

- 1.7.2.1. Entrega de documentação de inventário do core existente contemplando os seguintes itens:
- 1.7.2.1.1. A especificação de hardware/software do atual dispositivo do core da LAN;
 - 1.7.2.1.2. A especificação de versão de SO (firmware/IOS);
 - 1.7.2.1.3. A Configuração lógica dos switches core atuais, contemplando todas as funcionalidades solicitadas e necessárias para seu correto funcionamento: VLAN, Rotas estáticas ou dinâmicas, configuração SNMP, configuração de segurança, ACL, 802.1x e demais serviços coletados;
 - 1.7.2.1.4. Lista completa do mapeamento das portas dos switches core existentes.
- 1.7.2.2. Entrega de documentação de análise do ambiente;
- 1.7.2.2.1. Esse documento tem como objetivo demonstrar um diagnóstico do ambiente core existente, apontando seus riscos e deficiências. Com base nas melhores práticas, serão citadas configurações que estejam inconsistentes e protocolos que possam gerar divergência ou indisponibilidade da operação.
- 1.7.2.3. Entrega de Documentação de propostas e melhorias aplicáveis:
- 1.7.2.3.1. Esse documento tem como objetivo demonstrar as alternativas e melhorias que possam agregar valor na solução de core da LAN, resultando em um cenário mais seguro, com alta disponibilidade, aumento de desempenho (largura de banda), controle de acesso e interoperabilidade de protocolos;
- 1.7.2.3.2. Também contempla o planejamento de migração e substituição de hardware considerando as funcionalidades existentes e validando a suportabilidade na nova solução. Plano de endereçamento IP, segmentação de rede, configurações lógicas e físicas do ambiente serão abordados conforme necessário.

1.7.3. PROJETO DE INFRAESTRUTURA E CABEAMENTO

- 1.7.3.1. Os serviços consistem na passagem, instalação, retirada (cabeamento UTP), organização e identificação de pontos de telecomunicações e cordões ópticos no TJCE e Fórum;
- 1.7.3.2. Instalação de pontos de telecomunicações: a passagem de cordões ópticos de 25 e 50 metros do tipo OM4, nas tubulações e leitos existentes, entre os racks no Datacenter do TJCE e Fórum;
- 1.7.3.3. Identificação de todos os pontos de telecomunicações: identificar e mapear os pontos a serem instalados por meio de etiqueta visando atender as melhores práticas de cabeamento e infraestrutura;
- 1.7.3.4. Organização da Infraestrutura: acomodação de cordões ópticos nos racks, mantendo a devida organização exigida pelo TJCE;
- 1.7.3.5. Retirada de Cabeamento metálico: consiste na retirada de todo o cabeamento metálico do tipo UTP existente nas dependências do Datacenter TJCE e Fórum e refazer a espuma expansível



nos leitos;

1.7.3.6. Todos os procedimentos relacionados ao **item 3**, serão através de PML (Plano de mudança e Liberação) e devidamente autorizado pelo TJCE.

1.7.4. IMPLEMENTAÇÃO LÓGICA DA SWITCH CORE

1.7.4.1. Serviço de Instalação:

1.7.4.1.1. Compreende os serviços de instalação em rack, energização, conexão de portas de acesso, módulos e cabos de empilhamento, transceivers e ligação do cabeamento de rede (óptico e UTP).

1.7.4.2. Serviço de Configuração:

1.7.4.2.1. Ativação de módulos de interface e respectivos transceivers, de acordo com projeto de demandas da Contratante;

1.7.4.2.2. Configuração do padrão IEEE 802.3ad para realização a agregação entre os módulos;

1.7.4.2.3. Configuração de roteamento multicast;

1.7.4.2.4. Configuração de protocolo GVRP;

1.7.4.2.5. Configuração de controle de broadcast permitindo fixar o limite máximo de broadcasts por porta;

1.7.4.2.6. Configuração de controle de Multicast permitindo fixar o limite máximo de Multicasts por porta;

1.7.4.2.7. Configuração de controle de Unicast permitindo fixar o limite máximo de Unicasts por porta;

1.7.4.2.8. Configuração de roteamento IPv4 e IPv6, podendo ser utilizados um ou mais dos protocolos exigidos nas especificações técnicas;

1.7.4.2.9. Configuração de gerenciamento de banda identificando os fluxos através de listas de controle de acesso;

1.7.4.2.10. Configuração de gerenciamento de banda em valores absolutos em intervalos de 64 Kbps;

1.7.4.2.11. Configuração de mecanismos de controle de fila;

1.7.4.2.12. Configuração de protocolo NTP com autenticação;

1.7.4.2.13. Configuração de LLDP e LLDP-MED;

1.7.4.2.14. Configuração de módulos de Gerenciamento/Switch Fabric Redundantes;

1.7.4.2.15. Configuração de protocolo Spanning Tree e/ou Rapid Spanning Tree (802.3w) e/ou Multiple Spanning Tree (802.1s);

1.7.4.2.16. Configuração de BPDU Protection;

1.7.4.2.17. Configuração de módulos de interface, switch fabrics, ventiladores e fontes de



alimentação como hot-swappable;

- 1.7.4.2.18. Configuração de gerenciamento SNMP v1, v2c e v3, sendo v3 com Criptografia;
- 1.7.4.2.19. Configuração de gerenciamento RMON implementando no mínimo 2 grupos;
- 1.7.4.2.20. Configuração de gerenciamento por meio de interface web;
- 1.7.4.2.21. Configuração de espelhamento de portas de maneira remota;
- 1.7.4.2.22. Configuração de TELNET e TELNETv6;
- 1.7.4.2.23. Configuração de SSHv2;
- 1.7.4.2.24. Configuração através de console serial;
- 1.7.4.2.25. Configuração das VLANs de acordo com o projeto de segmentação da rede, segundo o protocolo IEEE 802.1Q por porta e IEEE 802.1v por protocolo;
- 1.7.4.2.26. Configuração de padrão IEEE 802.1x (network login), permitindo a configuração automática da VLAN e aplicação de ACL de acordo com o perfil do usuário;
- 1.7.4.2.27. Configuração de Guest VLAN;
- 1.7.4.2.28. Configuração de DHCP Snooping;
- 1.7.4.2.29. Configuração de ARP Proxy;
- 1.7.4.2.30. Configuração dos demais protocolos e serviços de rede utilizados pelo TJCE;
- 1.7.4.2.31. Configuração de listas de controle de acesso, devendo ser configuradas no mínimo 40 regras;
- 1.7.4.2.32. Todos os procedimentos relacionados ao item 1.7.4, serão através de PML (Plano de mudança e Liberação) e devidamente autorizado pelo TJCE.

2. VALIDAÇÃO DOS REQUISITOS TÉCNICOS FUNCIONAIS DA SWITCH DE NÚCLEO

2.1. O produto desta atividade deverá ser um relatório atestando a conformidade da solução com os requisitos técnicos e funcionais especificados. O prazo para conclusão desta atividade será de até 30 (trinta) dias corridos a partir da data de recebimento da Ordem de Serviço – OS, por parte da CONTRATADA e somente será aceito, após aprovação do TJCE;

2.2. Será dado o Aceite da atividade com o ambiente do TJCE completamente operacional.

3. Os procedimentos de validação deverão contemplar, no mínimo os itens abaixo Relacionados:

- 3.1.** Inspeção visual;
- 3.2.** Testes funcionais, incluindo o gerenciamento e a conectividade IP;
- 3.3.** Testes das configurações locais e em rede dos componentes;

- 3.4. Testes de integração com a rede de cabeamento estruturado existente;
- 3.5. Testes de integração com rede de longa distância existente;
- 3.6. Testes de integração com outros ativos das redes de dados locais existentes;
- 3.7. Testes de conectividade de uma estação de rede instalada em cada segmento de rede com os servidores;
- 3.8. Testes de funcionamento, com o sistema de suprimento de energia existente;
- 3.9. Testes de funcionamento, com o sistema centralizado de autenticação através do software de gerenciamento.

4. DOCUMENTAÇÃO TÉCNICA DO PROJETO

- 4.1. O produto desta atividade deverá ser o fornecimento dos documentos técnicos do projeto (as built), contendo todas as informações de configurações e instalações de acordo com o os testes funcionais conforme descritos no item anterior, procedimentos de contingência e demais informações necessárias para a devida operação e manutenção do switch de núcleo;
- 4.2. O prazo para conclusão desta atividade será de até 30 (trinta) dias corridos a partir da Emissão da OS e somente será aceito, após aprovação do TJCE;
- 4.3. A contratada deverá fornecer documentação técnica referente a todos os equipamentos e serviços fornecidos, devendo estar completa e atualizada, contendo os manuais, guias de instalação e outros pertinentes, sendo fornecida em sua forma original, não sendo aceitas cópias de qualquer tipo;
- 4.4. Esta documentação será analisada e aprovada pelo CONTRATANTE e será condicionante a aceitação final do projeto.

5. A documentação técnica do projeto deve apresentar no mínimo as seguintes características:

- 5.1. Informações do fabricante modelo e versão do switch núcleo e os softwares instalados;
- 5.2. Vista Frontal (Bay-face) e posterior dos switches;
- 5.3. Desenho em perspectiva da interligação dos dispositivos da solução proposta;
- 5.4. Desenho em perspectiva da topologia física e lógica da rede de computadores;
- 5.5. Informações de instalação e configuração de todos os equipamentos e da solução de gerenciamento fornecidos;
- 5.6. Outras informações que o TJCE e/ou a Contratada julguem necessárias para a documentação do projeto;
- 5.7. Os documentos de "as built" deverão ser entregues em papel e em mídia eletrônica, nos formatos compatíveis com o Microsoft Word ou LibreOffice Write e os desenhos digitalizados em formatos compatíveis com o Microsoft Visio;
- 5.1. Concluídos e homologados os serviços de instalação, configuração e migração e após a entrega da documentação, será emitido o Termo de Recebimento Definitivo, assinado pelo gestor do contrato.



LOTE 01

ANEXO IV – SOFTWARE DE GERÊNCIA

I. Quantidade: 01 (uma) unidade;

I.1. Deve ser fornecido com, no mínimo 1000 (Hum Mil) licenças, e deve gerenciar os equipamentos atuais do TJCE, que são:

EQUIPAMENTOS (Fabricante-Modelo)	QUANTIDADE (und.)
Switches Cisco – 3560	12
Switches Cisco – 2960	538
Roteadores Cisco – 1905	191
Roteadores Cisco – 3845	3
Controladoras de rede sem fio Cisco – 5508	2
Pontos de Acesso Cisco – 1142	200
Firewall Cisco – 5505	2
Firewall Cisco – 5550	26
RESERVA TÉCNICA	26

2. INSTALAÇÃO E CONFIGURAÇÃO DO SOFTWARE DE GERÊNCIA

2.1. O escopo do serviço Software de gerenciamento de Rede deve considerar, o planejamento, a instalação e a configuração da solução de gerenciamento integrada de rede. De acordo com as características e funcionalidades da ferramenta, o técnico da CONTRATADA fará as personalizações básicas e a integração com os dispositivos da rede local;

2.2. Deve ser do mesmo fabricante do switch fornecido;

2.3. Deve operar em modelo cliente-servidor utilizando Web Browser convencional como cliente ou software cliente do fabricante;

2.4. O conjunto composto pelo software de gerência mais o sistema operacional deve ser executado como uma máquina virtual em VMWARE ESX Server v5.0 ou superior;

2.5. Este item contempla o planejamento das atividades para implementação do software de gerência;

2.6. A contratada deverá conduzir uma reunião com a equipe do TJCE de levantamento dos dados;

2.7. Descrever a metodologia de avaliação e demonstrar o objetivo da atividade;

2.8. Definir os pré-requisitos para a coleta de dados;

2.9. Definir os processos operacionais de coleta de dados;

2.10. Fornecer recomendações iniciais e parâmetros operacionais para a coleta de dados;

- 2.11. Descrever configurações especiais e considerações sobre personalização para as ferramentas;
- 2.12. Analisar os dados e definir configurações a serem aplicadas nos equipamentos de rede envolvidos na solução;
- 2.13. Aplicar as configurações definidas a partir do Software de gerenciamento de Rede, nos equipamentos de rede que suportem a solução;
- 2.14. Executar os testes e validar se as funcionalidades foram aplicadas no equipamento;
- 2.15. Realizar a coleta de evidências;
- 2.16. Entende-se por instalação e configuração do software de gerência:
 - 2.16.1. A implantação da solução de gerenciamento de rede, no momento da instalação da switch de núcleo do DataCenter;
 - 2.16.2. A solução de gerenciamento de redes deverá ser implementada no momento da instalação da switch Core do DataCenter;
 - 2.16.3. A configuração compreende o serviço de instalação e ativação de licenças da Solução ofertada;
 - 2.16.4. A Configuração de arquitetura WEB, de forma a poder ser acessado por navegador de internet padrão;
 - 2.16.5. A Configuração de gerenciamento de capacidade, estado, configuração e uso dos recursos de rede, bem como dos serviços utilizados na rede e também dos usuários que tem permissão para acessar recursos da rede;
 - 2.16.6. A Configuração de funcionalidade de auto descobrimento de equipamentos na rede, exibindo a rede através de várias opções de visualização dos elementos descobertos: por topologia, por VLAN, por tipo de elementos, por uma visualização customizada com base na organização física dos equipamentos e por organização lógica dos mesmos;
 - 2.16.7. A Configuração de controle sobre quais usuários do sistema de gerência que terão permissão de gerência sobre os equipamentos e grupos de equipamentos, bem como deve ter o poder de restringir quais comandos podem ser implementados pelos usuários;
 - 2.16.8. A Configuração de monitoramento de performance, detecção de gargalos e outros problemas da rede, incluindo aqueles relacionados com a carga da CPU, uso da memória, utilização de banda, tempo de resposta e disponibilidade dos equipamentos;
 - 2.16.9. A Configuração de identificação das áreas mais carregadas da rede através de estatísticas sobre os maiores consumidores de recursos;
 - 2.16.10. A Configuração de limites de parâmetros que gerem alarmes em qualquer monitor, alertando rapidamente os operadores sobre qualquer questão considerada anormal;
 - 2.16.11. A Configuração de VLAN, QoS, ACL e outros parâmetros nos equipamentos da rede



que sejam compatíveis e que tenham suporte a essas funcionalidades;

2.16.12. A personalização dos modos de autenticação de acesso (802.1x, PAP, CHAP, EAPMD5, EAP-TLS, PEAP);

2.17. Caso o fabricante não possua solução de gerenciamento em software será aceita solução em appliance externo que implemente todas as funcionalidades solicitadas neste documento;

2.18. As licenças oferecidas deverão permitir a implementação e utilização de todos os módulos e todas as funcionalidades solicitadas neste documento, sem depender de integração com outros softwares fornecidos por outros fabricantes e sem ônus adicional para o TJCE;

2.19. Todo o licenciamento de software necessário para compor a solução de gerência deve estar incluído, no mínimo, pelo período de garantia do equipamento, inclusive o sistema operacional;

2.20. Todo o licenciamento deve ser feito em nome do TJCE. Não serão aceitas licenças temporárias, tampouco em nome de terceiros.

3. GERENCIAMENTO DE RECURSOS

3.1. Deve permitir a descoberta de elementos de rede através da faixa de endereços IP ou protocolo de descoberta de dispositivos;

3.2. Deve permitir a configuração, monitoramento, adição e gerência de um dispositivo e também de um grupo de dispositivos;

3.3. Deve gerar o mapa e permitir a visualização da topologia física da rede;

3.4. Deve permitir a customização dos mapas de topologia de rede, adicionar novos dispositivos e links e a visualização através do IP;

3.5. Deve gerar o mapa e permitir a visualização da topologia física da rede;

3.6. Deve permitir, através da interface gráfica, ativar cliente ssh ou telnet para acesso à interface CLI do equipamento;

3.7. Deve mostrar as estatísticas de utilização do Switch de Núcleo contemplando no mínimo utilização de memória e de CPU;

3.8. Deve permitir a visualização de informações dos dispositivos e componentes instalados, trazendo no mínimo, informações como fabricante, modelo, número de série, versão de hardware e software e outras informações que sejam disponibilizadas pelo equipamento gerenciado;

3.9. Realizar o inventário dos dispositivos;

4. GERÊNCIA DE CONFIGURAÇÃO E MUDANÇA

4.1. Deve permitir restaurar, comparar, aplicar e fazer o backup da configuração dos dispositivos gerenciados;

- 4.2. Deve permitir atualizar o software do dispositivo gerenciado;
- 4.3. Deve permitir a criação de modelos de configuração para serem aplicados aos dispositivos gerenciados;
- 4.4. Deve possuir capacidade de realizar atualização do sistema operacional ou firmware dos equipamentos que suportarem esse recurso.

5. GERENCIAMENTO DE FALHAS

- 5.1. Deve possuir capacidade de gerar alarmes a partir de traps SNMP e mensagens Syslog;
- 5.2. Deve possuir painel único de visualização dos alarmes e a partir desta tela verificar detalhes específicos de um alarme;
- 5.3. Exibir a disponibilidade do dispositivo.

6. GERENCIAMENTO DE DESEMPENHO

- 6.1. Deve possuir capacidade de monitorar o desempenho dos equipamentos gerenciados;
- 6.2. Deve possuir capacidade de monitorar a utilização de CPU, utilização de Memória, tráfego por porta.

7. GERÊNCIA DE LISTAS DE CONTROLE DE ACESSO

- 7.1. Deve permitir a visualização e configuração de listas de controle de acesso (ACL) nos equipamentos gerenciados e compatíveis;
- 7.2. Deve permitir a criação de templates ACLs para a distribuição em diversos equipamentos;
- 7.3. Deve permitir a criação de ACLs baseadas em endereço IP de origem e destino, porta TCP/UDP e horário de ativação.

8. GERÊNCIA DE VLANS

- 8.1. Deve possuir capacidade de configurar VLANs globalmente e individualmente por switch gerenciado compatível com a solução ofertada;
- 8.2. Deve possuir capacidade de configurar interface vlan.

9. ANÁLISE DE TRÁFEGO

- 9.1. Para a análise de tráfego, deverá ser disponibilizada 50 licenças;
- 9.2. Deve possuir interface gráfica de monitoramento de rede;
- 9.3. Deve fornecer informações em tempo real sobre o consumo de banda da rede;
- 9.4. Gerenciar os sistemas operacionais e *firmwares* dos equipamentos com ferramenta para upgrade



em lote. Caso este sejam suportados;

- 9.5. Deve possibilitar o monitoramento de rede nas camadas ISO 4 a 7;
- 9.6. Deve possibilitar a verificação do fluxo de dados da rede através da emissão de relatórios baseados na coleta de fluxos, análise e processamento dos dados da rede;
- 9.7. Deve possuir a capacidade de definir os dados recebidos pelo software de monitoramento, como estes dados devem ser interpretados e como serão apresentados para os administradores de rede;
- 9.8. Deve possuir licenças necessárias para o monitoramento de trafego, no quantitativo de 50 (cinquenta) licenças;
- 9.9. Deve suportar o monitoramento de equipamentos de rede geradores de fluxos de dados baseados em protocolos NetFlow V5 (ou superior) ou SFlow v5 (ou superior);
- 9.10. Deve possibilitar a visualização, adição, modificação e remoção dos dispositivos geradores de fluxo monitorados.

10. AUDITORIA E RELATÓRIOS DE TRÁFEGO

- 10.1. Deve permitir a configuração de filtros para definir quais fluxos de dados recebidos pelo software serão analisados ou descartados;
- 10.2. Deve possibilitar a visualização gráfica das estatísticas de sessões de origem dos dispositivos IP ou hosts gerenciados;
- 10.3. Deve suportar a configuração de filtros de fluxo de dados baseados em, no mínimo, endereço IP de origem e destino, número de porta e protocolo;
- 10.4. Deve fornecer gráfico com as sessões estabelecidas entre todos os dispositivos IP ou hosts configurados durante a última hora;
- 10.5. Deve fornecer relatórios de análise de trafego que demonstrem a taxa média de trafego de entrada e saída para todas as interfaces de rede monitoradas. Deve ser possível identificar, através destes relatórios, as estatísticas de utilização de um link, além do volume médio, mínimo e máximo do trafego monitorado;
- 10.6. Gerar gráficos de utilização da rede;
- 10.7. Gerar histórico de uso por protocolo.

11. RELATÓRIOS

- 11.1. Deve possuir capacidade de gerar relatórios ou exportar dados de:
 - 11.1.1. Ativos de Rede;
 - 11.1.2. Estado dos dispositivos e Links;
 - 11.1.3. Estatísticas de Links de conectividade;

11.1.4. Informações sobre os dispositivos ativos;

11.1.5. Topologia.

12. SERVIÇOS DE AUTENTICAÇÃO E AUTORIZAÇÃO

12.1. Deve ser baseado em servidor RADIUS para centralizar o gerenciamento de autenticação, autorização e "accounting" (AAA) dos dispositivos utilizados para a conexão e uso dos serviços da rede;

12.2. Deve implementar o protocolo Tacaes+ ou RADIUS;

12.3. Deve implementar autenticação dos operadores para acesso aos equipamentos gerenciados;

12.4. Deve monitorar e registrar as atividades dos operadores sobre os equipamentos gerenciados;

12.5. Deve implementar o controle de acesso para operadores acessando através de SSH, Telnet e FTP;

12.1. Deve permitir a autenticação através de certificados digitais auto-assinados ou gerados no formato ICP-Brasil.



LOTE 01

ANEXO V – TREINAMENTO

1. A CONTRATADA deverá ministrar treinamento e disponibilizar o material didático. O conteúdo do treinamento, deverá abordar o Software de Gerência (**Item 4 do LOTE 01 descrito no item 3**) e a solução a ser adquirida (**Item 1 e seus subitens e item 2 e seus subitens do LOTE 01 descritos no item 3**) ser ministrado em língua portuguesa, deverá contemplar os seguintes itens:
 2. Transferência de conhecimento (hands-on e mentoring);
 3. Visão geral dos recursos e funcionalidades da solução;
 4. Overview e considerações sobre a arquitetura do produto e sobre o Software de Gerência (**Item 4 do Item 3. DESCRIÇÃO DA SOLUÇÃO**);
 5. Tarefas básicas de administração, monitoração e manutenção:
 - 5.1. Planejamento de recursos para instalação;
 - 5.2. Instalação, configuração e administração;
 - 5.3. Todos os procedimentos necessários à instalação física e lógica, configuração técnica e à completa operação dos produtos;
 - 5.4. Gerenciamento de recursos;
 - 5.5. Configuração de dispositivos;
 - 5.6. Gerenciamento de planos de recuperação de dados;
 - 5.7. Criação de políticas;
 - 5.8. Troubleshooting e resolução de problemas comuns;
 - 5.9. Todos os procedimentos de manutenção dos produtos;
 - 5.10. Cobrir adequadamente os conhecimentos necessários para administração, configuração, otimização, troubleshooting e utilização da solução;
 - 5.11. Foco na implementação e manutenção do ambiente de produção;
 - 5.12. Planejamento e implementação de projeto de disaster recovery utilizando a ferramenta;
 - 5.13. Planejamento de capacidade;
 - 5.14. Análise de riscos;
6. A CONTRATADA deverá ministrar o treinamento para no mínimo 06 (seis) Servidores, indicados pela Secretaria de Tecnologia da Informação do TJCE;
7. Deverá ser presencial na cidade de Fortaleza/CE, nas dependências do TJCE e ministrada por profissional certificado pelo fabricante do produto ofertado, com duração mínima de 4 horas por dia;
8. Realizar laboratórios práticos entre cada unidade de conhecimento;

9. Disponibilizar para todos os participantes, material didático, atualizado e de primeiro uso, que aborde os tópicos sugeridos, preferencialmente em português ou inglês;
10. Os demais custos envolvidos para realização do Treinamento serão de responsabilidade da CONTRATADA;
11. A data de realização deverá ser definida com 30 (trinta) dias de antecedência pelo CONTRATANTE;
12. O prazo para início do serviço de treinamento será de no máximo 30 (trinta) dias corridos após emissão da Ordem de Serviço pelo CONTRATANTE;
13. A CONTRATADA deverá comprovar ser parceira autorizada do fabricante, através de Carta ou Certificado emitido, ou de seu representante legal no Brasil;
14. Ao final de cada treinamento será realizada uma avaliação da qualidade do mesmo, o não atendimento satisfatório implicará na realização de um novo treinamento sem ônus adicional ao TJCE. Para o treinamento ser considerado satisfatório, o mesmo deverá atingir o valor mínimo de 60% (sessenta por cento) de satisfação da turma;
15. A CONTRATADA deverá emitir para o servidor participante, sem ônus para o TJCE e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária;
16. A carga horária total do treinamento será de 80 (oitenta) horas;
17. A carga horária mínima do treinamento não poderá ser inferior a 20 (vinte) horas semanais;
18. A CONTRATADA deverá arcar com todas as despesas para realização do treinamento, tais como material didático, instrutores (passagens, diárias e deslocamentos), e quaisquer outras despesas diretas ou indiretas.

LOTE 01

ANEXO VI – CORDÕES ÓPTICOS E ACESSÓRIOS

1. CORDÕES ÓPTICOS E ACESSÓRIOS

1.1. Cordão óptico Duplex Multimodo (50), tipo OM4, 10 GIGABIT LC-SPC/LC-SPC de 25 metros de comprimento:

1.1.1. **Quantidade:** 160 (cento e sessenta) unidades;

1.2. Cordão óptico Duplex Multimodo (50), tipo OM4, 10 GIGABIT LC-SPC/LC-SPC de 50 metros de comprimento:

1.2.1. **Quantidade:** 80 (oitenta) unidades;

1.3. Estes cordões deverão ser constituídos por um par de fibras ópticas multimodo 50/125 (cor amarela), tipo “tight”;

1.4. Utilizar padrão “zip-cord” de reunião das fibras para diâmetro nominal de 2mm;

1.5. A fibra óptica destes cordões deverão possuir revestimento primário em acrilato e revestimento secundário em PVC;

1.6. Sobre o revestimento secundário deverão existir elementos de tração e capa em PVC não propagante à chama;

1.7. As extremidades destes cordões ópticos duplos devem vir devidamente conectorizadas e testadas de fábrica;

1.8. O fabricante deverá apresentar certificados ISO 9001 e ISO 14001;

1.9. Possuir impresso na capa externa nome do fabricante, identificação do produto e data de fabricação;

1.10. Os cordões devem estar de acordo com a norma ABNT 14106;

1.11. Os conectores ópticos devem atender os requisitos mínimos previstos na norma ABNT NBR 14433;

1.12. O fabricante deve estar totalmente de acordo com normas e certificações aplicáveis;

1.13. Os cabos (cordões) ópticos deverão possuir certificação ANATEL.

1.14. Cabo Direct Attach

1.14.1. **Quantidade:** 24 (vinte e quatro) unidades, de no mínimo 5 metros, cada.

1.14.1.1. Cabo direct attach com SFP+ GBICS 10G nas duas pontas. Sendo metálico ou fibra óptica, já conectorizado ou soldado.



ANEXO VII – SWITCH DE ACESSO

1.1. CARACTERÍSTICAS

1.1.1. Quantidade: 50 (cinquenta) unidades;

1.1.2. GERENCIAMENTO

- 1.1.2.1. Deve possuir LEDs indicativos do estado de funcionamento do equipamento;
- 1.1.2.2. Deve permitir a atualização de versões de código utilizando os protocolos FTP ou TFTP;
- 1.1.2.3. Deve suportar o protocolo Secure Copy Protocol (SCP) ou File Transfer Protocol (FTP) para cópias seguras de arquivos de configuração do switch;
- 1.1.2.4. Deverá implementar mecanismos de monitoramento e análise local e remota de tráfego em portas de *switches* pertencentes a uma mesma VLAN, através de configuração de espelhamento de portas;
- 1.1.2.5. Deve implementar comandos de traceroute para o descobrimento do caminho seguido por um pacote dentro da rede;
- 1.1.2.6. Deve permitir enviar logs para servidores remotos (Syslog);
- 1.1.2.7. O equipamento deve implementar ajuste de clock utilizando NTP;
- 1.1.2.8. Deve possibilitar a criação de perfis de configuração da porta para cada tipo de máquina, como switches, roteadores, servidores, estações, telefones IP, Pontos de Acesso, que será conectada ao switch;
- 1.1.2.9. Deve estar equipado com recursos que implementem funcionalidades de gerenciamento relativas ao padrão de gerenciamento SNMP (Simple Network Management Protocol), com suporte a RFC 1213 (MIB-II). Deve suportar SNMP v1, v2 e v3;
- 1.1.2.10. Permitir a monitoração de desempenho de tráfego entre o switch e outro equipamento via MIB SNMP;
- 1.1.2.11. Deve estar equipado com recursos que implementem funcionalidades de gerenciamento relativas aos padrões de gerenciamento RMON (Remote Network Monitor), com suporte a RFC 1757. Ou RFC 2819;
- 1.1.2.12. Possuir suporte nativo a 4 grupos de RMON(History, Statistics, Alarms, Events).
- 1.1.2.13. Possuir porta do console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232. (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
- 1.1.2.14. Deve ser gerenciável via SSH versão 2 (SSHv2) suportando, no mínimo, o algoritmo de criptografia 3DES;

A



1.1.2.15. Deverá estar equipado com recursos que permitam o gerenciamento através de TELNET;

1.1.2.16. Deverá estar equipado com recursos que permitam o gerenciamento através de *web browser* com suporte a SSL (*Secure Socket Layer*) versão 3;

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

1.1.3. CAPACIDADE DE PROCESSAMENTO

1.1.3.1. Capacidade mínima de encaminhamento de pacotes na camada 2 (modelo OSI), em 6,5 milhões de pacotes por segundo, com a qual cada equipamento deverá estar equipado;

1.1.3.2. Capacidade mínima de comutação em 16 Gbps, com a qual cada equipamento deverá estar equipado;

1.1.4. PORTAS INSTALADAS

1.1.4.1. Quantidade mínima de 24 portas com interfaces RJ-45, padrão 10/100BaseT que deverão estar instaladas em cada comutador (switch);

1.1.4.2. Quantidade mínima 02 de portas com interfaces RJ-45, padrão 1000BaseT ou Small Form-Factor Pluggable (SFP) padrão IEEE802.3z, que cada comutador (switch) deverá possuir, com suporte a diversos transceivers SFP conforme padrão IEEE 802.3z, incluindo 1000BASE-SX, 1000BASE-LS/LH OU 1000BASE-ZX OU 1000BASE-CWDM. Essas portas devem permitir que o usuário escolha se vai utilizar as portas 10/100/1000 Ethernet ou a SFP-based Gigabit Ethernet, sendo que somente uma estará ativa por vez;

1.1.4.3. Deverá implementar o aumento da largura de banda através da agregação de até 8 portas físicas iguais funcionando como uma única porta lógica, conforme padrão IEEE 802.3ad;

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

1.1.4.5. Deve suportar Jumbo Frames de até 9000 bytes.

1.1.5. RECURSOS DE REDUNDÂNCIA

1.1.5.1. Possuir suporte ao Protocolo Spanning-Tree Protocol (IEEE 802.1d);

1.1.5.2. Deve implementar mecanismos de minimização do tempo de convergência de Spanning-Tree em caso de falha de enlace ou switch da rede local nas seguintes funcionalidades: configuração da porta para o estado de forwarding automaticamente, manutenção da raiz do Spanning-

Tree (STP Root Guard ou similar) e detecção de tráfego Spanning-Tree com opção de desabilitação da porta em caso de detecção positiva;

- 1.1.5.3. Deve implementar o protocolo Rapid Spanning Tree (IEEE 802.1w);
- 1.1.5.4. Deve implementar o protocolo Multiple Spanning Tree (IEEE 802.1s);
- 1.1.5.5. Implementar o padrão IEEE 802.1s com suporte a no mínimo 32 instâncias simultâneas do protocolo Spanning Tree;
- 1.1.5.6. Deve implementar os protocolos UDLD ou DLDAP, para detecção de links com tráfego unidirecional.

1.1.6. VLANs

- 1.1.6.1. Quantidade mínima de 255 (duzentos e cinquenta e cinco) VLAN's que deverão ser suportadas simultaneamente;
- 1.1.6.2. Deve implementar o protocolo de trunking IEEE 802.1q para que o tráfego de várias VLANs possa passar por um enlace. O switch deve implementar protocolo de negociação de trunking;
- 1.1.6.3. Deve implementar a configuração de uma VLAN de voz em cada porta para a separação do tráfego de telefonia IP;
- 1.1.6.4. Permitir a criação, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q através do protocolo VTP, GVRP ou equivalente.

1.1.7. DHCP

- 1.1.7.1. Possuir suporte a DHCP Server e DHCP Relay;
- 1.1.7.2. Possuir mecanismo de proteção contra mensagens DHCP não confiáveis, através do mecanismo DHCP Snooping;
- 1.1.7.3. Deve possuir a funcionalidade de download automático de imagens de software e configuração para um ou mais switches através de um DHCP server. Essa funcionalidade assegura que cada novo switch utilizado na rede possua a mesma imagem de software.

1.1.8. MULTICAST

- 1.1.8.1. Implementar IGMP Snooping para otimização de IP Multicast;
- 1.1.8.2. Deve suportar no mínimo 64 diferentes grupos IGMP.

1.1.9. IPv6

- 1.1.9.1. Gerenciamento básico de IPv6, contemplando suporte a endereçamento unicast, ICMPv6, Secure Shell (SSH) for v6, Telnet, DNS entre outros.

1.1.10. SEGURANÇA

- 1.1.10.1. Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas “isoladas” e portas “promíscuas”, de modo que “portas isoladas” não se comuniquem com outras “portas isoladas”, mas tão somente com as portas promíscuas de uma dada VLAN;
- 1.1.10.2. Permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao switch via Telnet. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- 1.1.10.3. Implementar ACLs baseadas em Portas (Ethernet) Físicas do Switch;
- 1.1.10.4. Deve implementar Listas de Controle de acesso baseadas em Tempo;
- 1.1.10.5. Suportar autenticação, autorização e “accounting” via RADIUS;
- 1.1.10.6. Deve suportar autenticação de login/senha para a liberação de tráfego na porta através do protocolo IEEE 802.1x com as seguintes funcionalidades: atribuição de VLAN conforme a autenticação do usuário, posicionamento da porta em uma VLAN “de convidados” caso não haja falha de autenticação, reautenticação forçada de todas as portas, reautenticação periódica e definição de período de inatividade após falha de autenticação;
- 1.1.10.7. Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional;
- 1.1.10.8. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;
- 1.1.10.9. Implementa mecanismos de AAA (“Authentication”, “Authorization” e “Accounting”) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA;
- 1.1.10.10. Criptografa todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- 1.1.10.11. Permitir controlar quais comandos os usuários e grupos de usuário podem executar nos equipamentos gerenciados. Devem ser registrados no servidor AAA todos os comandos executados, assim como todas as tentativas de execução de comandos não autorizadas feitas por usuários que tiverem acesso ao equipamento gerenciado;
- 1.1.10.12. Deve permitir a configuração de portas confiáveis e não confiáveis de forma a manter uma tabela correlacionando informações como porta, VLAN, IP, MAC para cada interface não confiável. Os servidores DHCP, por exemplo, devem estar conectados a interfaces confiáveis, pois qualquer resposta a uma solicitação DHCP será descartada em interfaces não confiáveis. Tal funcionalidade garante maior segurança e controle das redes LAN;
- 1.1.10.13. Deve possuir capacidade de limitação de endereços MAC por porta;
- 1.1.10.14. Suportar a visualização de endereços MAC aprendidos pelo Switch;
- 1.1.10.15. Deve permitir a autenticação de um cliente via endereço MAC caso não seja suportado a funcionalidade IEEE 802.1x;
- 1.1.10.16. Possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.

1.1.11. QoS

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

1.1.11.1.1. Prioridade Estrita;

1.1.11.1.2. Weighted Round Robin (WRR) ou Shaped Round Robin (SRR).

1.1.11.2. Implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

1.1.11.3. Deve suportar configuração automática de QoS para VoIP através de um único comando de CLI ou vir configurado de fábrica;

1.1.12. PROTOCOLOS DE ROTEAMENTO

1.1.12.1. Deve implementar roteamento estático;

1.1.12.2. Deve suportar no mínimo 16 (dezesesseis) rotas estáticas IPv4 (Unicast).

1.1.13. ESTRUTURA

1.1.13.1. Deve possuir estrutura apropriada para acondicionamento em armário de fiação (*rack*) de 19" polegadas;

1.1.13.2. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19" polegadas.

1.1.14. SISTEMA DE ALIMENTAÇÃO

1.1.14.1. A fonte alimentação deverá funcionar com tensão elétrica nominal de 100V~240V AC, 50~60Hz, de modo automático;

1.1.14.2. Possuir suporte opcional para fonte de alimentação redundante garantindo tolerância a falhas e disponibilidade da rede. Essa fonte pode ser externa ao equipamento, mas obrigatoriamente deve ser do mesmo fabricante.

1.1.15. DOCUMENTAÇÃO

1.1.15.1. Deverá ser acompanhado de documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

ANEXO VIII – GARANTIA



1. Todos os equipamentos, acessórios e softwares deverão possuir garantia do tipo NBD (Next Business Day) do fabricante, disponível 24 (vinte e quatro) horas por dia, durante os 07 (sete) dias na semana, pelo período de no mínimo 36 (trinta e seis) meses contados a partir da data de emissão do Termo de Recebimento Definitivo, com quantitativo ilimitado de requisições de chamados, podendo o atendimento ser presencial ou remoto. Compreendendo toda e qualquer configuração, instalação de atualizações, patches e fixes de software. Devendo ser capaz de detectar problemas de software e hardware e emitir relatório ao TJCE que indique a necessidade de abertura de chamado com o fabricante para solicitar o serviço de garantia. Sendo a CONTRATADA responsável pela execução da garantia.
2. Os chamados referentes a problemas nos equipamentos, partes, componentes e softwares, seja reparação ou garantia, deverão ser abertos diretamente com a CONTRATADA e gerenciados pela mesma através de número telefônico 0800 ou equivalente a ligação gratuita, fornecendo neste momento o número, data e hora de abertura do chamado. A data e a hora do registro do chamado será considerado o início para contagem dos prazos estabelecidos;
3. O prazo para solução do problema compreende o tempo entre o registro do chamado ate a efetiva solução do problema. Os Níveis Mínimos de Serviços ou prazos para solução do problema estão descritos na tabela abaixo:

NÍVEL DE SEVERIDADE	DESCRIÇÃO	Prazo para Solução
1	Um problema que tenha um impacto crítico na capacidade do CONTRATANTE em manter sua infraestrutura ativa. Um número significativo de usuários da rede é incapaz de executar adequadamente as suas tarefas. O sistema e/ou a rede estão inoperantes ou severamente degradados.	2 horas
2	Um problema que tenha um impacto na capacidade do CONTRATANTE em manter sua infraestrutura ativa, cuja severidade seja significativa, porém não crítica, e que possa ser de natureza repetitiva. O funcionamento da rede ou do produto é afetado, mas o desempenho não foi severamente degradado.	4 horas
3	Um problema que não cause impacto na capacidade do CONTRATANTE em manter sua infraestrutura ativa.	6 horas
4	Suporte para ajustes ou otimizações.	8 horas

4. Na impossibilidade de solução definitiva do problema no prazo estabelecido, obriga-se a CONTRATADA a disponibilizar para uso imediato, nas instalações do TJCE, outros equipamentos,

peças ou componentes e também softwares de características iguais e/ou superiores ao que está sendo objeto da garantia, sem qualquer ônus ao TJCE;

5. Caso seja impossível a substituição dos equipamentos, componentes, materiais ou peças por outros que não os que compõem o item proposto, esta substituição obedecerá ao critério de compatibilidade, que poderá ser encontrado no site do fabricante, por meio de equivalência e semelhança e só poderá ser efetuada mediante expressa autorização por escrito do CONTRATANTE, para cada caso particular. Caso o CONTRATANTE recuse o equipamento, componente, material e/ou peça a ser substituído, a CONTRATADA deverá apresentar outras alternativas, porém o prazo para solução do problema não será alterado;

6. Para prestar os serviços de correção a erros ou falhas, a CONTRATADA deverá possuir, no mínimo, um técnico com experiência e formação técnica certificada pelo fabricante nos equipamentos e softwares deste documento e que já tenha prestado serviços similares aos solicitados neste documento. A formação técnica deverá ser comprovada através de certificado no equipamento e software emitidos pelo fabricante e a experiência em serviços similares aos solicitados neste documento deverá ser comprovada mediante apresentação de Atestado de Capacidade Técnica – ACT, fornecidos por pessoa jurídica de direito público ou privado;

7. Todo atendimento deverá ser acompanhado de relatório técnico detalhado, que explicita o diagnóstico e a solução implementada;

8. Para a correção de erros ou falhas, a CONTRATADA deverá utilizar apenas peças e componentes novos, de primeiro uso e originais do fabricante dos equipamentos, ou homologadas pelo mesmo. Caso haja a descontinuidade de fabricação dos componentes deverá ser garantida a total compatibilidade dos itens substituídos com os originalmente fornecidos.



ANEXO IX – MODELO DE ORDEM DE SERVIÇO OU FORNECIMENTO DE BENS – OS/OF

(PJSETINAAAANN, se for projeto) – (Nome do Projeto/Contratação)

IDENTIFICAÇÃO

Data de Emissão:	(DD/MM/AAAA)	Emergencial: Sim () Não ()
OS/ OF:	<Identificação da Ordem de Serviço ou de Fornecimento de Bens>	
Nome do Projeto / Sigla:	<identificação única do projeto e sigla quando houver>	
Contratada/Nº Contrato:	<Identificação do nome da contratada e Nº do contrato>	
Requisitante:	<identificação da área requisitante>	

ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS E VOLUMES

<Relação dos entregáveis que compõem a OS/OFB>

ID	Produto / Serviço	Métrica	Quant	Valor RS
1	<Descrição dos produtos e/ou serviços requisitados na OS/OFB>	<Descrição da unidade de medida para avaliação do serviço ou fornecimento para o item relacionado>		RS 0,00
2				RS 0,00
Total				RS 0,00

Instruções Complementares

<Descrever instruções necessárias à execução da OS/OFB>

- Realizar a modelagem dos processos relativos às aquisições de soluções de TI.
- Elaborar...
- <...>
- <...>

CRONOGRAMA

ID	Tarefa	Início	Termino
1	<Descrição das tarefas incluídas na OS/OFB>	<Data de início da tarefa>	<Data de Término da tarefa>
2		00/00/00	00/00/00

DOCUMENTOS ENTREGUES

<Descrever os documentos que foram entregues a contratada acompanhado da OS/OF, para subsidiar a execução do(s) serviço(s) ou a entrega do(s) bem(ns)>

()	()
()	()
()	()

DATAS E PRAZOS

Data Prevista para Início dos Produtos / Serviços	Data Prevista para Entrega dos Produtos / Serviços	Prazo Total do Contrato (com a Garantia)
(DD de MMMM de AAAA)	(DD de MMMM de AAAA)	(DD de MMMM de AAAA)

APROVAÇÕES

<Ao final, assinam o Gestor do Contrato, o Fiscal Requisitante (ou o Responsável pelo Projeto na área requisitante) e o preposto, que preenche também a data de recebimento do artefato>

 (Nome) – (Matrícula)
 Área/Fiscal Requisitante da Solução - Contratante

 (Nome) – (Matrícula)
 Gestor do Contrato - Contratante

 (Nome) – (Qualificação)
 Preposto - Contratada

Fortaleza, (DD de MMMM de AAAA)

ANEXO X – MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO



IDENTIFICAÇÃO

Contrato Nº		N. da OS/OFB
Objeto		
Contratante		
Contratada		CNPJ

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 34, inciso I, da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 11/09/2014, que os serviços (ou bens), relacionados na OS identificada, foram recebidos nesta data e serão objetos de avaliação quanto à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo CONTRATANTE.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até (DD) dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

APROVAÇÃO

<Ao final, assinam o Fiscal Técnico e o Preposto, preenchendo-se a data de aprovação do artefato>

Fiscal Técnico
(Nome) - (Matrícula)

Preposto
(Nome) - (Qualificação)

Fortaleza, (DD de MMMM de AAAA)

ANEXO XI – MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

IDENTIFICAÇÃO

Contrato Nº	N. da OS/OFB
Objeto	
Gestor do Contrato	
Fiscal Requisitante do Contrato	

Por este instrumento, os servidores acima identificados atestam, para fins de cumprimento do disposto no art. 34, inciso VIII, da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 11/09/2014, que o(s) serviço(s) ou bem(ns) integrante(s) da Ordem de Serviço ou de Fornecimento de Bens acima identificada possui(em) qualidade compatível com a especificada no Termo de Referência/Projeto Básico do Contrato supracitado.

APROVAÇÃO

<Ao final, assinam o Fiscal Requisitante e o Gestor do Contrato, preenchendo-se a data de aprovação do artefato>

Fiscal Requisitante
(Nome) – (Qualificação)

Gestor do Contrato
(Nome) - (Matrícula)

Fortaleza, (DD de MMMM de AAAA)

Ciente,



ANEXO XII – MODELO DE TERMO DE COMPROMISSO – TC

PJSETIN(AAAAANN) – (Nome do Projeto/Contratação, se for projeto)



CONDIÇÕES DO TERMO

O (NOME DO ÓRGÃO), sediado em (ENDEREÇO), CNPJ n.º (CNPJ), doravante denominado CONTRATANTE, e, de outro lado, a (NOME DA EMPRESA), sediada em (ENDEREÇO), CNPJ n.º (CNPJ), doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º DD/AAAA doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 4.553 de 27/12/2002 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Primeira – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

I - Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

II - Informação Pública ou Ostensiva: é aquela cujo acesso é irrestrito, obtida por meio de divulgação pública ou por meio de canais autorizados pelo CONTRATANTE.

III - Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

IV - Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar

A handwritten signature in blue ink, located at the bottom right of the page.

qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

V - Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- I – Sejam comprovadamente de domínio público no momento da revelação;
- II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte



exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação,

caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretroatável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser



exercidos a qualquer tempo;

IV – Todas as condições, Termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessária a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

A CONTRATANTE elege o foro da (CIDADE DA CONTRATANTE), onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

De Acordo

<Ao final, assinam um representante do contratante e da contratada, preenchendo-se a data de aprovação do artefato>

_____ Contratante (Nome do Contratante) (Matricula)	_____ Contratada (Nome da Contratada) (Qualificação)
_____ Testemunha 1 (Nome) (Qualificação)	_____ Testemunha 2 (Nome) (Qualificação)

Fortaleza, (DD de MMMM de AAAA)

ANEXO XIII – MODELO DE TERMO DE CIÊNCIA – TCI

(PJSETINAAAANN, se for projeto) – (Nome do Projeto/Contratação)

FINALIDADE

Este documento tem como finalidade obter comprometimento formal dos empregados da contratada diretamente envolvidos nos projeto sobre o conhecimento da declaração e manutenção de sigilo e das normas de segurança vigentes na instituição.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO.

Contrato Nº:	
Objeto:	
Gestor do Contrato	Matricula:
Contratante:	
Contratada:	CNPJ
Preposto da Contratada:	CPF

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.

CIÊNCIA E APROVAÇÃO

(Nome) – (Matricula)
Preposto da Contratada

(Nome) – (Matricula)
Funcionário

(Nome) – (Matricula)
Funcionário

(Nome) – (Matricula)
Funcionário

(Nome) – (Matricula)
Funcionário

(Nome) – (Matricula)
Funcionário

Fortaleza, (DD de MMMM de AAAA)

ANEXO XIV – TOPOLOGIAS



Figura 1: TOPOLOGIA ATUAL

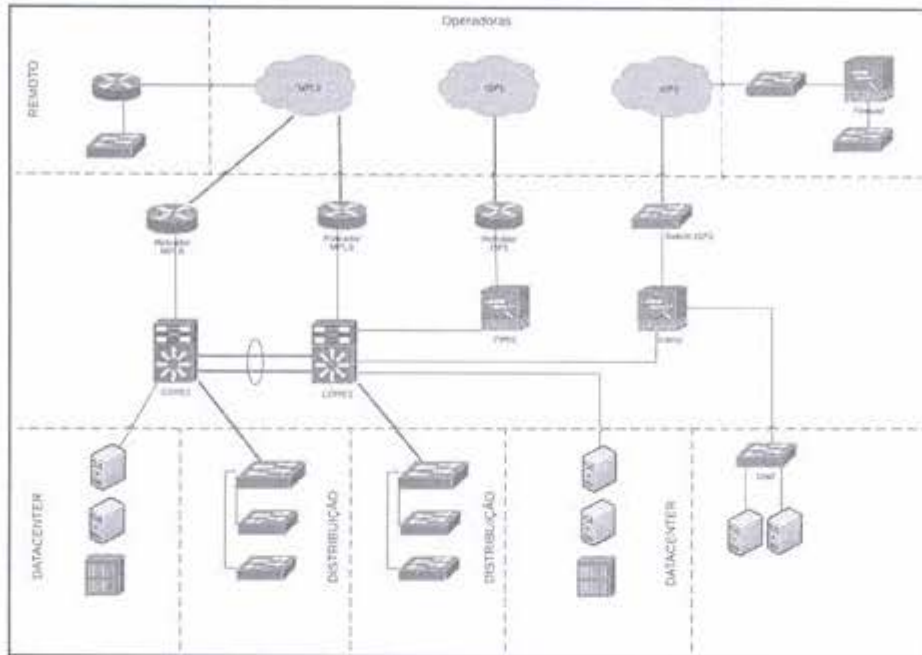
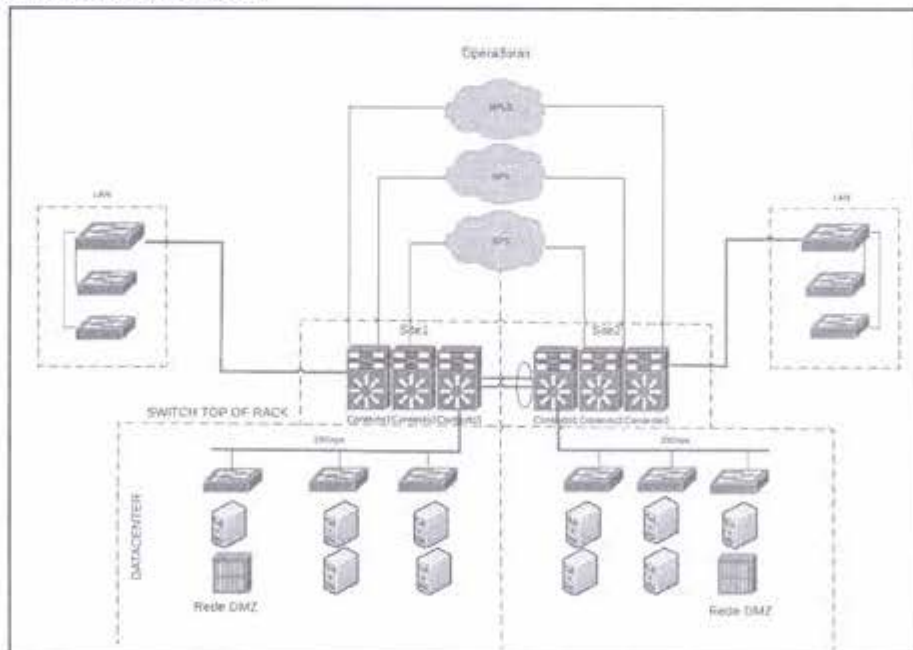


Figura 2: TOPOLOGIA PROPOSTA



Plano de Mudança e Liberação

Descrição:	[Preencher]
Solicitante:	[Preencher]
Data da Solicitação:	[Preencher]





Autorizadores

Nome	Cargo
Andrea Antunes de Carvalho	Chefe de Serviço de Suporte Técnico
Cristiano Henrique Lima de Carvalho	Diretor da Divisão de Segurança da Informação

2. Motivação da Mudança

[Preencher]

3. Descrição da Mudança

[Preencher]

4. Janela de Execução

Horário Previsto	Data Prevista
[Horário para execução]	[Data da execução]

5. Serviços Afetados

Nome do Serviço	IC Relacionado	Impacto Previsto
[Preencher]	[Preencher]	[Preencher]

6. Plano de Comunicação [preencher ou remover se necessário.]

Nome Parceiro / Contratado / Funcionário	Motivo
Grupo Notificação de PML	Comunicar ao final da atividade (notificacao.pml@tjce.jus.br)

A

7. Material necessário [descrição de material extra, necessário para a mudança]

Descrição	Motivo	Quantidade
[Preencher]	[Preencher]	[Preencher]

8. Detalhamento de Execução

ITEM	ATIVIDADE	HORAS PREVISTAS	RESPONSÁVEL
	[Preencher]	[Preencher]	[Preencher]
	[Preencher]	[Preencher]	[Preencher]

TEMPO TOTAL DA ATIVIDADE	[Preencher]
--------------------------	-------------

9. Plano de contingência / rollback

[Preencher em caso de retornar ao estado anterior a mudança]

10. Necessidades Adicionais

ITEM	OPÇÃO	DESCRIÇÃO
CMDB	[sim / não]	Incluir / Alterar / Excluir do CMDB a informação do IC
Backup	[sim / não]	Solicitar a INCLUSÃO na política de backup
Backup	[sim / não]	Solicitar EXCLUSÃO da política de backup
Antivirus	[sim / não]	Solicitar remoção da console do Antivirus
Monitoramento	[sim / não]	Solicitar a INCLUSÃO no sistema de monitoramento
Monitoramento	[sim / não]	Solicitar a EXCLUSÃO no sistema de monitoramento



Firewall	[sim / não]	Solicitar a INCLUSÃO de regras no firewall
Firewall	[sim / não]	Solicitar a EXCLUSÃO de regras no firewall
Registro no DNS	[sim / não]	Solicitar a EXCLUSÃO do registro no DNS

11. Documentação a Ser Atualizada

ARQUIVO	LOCAL
[Preencher]	[Preencher]

12. Equipe Necessária

NOME	ESPECIALIDADE
Marcelo Oliveira	Coordenador de Mudanças

13. Revisão Pós-implementação

[Preencher com testes ou verificações para após a mudança]

