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accouting, a modificação destes pacotes e o encaminhamento deles para vários outros pontos.

5. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

5.1. Este serviço compreende a substituição dos atuais pontos de acesso através da instalação física e lógica de acordo com as especificações do fabricante nos pontos de rede lógicos já existentes.
5.2. A instalação dos access points (pontos de acesso) deverá ser efetuada nos locais designados, juntamente com a configuração inicial e a garantia de que a rede esteja operando de acordo com os padrões estabelecidos.
5.3. Caberá a CONTRATATA a integração ou migração da CONTROLADORA em produção, bem como de toda a configuração e pontos de acessos existentes na CONTRATADA.
5.4. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.
5.5. Os serviços de instalação e configuração deverá ser realizado por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;
5.6. O serviço de instalação dos hardwares compreende, mas não se limita as seguintes atividades:

5.6.1. Remoção física dos equipamentos em operação no Tribunal;
5.6.2. Instalação física dos novos equipamentos nas dependências do contratante nos locais indicados pela equipe técnica do Tribunal, sendo de responsabilidade do contratante prover níveis básicos de fixação e acomodação.
5.6.3. Efetuar a configuração otimizada que aproveite a melhor performance da solução.
5.6.4. Aplicar patchs para atualização do sistema e firmware caso necessário;

5.6.5. Configuração lógica dos equipamentos na controladora e definição de grupos e regras de acesso de acordo com as políticas estabelecidas pelo Tribunal;
5.6.6. O serviço deve ser executado por técnico certificado pelo fabricante do equipamento.
5.6.7. É de responsabilidade da contratada qualquer dano físico ao equipamento;
5.6.8. É proibida a divulgação de qualquer configuração destes equipamentos, por questões de segurança, por parte da licitante;
5.6.9. Todas as senhas e usuários usados pelo licitante para as configurações dos equipamentos devem ser notificadas e entregues por escrito.
5.6.10. Realização de testes de conectividade para garantir o funcionamento adequado da rede.
5.6.11. Documentação detalhada de todas as configurações, senhas e informações relevantes relacionadas à ativação e configuração de todos os hardwares.

5.7. Deverá ser considerado a configuração das redes lógicas wireless conforme padrões e políticas adotados pelo Tribunal;
5.8. Deverá ser considerado a configuração de portal de acesso (captive portal) que conceda acesso aos usuários visitantes por meio de auto-registro através do fornecimento de informações como “nome”, “e-mail” e “cpf”.
5.9. Ao final da execução do serviço de instalação a CONTRATADA deverá apresentar Documentação As-Built que evidencie roteiro completo de configuração, implementação e topologia, com detalhamento de todas as configurações dos produtos e programas integrantes da solução.

6. SERVIÇO DE TREINAMENTO

6.1. A licitante vencedora deverá prestar o treinamento de toda a solução ofertada, para 6 (seis) profissionais designados pelo TCE-GO, referente à instalação, configuração e operação dos equipamentos e softwares;
6.2. Fica estabelecido que o treinamento e transferência de tecnologia seja em horário de funcionamento normal do TCE-GO, de segunda a sexta-feira. Caso haja a necessidade de ser realizado durante finais de semana, ou mesmo em horários distintos ao estabelecido, será necessária prévia negociação com a equipe técnica designada para acompanhar o projeto;

6.3. O treinamento e transferência de tecnologia deverão ser de maneira presencial e sem a interrupção de qualquer dos serviços habilitando assim os funcionários do TCE-GO à nova solução ofertada;
6.4. Todas as despesas com o instrutor deverão ser de total responsabilidade do fornecedor;
6.5. Deverá ser emitido certificado ao final do curso;
6.6. No caso do treinamento fornecido não for satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a licitante vencedora deverá realizar novo treinamento sem ônus adicional o TCE-GO;
6.7. Garantir, em todas as fases do projeto, a total transferência de tecnologia aos profissionais técnicos designados pelo TCE-GO;
6.8. Socializar todas as informações aos envolvidos no projeto, deixando a equipe técnica designada para acompanhamento ciente, capacitada e com total domínio da solução de infraestrutura implementada.

7. SERVIÇO DE INFRAESTRUTURA – CABEAMENTO ESTRUTURADO

7.1. Refere-se a serviço, sob demanda, para fornecimento de materiais e mão de obra especializada para execução de infraestrutura de telecomunicações horizontal compreendendo o lançamento e conectorização de cabos U/UTP Categoria 6, identificação e certificação do cabeamento estruturado.
7.2. A execução do serviço refere-se à criação de novos pontos lógicos, até o limite de **40 (quarenta),** conforme a necessidade do Tribunal, de forma a prover conectividade aos equipamentos access points à rede de dados, aproveitando-se da infraestrutura preexistente (eletrocalhas, perfilados etc).
7.3. A proposta deverá considerar o valor unitário para execução do serviço de instalação de um ponto de cabeamento incluindo todos os materiais como cabos de rede, conectores, miscelâneas, lançamento e conectorização dos cabos e certificação dos pontos de rede.
7.4. A CONTRATADA deverá fornecer garantia contra defeitos/vícios, impropriedades de fabricação dos produtos de, no mínimo, 36 (trinta e seis) meses, a contar da data de recebimento definitivo do objeto.
7.5. O escopo do serviço compreende, mas não se limita a execução das seguintes atividades:

7.5.1. Lançamento de cabeamento horizontal entre o rack e o local de instalação do ponto de acesso aproveitando-se da infraestrutura preexistente;

7.5.2. Conectorização do ponto lógico ao patch panel instalado no rack;

7.5.3. Para cada ponto de cabeamento estruturado serão instalados 01 (um) conector modulare de 8 pinos, fêmea, padrão RJ-45(Cat. 6), sem blindagem, com terminais de conexão em cobre – berílio, estanhados, padrão 110 IDC, para condutores de 22 a 26 AWG.

7.5.3.1. Corpo em termoplástico de alto impacto não propagante à chama.

7.5.4. Os espelhos das tomadas embutidas em parede deverão ser da linha modular, cor branca. Ref.: Linha Talari da IRIEL ou similar. Para as tomadas aparentes, deverá ser utilizada a tampa específica para a caixa de derivação (condulete desmontável). Essa exigência é justificada pela necessidade de preservar o padrão estético e a qualidade das instalações do TCE-GO.

7.5.5. Todas as novas tomadas deverão ter todos os pinos conectados conforme o padrão 568-A, e deverão obedecer às características técnicas estabelecidas pela norma EIA/TIA ANSI/TIA-568.2-D para Categoria 6.

7.5.6. Fornecimento e instalação de eletroduto tubular de PVC, PEAD (Polietileno de Alta Densidade) ou de aço galvanizado. Os dutos de PVC e PEAD podem ser corrugados ou lisos, rígidos ou flexíveis entre o ponto de acesso e a eletrocalha ou perfilado;

7.5.7. A conexão de cada ponto de acesso à tomada RJ-45 deverá ser executada com a utilização de patch cords RJ-45, Categoria 6, de até 1m (um metro) de comprimento. Os patch cords devem ser certificados pelo fabricante dos produtos de cabeamento;

7.5.8. Os cabos U/UTP da rede lógica partirão dos Patch Panel a serem instalados nos racks e seguirão diretamente ao ponto lógico, sem interrupções, derivações ou emendas, os mesmos deverão ser organizados no interior do rack em feixes, acintados por velcro e fixados à estrutura do rack.

7.5.9. Os cabos UTPs deverão ser conectados ao Patch Panel obedecendo a uma curvatura de raio externo de 1”.

7.5.10. Os referidos cabos não poderão ter emendas, dobras e partes desencapadas, em nenhuma hipótese, pois estas ocorrências alteram as características físicas dos mesmos, acarretando funcionamento inadequado da rede, de uma maneira geral.

7.5.11. No Patch Panel, o cabo UTP deve ter folga suficiente em seu comprimento para possibilitar a troca de porta para qualquer outra porta RJ-45 do Patch Panel. No lado da tomada da estação de trabalho, o cabo deve ter uma folga de 30cm.

7.5.12. Todo novo cabeamento deverá ser testado e certificado, com vistas a comprovação da conformidade com a norma EIA/TIA ANSI/TIA-568.2-D Categoria 6, no que tange a: Wire Map, Lenght, Insertion Loss, NEXT Loss, Power Sum NEXT Loss, ELFEXT Loss, Power Sun ELFEXT Loss, Return Loss, Propagation Delay, Delay Skew, onde todos os testes deverão ser aprovados.

7.5.12.1. A certificação deverá ser de Link Permanente e todos os relatórios deverão apresentar o tipo de certificação que foi realizada (Certificação de Link Permanente),o tipo de conector utilizado (Conector para teste de Link Permanente), a norma que foi utilizada para certificação EIA/TIA ANSI/TIA-568.2-D Categoria 6 e a data da última calibração do aparelho certificador que deverá ser, obrigatoriamente, inferior a um ano (365 dias) da data de certificação dos pontos.

7.5.12.2. Um segmento de cabo UTP com terminação nas pontas será considerado certificado quando o resultado do aparelho for “aprovado” e dentro de todas as exigências descritas na norma TIA/EIA 568-B.2-1, para a categoria 6, não sendo admitidos valores e resultados marginais, ou muito próximos aos parâmetros mínimos da norma.

7.5.12.3. Os relatórios gerados pelos aparelhos deverão apresentar a identificação e tipo de cabo testado conforme a descrição constante no projeto.

7.5.12.4. Os relatórios serão entregues em forma de relatório impresso e arquivo digital, datados (coincidente com a data do teste) e rubricados pelo Responsável Técnico.

7.5.12.5. Não serão aceitos testes por amostragem. Todos os pontos deverão ser testados na extremidade da tomada e na extremidade do painel distribuidor (bi-direcional).

7.5.13. Para manobra entre o Patch Panel e os equipamentos ativos deverão ser fornecidos Patch cords para sistemas de cabeamento estruturado para tráfego de voz, dados e imagens, segundo requisitos da norma ANSI/TIA/568.2-D Categoria 6. Estes cordões devem ser certificados pelo fabricante dos produtos de cabeamento.

7.6. **Padrão de identificação do cabeamento estruturado:**

7.6.1. Todos os cabos U/UTP deverão ser identificados em suas duas extremidades (tanto no patch panel como na tomada lógica);

7.6.2. Os cabos deverão ser identificados utilizando marcadores para condutores elétricos Hellermann, ou similar, do tipo Helagrip, referência número H0 85, de tal modo que estes não deslizem pelo cabo e indiquem o número do terminal de trabalho correspondente.

7.6.3. A identificação deve ser colocada a uma distância, conforme descrita a seguir, de modo que a visualização desta não seja prejudicada, conforme descrito abaixo:

7.6.3.1. Distância do conector RJ-45 do lado do Patch Panel d= +/- 1,0 cm

7.6.3.2. Distância do conector RJ-45 do lado do ponto de rede d= +/- 20,0 cm

7.6.3.3. A identificação será feita no cabo através de etiquetas plásticas ou Poliéster branco do tipo BRADY ou equivalente técnico;

7.6.4. Cada cabo U/UTP será identificado da seguinte forma:

7.6.4.1. cor de fundo: branca;

7.6.4.2. cor da identificação: preta;

7.6.4.3. codificação: Rack XX onde XX identifica o Rack de origem do cabo;

7.6.4.4. codificação: PPYY onde YY identifica o Patch Panel de origem do cabo;

7.6.4.5. codificação: ZZ onde ZZ identifica o número da porta no Patch Panel;

7.6.5. Deverá ser feita a identificação dos novos pontos nos Patch Panel através de etiquetas plásticas ou Poliéster branco do tipo BRADY ou equivalente técnico;

7.6.5.1. cor de fundo: branca;

7.6.5.2. cor da identificação: preta;

7.6.5.3. codificação: Rack XX onde XX identifica o Rack;

7.6.5.4. codificação: PPYY onde YY identifica o número do Patch Panel no Rack;

7.6.6. Os patch cords que conectam o patch panel ao switch deverão ser identificados em suas duas extremidades através de etiquetas plásticas ou Poliéster branco do tipo BRADY ou equivalente técnico;

7.6.6.1. cor de fundo: branca;

7.6.6.2. cor da identificação: preta;

7.6.6.3. codificação: WWW onde WWW identifica o Patch Cord;

7.6.7. Todas as tomadas deverão ser identificadas através de etiquetas plásticas com fundo branco e letras pretas, colada no espelho da caixa com a identificação do circuito a que pertencem conforme exemplo:

7.6.7.1. cor de fundo: branca;

7.6.7.2. cor da identificação: preta;

7.6.7.3. codificação: Rack XX onde XX identifica o Rack de origem do cabo;

7.6.7.4. codificação: PPYY onde YY identifica o Patch Panel de origem do cabo;

7.6.7.5. codificação: ZZ onde ZZ identifica o número da porta no Patch Panel;

7.7. **Não faz parte do escopo desse serviço:**

7.7.1. Fornecimento ou instalação de eletrocalhas, rack para acomodação de equipamentos de rede, patch painel ou switches de acesso.

7.8. **Características do cabo UTP 4 pares categoria 6**

7.8.1. Deverão ser utilizados cabos novos de cobre não blindados (UTP), 23 AWG x 4, categoria 6(250Mhz), com 4 (quatro) pares trançados, que atendam plenamente a todos os requisitos físicos e elétricos das Norma TIA/EIA-568-B.2-1 – Addendum 1, conectados numa ponta à parte traseira do Patch Panel e na outra aos conectores RJ-45 fêmeas e contatos com, no mínimo, 50 micropolegadas em ouro, nas caixas de tomadas nos pontos de rede.

7.8.2. A pinagem dos conectores obedecerá ao padrão “T568A” de acordo com a norma TIA/EIA-568B.

7.8.3. Todos os cabos UTPs do mesmo trecho de duto deverão ser lançados simultaneamente.

7.8.4. É vedada a reutilização de cabos UTPs, para qualquer finalidade, devendo os cabos que apresentar problemas (danificados, muito curtos, etc.) serem integralmente substituídos.

7.8.5. Impedância característica de 100 Ohms;

7.8.6. O raio mínimo de curvatura para o cabo UTP deverá ser de no mínimo, 4 vezes o diâmetro do cabo;

7.8.7. Os cabos UTP deverão ser fixados e agrupados nos dutos, calhas ou racks utilizando-se abraçadeiras de velcro, e não abraçadeiras de material plástico.
7.8.8. Ser composto por condutores de cobre sólido;
7.8.9. Capa externa em PVC não propagante à chama;
7.8.10. Apresentar certificado que comprove possuir no mínimo classe CM.
7.8.11. Tensão máxima de lançamento 110N (11,4Kgf); A sobra de cabo UTP deverá ser de 3m nos racks (sobra = trecho de cabo enrolado na base do rack), e a sobra de cabo UTP nas tomadas lógicas deverá ser de 30 cm.
7.8.12. O comprimento máximo de destrançamento do cabo UTP para a crimpagem será de 13 mm, tanto na tomada lógica como no patch panel.
7.8.13. Serão utilizados cabos, todos da mesma cor, para distribuição horizontal, para line cords e patch cords;
7.8.14. Possuir impresso na capa externa nome do fabricante, marca do produto e data de fabricação;
7.8.15. Na capa de proteção dos cabos, será marcada, de forma indelével e em intervalos regulares de, no máximo, 100 cm, a seguinte sequência de dizeres: Nome do fabricante; Seção nominal do condutor;
7.8.16. Apresentar certificação de performance elétrica e flamabilidade pela UL(Underwriters Laboratories), CSA ou ETL, conforme especificações da Norma TIA/EIA-568-B.2-1 – Addendum 1.
7.8.17. Deverá possuir a diretiva ROHS.
7.8.18. Deverá ser previsto uma sobra de no mínimo 3 (três) metros de cabo UTP para cada Cabo lançado. Esta sobra deverá ser acomodada dentro do respectivo AT ou sala de telecomunicação.

7.9. **PATCH CORD:**

7.9.1. Patch cord para sistemas de cabeamento estruturado para tráfego de voz, dados e imagens, segundo requisitos da norma ANSI/TIA/568.2-D Categoria 6. Previstos para cabeamento horizontal ou secundário, uso interno, em ponto de acesso à área de trabalho para interligação do hardware de comunicação do usuário às tomadas de conexão da rede e também nas salas de telecomunicações, para manobras entre os painéis de distribuição e os equipamentos ativos da rede;

7.9.2. Possuir, no mínimo, certificado de performance (VERIFIED) pela UL ou CSA ou ETL conforme especificações da norma ANSI/TIA/568.2-D. Os números dos certificados (certificado de performance (VERIFIED)) dos produtos ofertados deverão ser fornecidos para conferência no site dos laboratórios nos quais os produtos foram certificados;

7.9.3. Deve ter certificação Anatel conforme regulamento da entidade: cordão de manobra;

7.9.4. Deve cumprir com os requisitos quanto à taxa máxima de compostos que não agridam ao meio ambiente conforme a norma RoHS;

7.9.5. Deverão ser montados e testados em fábrica, com garantia de performance;

7.9.6. Deve ser confeccionado em cabo par trançado, U/UTP Categoria 6 24 AWG x 4 pares, composto por condutores de cobre flexível, multifilar, isolamento em poliolefina;

7.9.7. Devem ser conectorizados à RJ-45 macho Categoria 6 nas duas extremidades, devem atender às especificações contidas na norma ANSI/TIA/568.2-D 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, garras duplas para garantia de vinculação elétrica com as veias do cabo;

7.9.8. Possuir classe de flamabilidade, no mínimo, igual a CM impressa na capa;

7.9.9. Deve possuir capa protetora (boot) do mesmo dimensional do RJ-45 plug e proteção à lingueta de travamento. Esta capa protetora deve ajudar a evitar a curvatura excessiva do cabo em movimentos na conexão bem como proteger o pino de destravamento dos conectores contra enroscamentos e quebras.

7.10. **CONECTOR M8V RJ45 FÊMEA CATEGORIA 6:**

7.10.1. Conector utilizado em sistemas de cabeamento estruturado para tráfego de voz, dados e imagens, segundo requisitos da norma ANSI/TIA/568.2-D Categoria 6, para cabeamento horizontal ou secundário, uso interno, em ponto de acesso na área de trabalho para tomadas de serviços em sistemas estruturados de cabeamento e em sistemas que requeiram grande margem de segurança sobre as

especificações normalizadas para garantia de suporte às aplicações futuras;

7.10.2. Suporte a IEEE 802.3, 1000 BASE T, 1000 BASE TX, EIA/TIA-854, ANSI/TIA-862 e ATM;

7.10.3. Possuir, no mínimo, certificado de performance (VERIFIED) pela UL ou CSA ou ETL conforme especificações da norma ANSI/TIA-568.2-D. Os números dos certificados (certificado de performance (VERIFIED)) dos produtos ofertados deverão ser fornecidos para conferência no site dos laboratórios nos quais os produtos foram certificados;

7.10.4. Com corpo em termoplástico de alto impacto não propagante a chama;

7.10.5. Os contatos do jack modular são banhados com um mínimo de 50 micropolegadas de ouro na área do contato e um um banho-baixo mínimo de 100 micropolegadas de níquel. Deve ser compatível para as terminações T568A e T568B, segundo a ANSI/TIA/568.2-D;

7.10.6. Possuir terminação do tipo 110 IDC (conexão 90º/180º) estanhados para a proteção contra oxidação e permitir inserção de condutores de 22 AWG a 26 AWG;

7.10.7. Deve possibilitar a crimpagem dos 8 condutores ao mesmo tempo proporcionando deste modo uma conectorização homogênea.

7.10.8. Deve suportar ciclos de inserção, na parte frontal, igual ou superior a 750 (setecentas e cinqüenta) vezes com conectores RJ-45 e 200 inserções com RJ11;

7.10.9. Deve suportar ciclos de inserção, igual ou superior a 200 (duzentas) vezes com terminações 110 IDC;

7.10.10. Deve exceder as características elétricas contidas na norma ANSI/TIA/568.2-D Categoria 6;

7.10.11. Deve cumprir com os requisitos quanto a taxa máxima de compostos que não agridam ao meio ambiente conforme a diretiva RoHS.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DO TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS, em Goiânia, 19 de dezembro de 2024.

LICARDINO SIQUEIRA PIRES

DIRETOR DE TECNOLOGIA DA INFORMAÇÃO

LICARDINO SIQUEIRA PIRES:85826294191

Assinado de forma digital por LICARDINO SIQUEIRA PIRES:85826294191
Dados: 2024.12.20 08:30:27 -03'00'

TCE
Fls:

TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

ANEXO/2024 - DI-TI

Digitally signed by LICARDINO SIQUEIRA PIRES:85826294191
Date: 2024.12.20 11:47:27 -03:00
Reason: Assinado eletronicamente com fundamento da Resolução Normativa 12/2017 do TCE-GO, Art. 6º, inc. II – certificado digital

ASSINADO ELETRONICAMENTE

Documento assinado eletronicamente com fundamento da Resolução Normativa 12/2017 do TCE-GO, Art. 6º.
Número do Processo: 202400047004061 / A autenticidade deste documento pode ser conferida no site:
http://www.tce.go.gov.br/ValidaDocumento?Key=92240226114125203123177198128135277103236135290 2