12121843 08006.000602/2020-71

Ministério da Justiça e Segurança Pública
Secretaria-Executiva
Diretoria de Tecnologia da Informação e Comunicações
Coordenação-Geral de Infraestrutura e Serviços
Coordenação de Infraestrutura de TIC

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO
PROCESSO 08006.000602/2020-71

1 - INTRODUÇÃO

1.1. Conforme previsto no artigo 11 da INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019, a elaboração dos Estudos Técnicos Preliminares da Contratação serve essencialmente para definição e especificação das necessidades de negócio e tecnológicas, e dos requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição. A análise comparativa de soluções, deve considerar, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

1.2. É na elaboração dos Estudos Técnicos Preliminares da Contratação que diversos aspectos devem ser levantados com maior profundidade para que os gestores se certifiquem, de que através de uma necessidade da área de negócio, claramente definida, há condições de atendê-la, tendo como premissa que os riscos de atendê-la são gerenciáveis e os resultados pretendidos com a contratação valem o preço estimado inicialmente, além de embasar a elaboração do Termo de Referência ou o Projeto Básico, que somente é elaborado se a contratação for considerada viável.

1.3. A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica da aquisição de equipamentos de rede de dados para a modernização e expansão da capacidade, incluindo novos ativos de núcleo e de camada de agregação, contemplando os serviços de instalação e suporte técnico com garantia pelo período de 60 meses para atendimento das necessidades do Ministério da Justiça e Segurança Pública (MJSP).

Referência: Art. 11 da IN SGD/ME nº 1/2019.

2 - DEFINIÇÃO DAS NECESSIDADES E REQUISITOS

2.1. Identificação das necessidades de negócio

2.1.1. Conforme previsto no Art. 11, Inciso I da IN 01/2019 SGD/ME, o Estudo Técnico Preliminar da Contratação deve definir e especificar as necessidades de negócio e tecnológicas, e os requisitos necessários e suficientes à escolha da solução de TIC, contendo de forma detalhada, motivada e justificada, inclusive quanto à forma de cálculo, o quantitativo de bens e serviços necessários para a sua composição.

2.1.2. Principais necessidades de negócio:

1	Reestruturar e modernizar a arquitetura de rede do Ministério, provento a reestruturação da camada core da rede e consolidação da camada de agregação do Data Center
2	Garantir a continuidade dos negócios do MJSP por meio de melhorias, apoio técnico e manutenções da solução a ser adquirida
3	Prover a mitigação de impactos para as áreas de negócios decorrentes de problemas no funcionamento dos equipamentos de conectividade de rede
4	Aumentar a velocidade de conexão entre os servidores e ativos de rede do Data Center
5	Prover solução de gerenciamento e monitoramento eficiente dos ativos de rede do Data Center
6	Prover mecanismos de alta disponibilidade, mecanismos de segurança e balanceamento de carga entre Data Centers dos ambientes de infraestrutura do MJSP

2.2. Identificação das necessidades tecnológicas

2.2.1. A modernização e expansão da capacidade do ativos de rede deve possibilitar a implementação de ambientes com alta disponibilidade e que consigam proporcionar uma imagem fiel e em tempo real do panorama local e global dos eventos e dos recursos envolvidos nas diversas atividades do Ministério. Para isto, o ambiente atual deverá ser revisto de forma que permita à DTIC/MJSP, minimamente:

1	Prover substituição de ativos de rede, sem contrato de garantia e suporte, do núcleo central do MJSP e da sala cofre do CICCN
2	Manter a compatibilidade tecnológica do parque de ativos em funcionamento na rede do Ministério
3	Manter as soluções com suporte e garantia do fabricante com por no mínimo 60 meses
4	Adquirir solução de balanceamento de carga e mecanismos de inspeção SSL para os ambientes de infraestrutura do MJSP
5	Prover serviço de instalação, configuração e treinamento da solução a ser adquirida

2.3. Demais requisitos necessários e suficientes à escolha da solução de TIC

2.3.1. Importante destacar também que, de acordo com o exposto na Nota Técnica n.º 1/2019/CGISE/DTIC/SE/MJ (9159487), elaborada pela Coordenação-Geral de Infraestrutura e Serviços, e que teve como objetivo relacionar as necessidades de contratações para a área de Tecnologia da Informação e Comunicações visando a evolução e sustentação dos projetos estratégicos do Ministério da Justiça e Segurança Pública, que tratam de sistemas capazes de realizar o processamento e a análise de grandes volumes de dados, denominados "Projetos de Big Data", alguns pontos foram expostos, e que dizem respeito ao presente projeto como:

1	Principais desafios no processamento de grandes volumes de dados
2	Necessidade de segurança das informações
3	Necessidade de expansão da infraestrutura para os projetos de Big Data
4	Arquitetura tecnológica de rede de dados

3 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS E JUSTIFICATIVA DA CONTRATAÇÃO

3.1. A Diretoria de Tecnologia da Informação e Comunicação do Ministério da Justiça e Segurança Pública (DTIC/MJSP) passou por mudanças estruturais e regim ocasionando um crescimento nas demandas das áreas de negócio por soluções de tecnologia da informação e comunicação, tornando-se necessária a busca proporcionem uma infraestrutura tecnológica escalável e atualizada com o mercado.

3.2. A busca por evolução dos serviços de informática vem resultando em mudanças no perfil de tráfego de suas aplicações internas e externas, exigindo uma rev de rede atualmente em funcionamento, requerendo dos equipamentos ativos maiores taxas de transmissão e maior poder de processamento.

3.3. Tal implementação requer uma maior interatividade da parte de gerência entre os sistemas, procedimentos de configuração, desempenho, qualidade informação, bem como a total interoperabilidade, visando uniformização dos recursos como um todo.

3.4. Nesse sentido, a adoção de tecnologias modernas e inovadoras, como switches de alto desempenho e disponibilidade, equipamentos balanceadores de ca informação aplicada às camadas superiores, deixaram de ser uma tendência e passaram a ser uma realidade na Administração Pública Federal – APF, que dev modernas e eficientes práticas do mercado.

3.5. ATUAL ARQUITETURA E TOPOLOGIA DE REDE, BALANCEAMENTO E SEGURANÇA

3.5.1. Seguindo as boas práticas de mercado, a implementação do modelo de arquitetura de redes em camadas é amplamente difundida no mundo todo. Existem na adoção da arquitetura de rede em camadas, como por exemplo:

- Escalabilidade - facilmente expandidas;
- Redundância - aumentar drasticamente a disponibilidade por meio de implementações redundantes simples com redes hierárquicas;
- Desempenho - taxas de transmissão próximas ao máximo suportado em toda a rede;
- Segurança - segurança de porta do nível de acesso e políticas no nível de distribuição tornam a rede mais segura;
- Gerenciamento - relativamente simples em uma rede hierárquica;
- Sustentabilidade - permite a escala da rede sem que haja muitas complicações.

3.5.2. A atual plataforma de ativos de rede (Switches) do MJSP, formada pela rede do núcleo central, é composta por três camadas:

- Camada Central;
- Camada de Distribuição e
- Camada de Acesso.

3.5.3. A Camada Central abriga os switches do tipo core, que são equipamentos de alto desempenho, os quais devem ser robustos para suportarem grande trá arquitetura desta camada deve proporcionar alto grau de disponibilidade, capacidade, redundância e resiliência.

3.5.4. A Camada de Distribuição é responsável pela interconexão entre a camada Central e de Acesso, sendo responsável pela concentração dos pacotes de Camada de Acesso para encaminhamento à Camada Central. A Camada de Distribuição controla o fluxo do tráfego da rede usando políticas e determina dom realizando funções de roteamento entre VLANs, além de conectar os pontos de acesso da rede sem fio (APs).

3.5.5. A Camada de Acesso é a camada de switches mais próxima das máquinas dos usuários, sendo que os equipamentos ativos desta camada captam os pacotes das máquinas de usuários, impressoras, telefones VoIP e outros equipamentos da ponta, e os encaminham à Camada de Distribuição. O principal propósito da c fornecer um meio de conectar dispositivos à rede e controlar quais têm permissão de comunicação na rede.

3.5.6. Cabe destacar que a manutenção de todas as camadas apresentadas é fundamental para o perfeito funcionamento da rede do MJSP, tendo em vista que a incidente ou problema em um dos equipamentos da estrutura de rede em questão, impacta diretamente no trabalho dos usuários, tornando indisponível todo como internet, impressoras, acesso ao correio eletrônico, entre outros.

3.5.7. Salienta-se que no ano de 2016, através do processo (08006.001634/2016-15), foram adquiridos novos equipamentos de Acesso para substituição somer andares do Edifício Sede, onde encontram-se a Secretaria Executiva e Gabinete do Ministro. No mesmo processo, também foram adquiridos equipamentos para servidores de rede do Datacenter do INFOSEG, e substituição de switches nas então quatro Penitenciárias Federais.

3.5.8. Na época, uma das motivações para a troca desses equipamentos, era a ocorrência constante de incidentes em alguns switches de acesso, fato que gerou t de negócio, impossibilitando a comunicação de dados e telefonia e que levou a DTIC a adotar soluções paliativas de contorno como reinicialização dos equipamento

3.5.9. Além disso, naquele período, cerca de 80% dos equipamentos de acesso, e 100% dos equipamentos de distribuição, encontravam-se sem contrato de necessitando de atualização tecnológica, garantia e serviço de suporte do fabricante.

3.5.10. Salienta-se que, no ano de 2018, por meio do processo de aquisição (08006.001282/2018-51), foram adquiridos switches de distribuição e acesso contem cerca de 80% de todo o nosso parque desses ativos, tendo o final de suporte e garantia em março de 2024. A referida aquisição teve como principal objetivo supr switches que não foram adquiridos no ano de 2016.

3.5.11. Cabe ainda ressaltar, que no ano de 2014, por meio do processo 08006.001074/2014-29, foram adquiridos switches da Camada Central (Core) er equipamentos defasados naquele período, além de solução de controle de acesso à rede e dispositivos e solução de rede sem fio, todos instalados no Data Center andar, sala 201.

3.5.12 Os referidos equipamentos foram adquiridos em dezembro de 2014, com 48 meses de garantia e suporte, os quais tiveram sua expiração em dezembro de 2

3.5.13 Atualmente, os equipamentos da Camada Central já atingiram seu tempo de vida útil e estão desatualizados tecnologicamente, além de terem disponibilidade comprometidas pela falta de contrato de suporte, manutenção e garantia.

3.5.14 A atual estrutura de Data Centers do MJSP é formada pelos Data Centers do núcleo central e pelo Data Center do Centro Integrado de Comando e Controle N – CICCN-DF, que está sob responsabilidade tecnológica da DTIC/MJSP, após a extinção da Secretaria Extraordinária de Segurança para Grandes Eventos – SESGE, cu ocorreu no dia 31 de julho de 2017, conforme Figura 1:

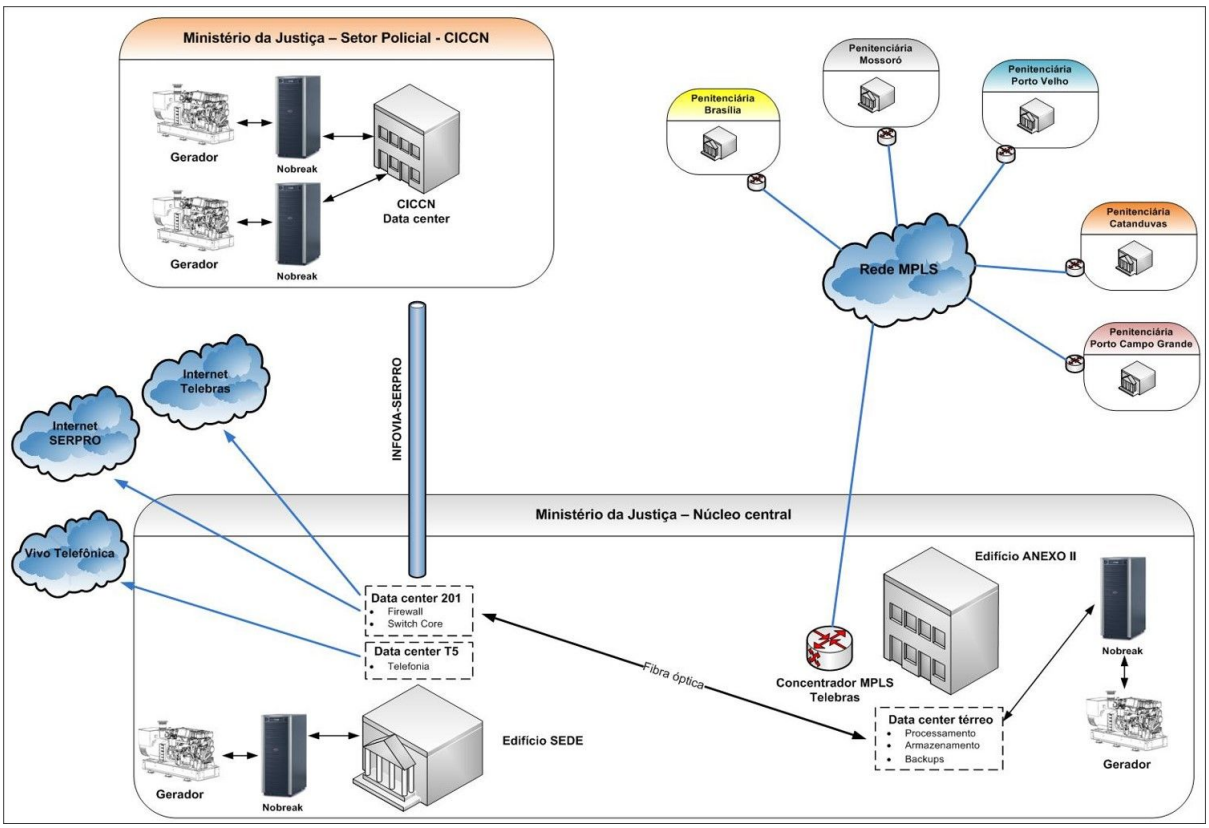

Figura 1 - Estrutura de Data Centers MJSP - Cenário atual

3.5.15 Conforme pode ser observado na Figura 1, atualmente o Ministério possui no núcleo central dois CPD's, e uma sala técnica que abriga a solução de telefo edifício Sede).

3.5.16. No primeiro CPD, mais antigo, localizado no segundo andar do Edifício Sede, sala 201, estão concentrados todos os equipamentos que formam o núcle como Switch Core, convergência de todas as fibras ópticas dos andares do Edifício Sede, Anexo I e Anexo II. Salienta-se que atualmente existe uma limitação de velo entre os andares e o núcleo da rede, tendo em vista que os cabos de fibra óptica são do padrão monomodo e ainda funcionam com transeivers antigos, também m

3.5.17. Os atuais switches Core da rede estão configurados para formarem dois VSS (*Virtual Switching System*): VSS-LAN e VSS-DC. No VSS-LAN são configuradas to rede que recebem as fibras dos andares, já no VSS-DC, são concentradas as fibras ópticas de interligação do outro Data center que fica localizado no térreo do A ilustra a topologia descrita:

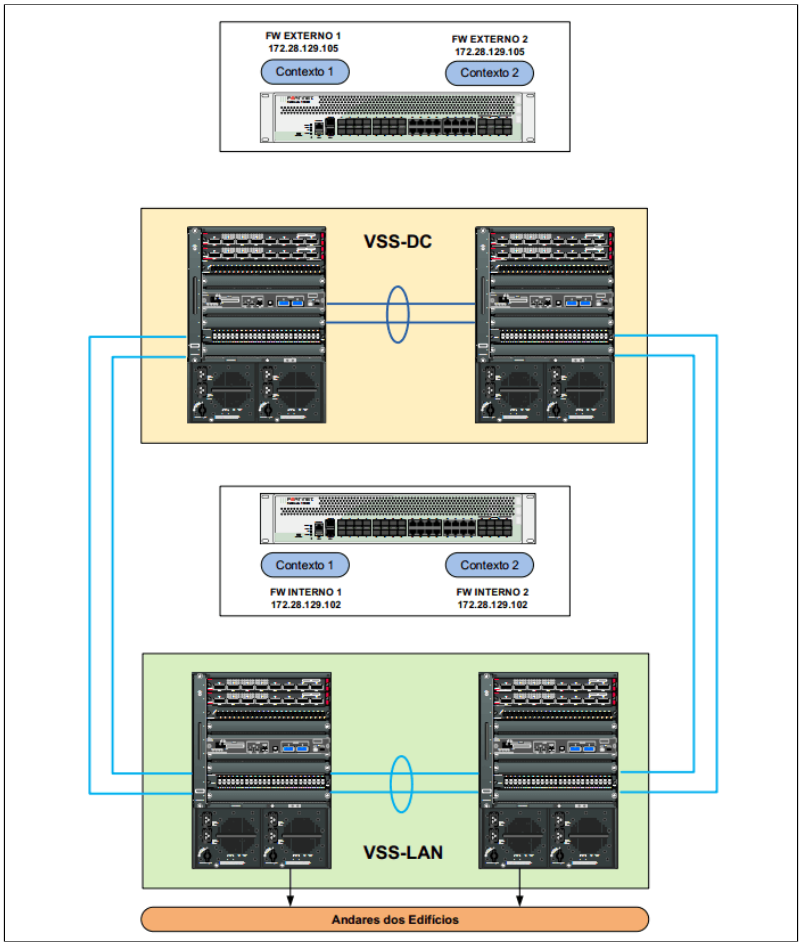

***Figura 2 - Topologia* VSS-LAN e VSS-DC**

3.5.18 Ligados ao switch Core da rede, estão os equipamentos de firewall da rede do MJSP, que fazem a segmentação e proteção externa e interna da r equipamentos estão cobertos por contrato de suporte e garantia do fabricante, e além das funções de firewall, executam também funções de IPS/IDS e filtro de cor

3.5.19. A rede sem fio do órgão também possui equipamentos instalados nesse Data Center, quais sejam duas controladoras e appliances ISE que fazem o autenticação da rede sem fio de visitantes, bem como o controle de acesso à rede e usuários.

3.5.20. Também estão concentrados no Data Center, os equipamentos de videoconferência do MJSP, que foram substituídos por equipamentos adquiridos pelo processo (08016.000044/2015-67).

3.5.21. Por último, tem-se a chegada da operadora SERPRO, que atualmente é responsável pela interligação das unidades do MJSP, via INFOVIA, e também pe Internet.

3.5.22. No segundo CPD, localizado no térreo do Anexo II, antiga sala do INFOSEG, concentra-se todo o ambiente de processamento e armazenamento da rede M de Virtualização, Sistema de CFTV, Controle de Acesso do órgão, Storages e Backup. Também estão instalados no referido Data Center, os concentradores MPl redundante da TELEBRAS, e solução de aceleradores de WAN, que otimizam o tráfego das cinco Penitenciárias Federais, as quais são suportadas pela DTIC/MJSP.

3.5.23. Destaca-se que para interconexão de todos os equipamentos listados no Data Center em questão, o MJSP dispõe de uma estrutura de *switches* de alto de de interligar a altas velocidades, os servidores do ambiente de processamento, os quais formam a base para todo o ambiente de virtualização, aos demais *switch* também ao *firewalls* da rede, que estão instalados fisicamente no Data Center do edifício Sede, sala 201. A Figura 3 ilustra a topologia de switches no Data Center e

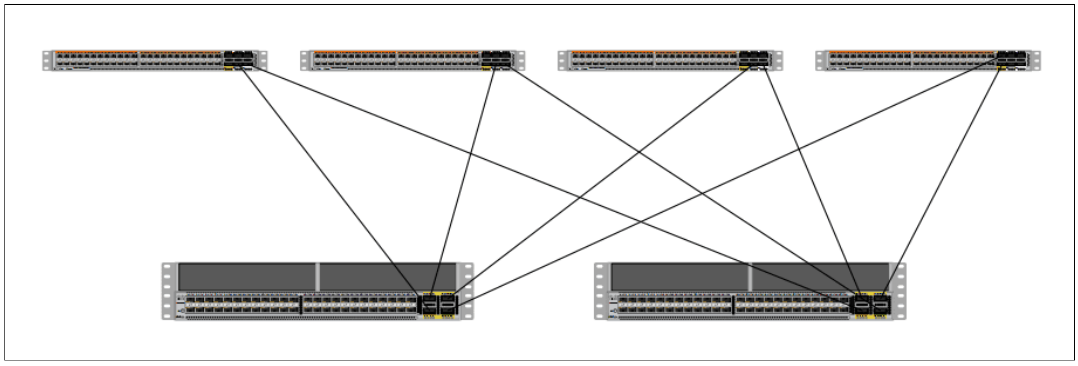

***Figura 3 - Topologia* Data Center INFOSEG**

3.5.24. Historicamente, este Data Center era utilizado pela rede INFOSEG, que possuía servidores, aplicações e banco de dados dedicados para aquela estrutur anos, a rede INFOSEG foi migrada para o SERPRO e o espaço foi ocupado pela então CGTI para instalação de equipamentos da rede do Ministério, tendo em vista do edifício sede estava com infiltrações que gerava risco para os equipamentos de processamento e armazenamento, que lá estavam instalados. Com isso, houve equipamentos de Data Center do órgão, que com o passar do tempo foi crescendo, não havendo espaço físico em nenhum dos locais para concentração e equipamentos de rede, segurança, processamento, armazenamento e backup. Foi a partir daí, que os equipamentos começaram a operar separadamente, ger diversos pontos de falhas. A Figura 4 ilustra a situação em questão:

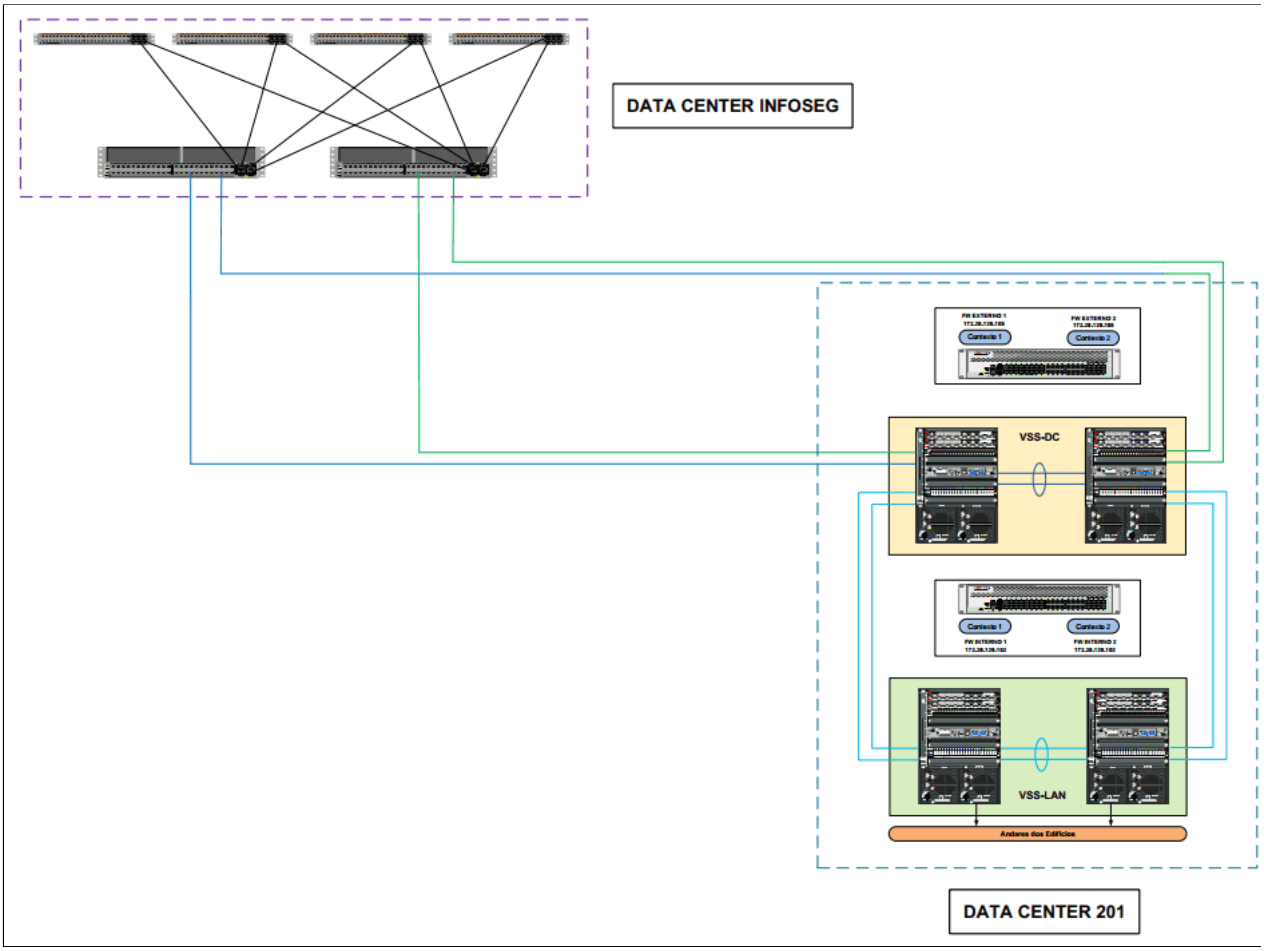

***Figura 4* - *Topologia* Data Centers 201 x INFOSEG**

3.5.25. O atual cenário não se deu a curto prazo, mas sim ao longo dos anos, onde mudanças naturais da conjuntura política, de gestão e de empresas administração dos ambientes, resultaram no atual panorama. Outro fator que levou a este cenário, foi a falta de recursos financeiros e priorização para realiza infraestrutura com o objetivo de proporcionar a concentração dos ativos do órgão em um único local físico com a segurança e a proteção adequada.

3.5.26. Importante esclarecer que o fato de os equipamentos de *firewalls* estarem instalados em outro Data Center gera um *delay* na comunicação entre as aplicaç de banco de dados.

3.5.27. Salienta-se que o fato de a infraestrutura de Data Center do MJSP ser composta por locais separados fisicamente para acomodação de seus equipa fragilidade nos sistemas, pois os locais funcionam de forma complementar e gerando uma dependência mútua, sendo que um suporta as soluções de rede e seg parte de processamento, armazenamento e backup. Para a interconexão entre as duas partes, são necessários links de fibra óptica de forma a manter a maior ta possível entre os dois locais.

3.5.28. Cabe destacar que atualmente o Ministério possui appliances ISE, que fazem o gerenciamento da autenticação da rede sem fio de visitantes, bem como o c rede e usuários. Essa ferramenta foi adquirida no ano de 2014, por meio do contrato 74/2014, que já encontra-se expirado. Na época, como não havia lice equipamentos da rede de acesso, o escopo da contratação consistiu na utilização a solução para o controle de acesso da rede sem fio visitante.

3.5.29. É oportuno mencionar que foram adquiridos novos equipamentos de Acesso para substituição para o 3º e 4º andares do Edifício Sede, os quais pos permitem a implementação de controle de acesso, assim como, no ano de 2018, por meio do processo de aquisição (08006.001282/2018-51), foram adqu distribuição e acesso contemplando a troca em cerca de 80% de todo o parque desses ativos, os quais também contemplam licenças para utilização nesse atualmente todos os switches da rede possuem licenciamento para funcionamento com solução de controle de acesso.

3.5.30. Para modernizar o controle de acesso da rede de computadores do Órgão é necessário que o funcionamento da referida solução seja revisto de forma qu todos os switches, provendo o controle de acesso de todas as portas do equipamentos da rede acesso, bem como seja reativado o suporte e garantia do fabricante

3.5.31. Além da estrutura de Data Centers do núcleo central do Ministério, a DTIC é responsável pela gestão do Data Center do Centro Integrado de Comando e Co Brasília – CICCN-DF (sala cofre), que também possui ativos de rede, responsáveis pela interconexão dos equipamentos internos o Data Center e também inter técnica da pétala H do complexo do Departamento de Polícia Rodoviária Federal.

3.5.32. Atualmente a estrutura de switches do Data Center do CICCN-DF é composta por 2 (dois) switches Extreme Networks, modelo Black Diammond 8810 (RA para atender às camadas de distribuição e as de acesso do edifício e 2 (dois) switches Extreme Networks Summit X440-24t para realizarem conexão com os servi sala cofre. Os equipamentos foram adquiridos em 2013, Contrato 18/2013, 08131.000437/2013.92, e estão sem contrato de garantia e suporte. A Figura 5 ilus questão:

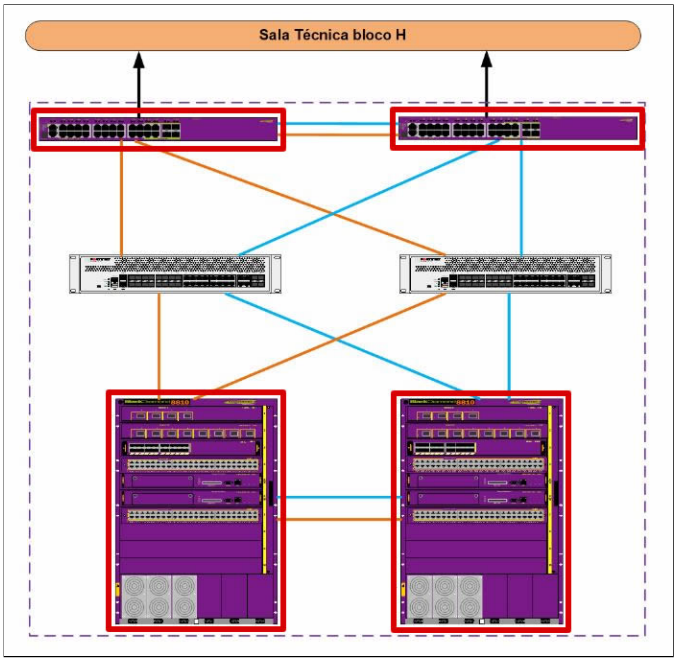

Figura 5 - Topologia Sala Cofre (Core)

3.5.33. Com o objetivo de prover a alta disponibilidade entre os dois Data centers (MJSP e CICCN-DF), a DTIC, no ano de 2018, iniciou projetos para este fim, modernização das ferramentas de virtualização, por meio do contrato 30/2018 (7794421) com novas ferramentas de virtualização, como *Vmware vSphere E Operations Management (vSOM), Software de Gerenciamento Vcenter Server Standard e Software NSX - ENTERPRISE PLUS*, as quais estão em fase final irão modernizar o ambiente de virtualização e implementar alta disponibilidade com o Data Center do CICCN-DF, também de responsabilidade desta DTIC.

3.5.34. Cabe destacar ainda que, além das ferramentas possibilitarem alta disponibilidade entre os Data centers, ainda será possível a implantação do recursos de r para máquinas virtuais e containers, assim como monitoramento e detecção de problemas para aplicativos tradicionais e nativos em nuvem. Com o NSX, as funç switch, roteamento e firewall, são incorporadas ao hypervisor e distribuídas em todo o ambiente. Isso possibilita a implantação de um "hypervisor de rede" que f plataforma para sistemas de redes virtuais e serviços de segurança. De maneira semelhante ao modelo operacional de máquinas virtuais, as redes virtuais s programaticamente e gerenciadas sem depender do hardware subjacente. A Figura 6 ilustra a topologia que está sendo implantada para prover alta disponib Centers do MJSP:

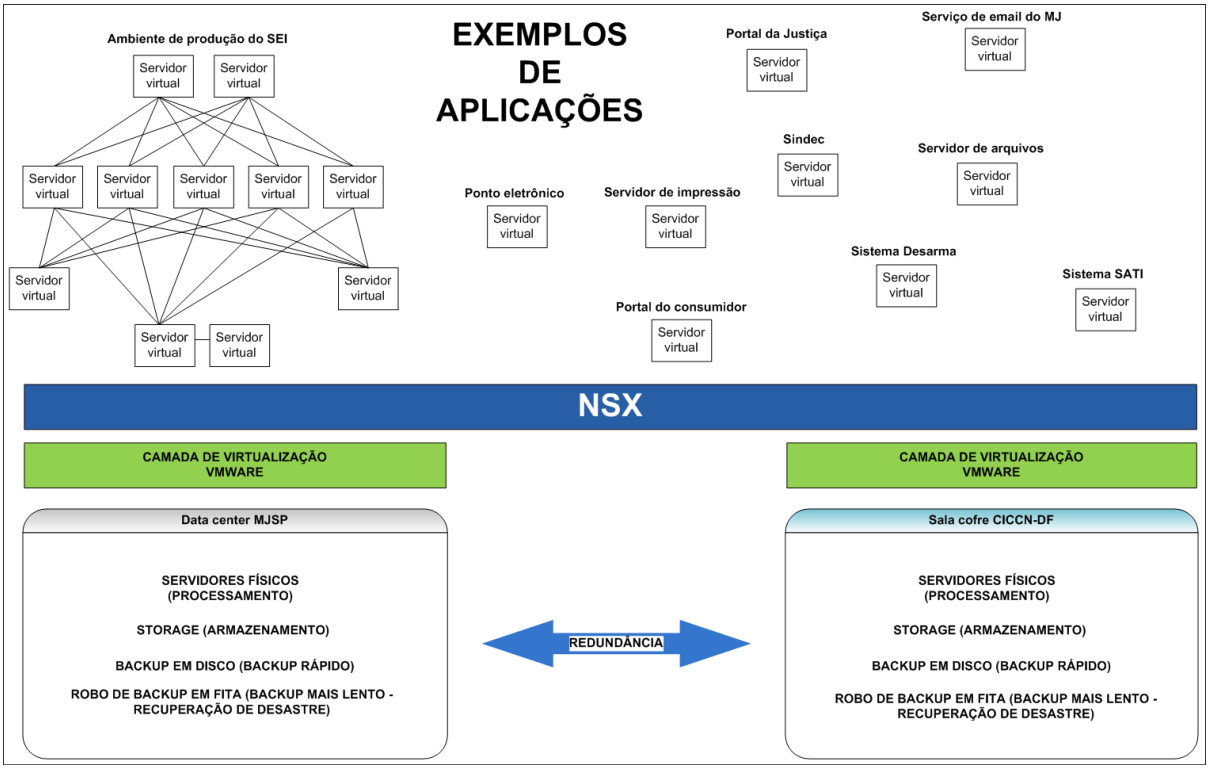

Figura 6 - Topologia Sala Cofre CICCN x Data Center MJSP

3.5.35. Importante destacar que para que dois Data Centers funcionem em alta disponibilidade de forma plena, várias ações precisam ser consideradas em todos camada física até a camada de aplicações. Nesse sentido, é necessário uma solução que tenha a capacidade de balancear carga entre servidores (Server Load utilizando para isso funções de *Global Server Load Balancing* (GSLB), que proporciona a hospedagem de serviços em mais de um data center, permitindo alta dispo de balanceamento de links.

3.5.36. Esses balanceadores são importantes para momentos de pico de tráfego de acesso. Algoritmos inteligentes dedicam-se à distribuição de tarefas entre disponíveis para que usuário não se depare com situações inconvenientes em seu acesso à internet e aplicações no MJSP.

3.5.37. O balanceamento na utilização da rede passa, sobretudo, por reencaminhar o tráfego por caminhos alternativos a fim de descongestionar os acessos aos s 7 ilustra uma topologia (exemplo) utilizando redundância em balanceamento de carga:

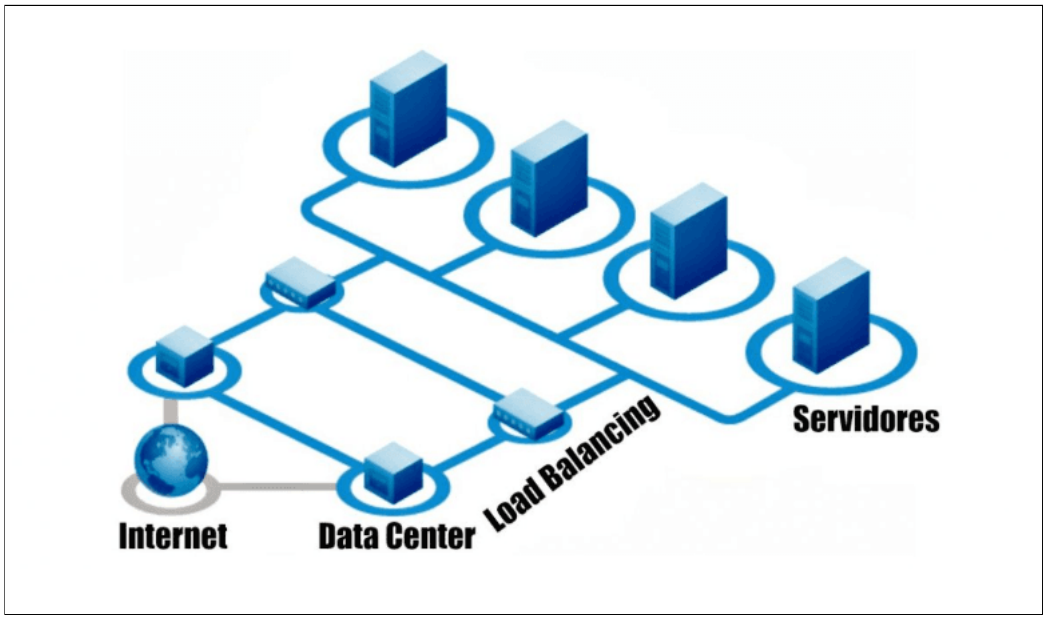

Figura 7 **- Exemplo de Topologia Balanceamento de Carga**

3.5.38. Sendo assim, também neste projeto, torna-se imprescindível a análise de solução com dispositivos que são responsáveis pelo balanceamento e que de *Global Server Load Balancing* (GSLB) e sincronização dos dados de forma automática.

3.5.39. Outro fator importante, que merece ser tratado como requisito essencial em um projeto comunicação entre os dois Data centers, é a capacidade rea conexões criptografadas, ou seja, uma visibilidade e inspeção de SSL. Além disso, há também necessidade de prover segurança nas camadas superiores (aplicação).

3.5.40. Soluções voltadas à segurança em redes de computadores são amplamente difundidas e necessárias em um ambiente com constantes atualizações e prope volatilidade, que são constantes e recorrentes em qualquer ambiente de TI.

3.5.41. Nessa linha, a criptografia é uma forma de garantir a confidencialidade das informações, protegendo a privacidade e a integridade de dados. Segundo o Ga do tráfego atual já utiliza criptografia para garantir maior segurança das informações (https://www.gartner.com/en/documents/3869861/encrypted-web-traffic0). utilização também cria um ponto cego que os invasores conseguem explorar para escapar dos controles de segurança, conforme mostra a Figura 8.

3.5.42. A partir de resultados recentes de testes do NSS Labs, concluiu-se que os dispositivos tradicionais de rede e segurança, ao inspecionar o tráfego cript desempenho afetado gravemente. Em média, o impacto no desempenho da inspeção profunda de pacotes é de 60%, com a média de queda nas taxas de conexão no tempo de resposta de 672% (https://www.nsslabs.com/press/2018/7/24/nss-labs-expands-2018-ngfw-group-test-with-ssl-tls-security-and-performance-test que representa uma taxa impressionante.

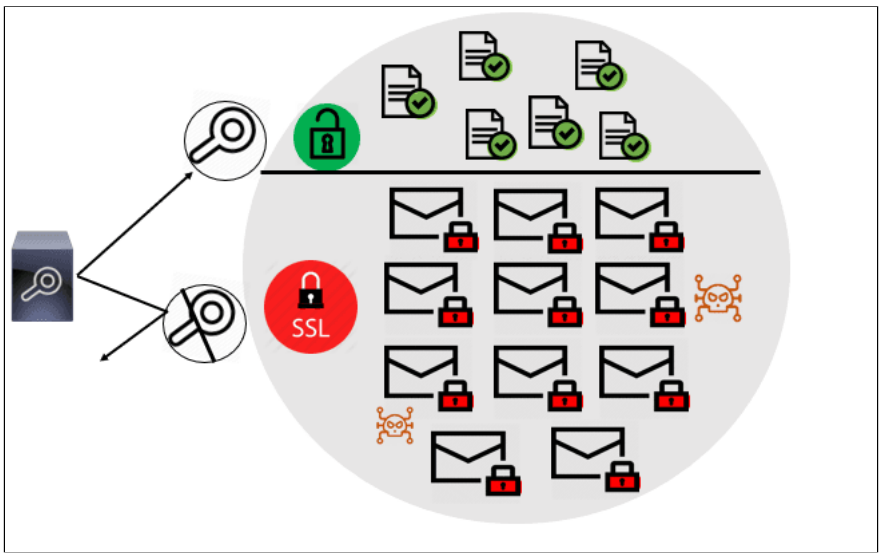

Figura 8 **- Visibilidade de tráfego criptografado**

3.5.43. A grande diferença entre a funcionalidade de SSL Offload e Orquestração SSL é que enquanto a funcionalidade de SSL Offload se concentra em rec tratamento SSL nos servidores, tem-se na orquestração um recurso que se destina a abrir, de forma centralizada e seletiva, as conexões criptografadas, com o ir exigência de processamento dos dispositivos clássicos de Segurança (Firewall, Sistemas IPS, WAF, web proxy, DLP, dentre outros).

3.5.44. Com tal abordagem, os elementos especializados em Segurança podem direcionar seus recursos computacionais para as tarefas de inspeção de tráfego otimizados. Além de proteger o investimento nas soluções existentes no que concerne a desempenho, tal mecanismo contribui para ampliar a segurança da r sentido de eliminar os “pontos cegos” que decorrem do significativo volume de canais SSL criptografados.

3.5.45. Cabe citar que o Ministério sempre buscou por soluções que atendam aos requisitos e melhores práticas disseminadas nesse mercado voltado à seguran ações e adquirindo equipamentos robustos e capazes de mitigar ações mal intencionadas.

3.5.46. Alguns equipamentos foram adquiridos em dezembro de 2017 por meio do processo 08006.001190/2016-18 (Contratação de empresa especializada para serviços de aquisição de Solução de Segurança de Perímetro, incluindo suporte técnico, manutenção e garantia de funcionamento, para o atendimento da Ministério da Justiça e Segurança Pública).

3.5.47. Essa solução (Firewall) é importante e essencial para proteção de ataques cibernéticos, sendo um dispositivo de segurança de rede que monitora o tráfego quanto de saída. Além disso, age de acordo com o conjunto de regras estabelecidas, ou seja, decide o que pode entrar e qual tráfego específico será bloquea objetivo é proteger a integridade dos dados, bem como a confidencialidade deles.

3.5.48. As funções de Inspeção SSL podem ser habilitadas nos firewalls atuais (Fortigate). Contudo, não são *hardwares* dedicados somente a essa atividade, pois Filtragem de pacotes, Web Filter, IDS e IPS e QOS. Além disso, os Firewalls do Ministério trabalham em cluster em modo ativo-passivo, o que quer dizer que em deles está responsável pelo tráfego do ambiente. A Figura 9 traz a visibilidade do throughput dos equipamentos de Firewalls em seus momentos de pico dos últimos

Device Name	Role	CPU Usage	▼Memory Usage	Disk Usage	Logs Per Second	Concurrent Sessions
MJ-HA-FG1K5D3I17802243		46%	82%	20%	21128.42	472,206
MJ-HA-FG1K5D3I17802261		29%	63%	20%	94236.79	438,810

***Figura 9* - Visibilidade do throughput dos equipamentos de Firewall**

3.5.49. Observa-se que, em certo momento, o device FG1K5D3I17802261 ultrapassou 12 GBPs de throughput e a memória do FG1K5D3I17802243 ultrapassou limite de 80% de consumo de memória o equipamento começa a desabilitar funções até que o consumo abaixe novamente a um nível seguro).

3.5.50. Ao avaliar as especificações técnicas dos firewalls (Fortigate), atualmente instalados no ambiente, observa-se que o limite máximo dos equipamentos q função *SSL-Inspection* atinge capacidade máxima de 5.7 Gbps, conforme Figura 10:

	FG-1500D	FG-1500DT
Hardware Specifications		
Hardware Accelerated 10 GE SFP+ / GE SFP Slots	8	4
Hardware Accelerated GE SFP Slots	16	
Hardware Accelerated 10 GE RJ45 Ports	–	4
Hardware Accelerated GE RJ45 Ports	16	
GE RJ45 Management / HA Ports	2	
USB Ports (Client / Server)	1 / 1	
Console Port	1	
Onboard Storage	2x 240 GB SSD	
Included Transceivers	2x SFP+ (SR 10GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	13 Gbps	
NGFW Throughput [2, 4]	7 Gbps	
Threat Protection Throughput [2, 5]	5 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 55 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	80 / 80 / 55 Gbps	
Firewall Latency (64 byte, UDP)	3 µs	
Firewall Throughput (Packet per Second)	82.5 Mpps	
Concurrent Sessions (TCP)	12 Million	
New Sessions/Second (TCP)	300,000	
Firewall Policies	100,000	
IPsec VPN Throughput (512 byte) [1]	50 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	20,000	
Client-to-Gateway IPsec VPN Tunnels	100,000	
SSL-VPN Throughput	4 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	5.7 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	3,100	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	800,000	

***Figura 10* - *Especificações* dos equipamentos de Firewall**

3.5.51. Sendo assim, caso a função de Inspeção SSL seja utilizada junto ao firewall existente, além de não ter capacidade de throughput necessária para o atual m risco de afetar os demais serviços existentes. Por fim, torna-se fundamental uma análise dos cenários e soluções viáveis para esta necessidade.

3.5.52. Já quando se trata de proteção nas camadas superiores (camada aplicação), apesar de serem equipamentos modernos e seguros, eles não são dedica efetiva na camada de aplicação, que necessita de uma proteção de seus aplicativos com análises comportamentais, defesa proativa contra bots e criptogra aplicativos de dados confidenciais.

3.5.53. Essa proteção pode ser aperfeiçoada com um Web Application Firewall (Firewall de Aplicação Web - WAF), que monitora, filtra e bloqueia pacotes de da viajam de e para um aplicativo da Web. Ele pode ser baseado em rede, host ou em nuvem e é frequentemente implantado através de um proxy. A Figura 11 ilu genérica utilizando solução WAF:

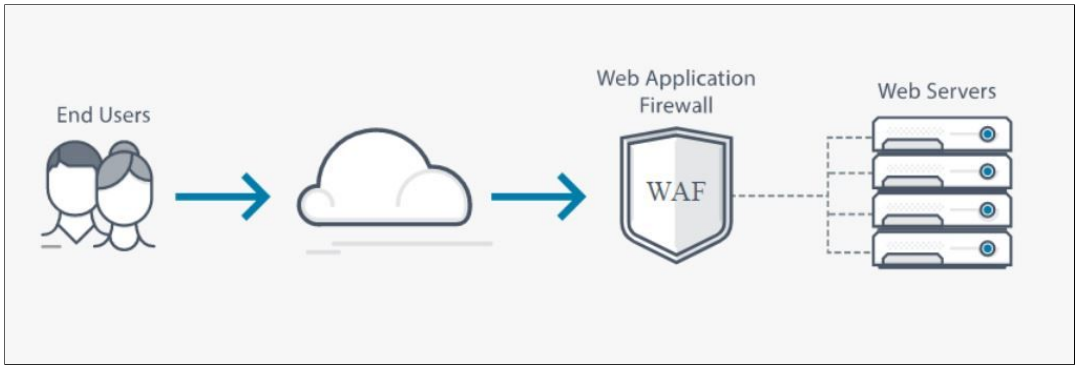

***Figura 11* - Exemplo de Topologia Utilizando Solução WAF**

3.5.54. Sendo assim, um Web Application Firewall (Firewall de Aplicação Web - WAF) fornece segurança na Web para serviços on-line contra ataques de segurança como injeção SQL, XSS (cross-site scripting). Os WAFs detectam e filtram ameaças que podem degradar, comprometer ou expor aplicativos online a ataques de (DoS). WAFs examinam o tráfego HTTP antes que ele atinja o servidor de aplicativos. Eles também protegem contra a transferência não autorizada de dados do serv

3.5.55. Diante o exposto sobre segurança em aplicações, torna-se fundamental a inserção, neste projeto, de uma solução de Web Application Firewall (Firewall d WAF) sendo dedicado para proteção efetiva da camada de aplicação.

3.5.56. É oportuno também destacar o cenário atual do balanceamento de carga entre aplicações. O Ministério possui mais de 200 aplicações sustentadas em pro sustentadas por meio de clusters de máquinas virtuais divididos por tecnologias, tanto para servidores de aplicação, como para bancos de dados. As tecnologia aplicação atualmente sustentadas pela DTIC/MJSP estão concentradas basicamente em: Jboss, Wildfly, Tomcat, PHP, IIS e Zope Plone, e para Sistemas Gerencia Dados são divididas em: Microsoft SQL Server, MySQL, PostgreSQL e Oracle.

3.5.57. Seguindo as melhores práticas de mercado, a DTIC/MJSP vem desenvolvendo, ao longo dos últimos anos, um trabalho de padronização e automatização de desenvolvimento, testes, homologação, produção e treinamento. Como padrão, para cada aplicação em produção, e sempre que necessário, a aplicação é rep demais trilhas, de forma que se tenha um processo de integração contínua no desenvolvimento e sustentação das aplicações. Destaca-se que a DTIC/MJSP ambiente de infraestrutura, bem como iniciando o desenvolvimento de novas aplicações, no conceito de containers, fato que exigirá ambientes ainda mais confiáve

3.6. IMPLANTAÇÃO DE SOLUÇÃO TECNOLÓGICA DE BIG DATA ANALYTICS

3.6.1. Salienta-se que o MJSP está em fase modernização e implantação de diversas ferramentas e soluções, para atendimento dos projetos estratégicos d ambiente *on-premisse*, com em nuvem. A presente contratação apresenta grande transversalidade em relação a todos os projetos em andamento na medi conectividade para todos os equipamentos, além de ter que suportar o desempenho e escalabilidade de todo o hardware do Data Center.

3.6.2. Uma das soluções que está sendo prospectada pela DTIC, é um ambiente de Big Data. O referido projeto consiste na implantação de solução tecnológica de B de plataforma para captura, curadoria, descoberta, análise, mineração e integração de grande volume de dados, de forma auxiliar o Ministério e suas Secretari execução das políticas públicas, no processo de tomada de decisão em nível estratégico, tático e operacional.

3.6.3. Nessa linha, a Nota Técnica n.º 1/2019/CGISE/DTIC/SE/MJ (9159487), elaborada pela Coordenação-Geral de Infraestrutura e Serviços, e que teve como ob necessidades de contratações para a área de Tecnologia da Informação e Comunicações visando a evolução e sustentação dos projetos estratégicos do Mini Segurança Pública, que tratam de sistemas capazes de realizar o processamento e a análise de grandes volumes de dados, denominados "Projetos de Big Data", essenciais à execução do projeto, como:

- Principais desafios no processamento de grandes volumes de dados;
- Necessidade de segurança das informações;
- Necessidades tecnológicas e independência de fornecedor;
- Necessidade de expansão da infraestrutura para os projetos de Big Data;
- Arquitetura tecnológica de armazenamento e processamento de dados;
- Arquitetura tecnológica de rede de dados;
- Estrutura física do Data Center do Ministério da Justiça e Segurança Pública.

3.6.4. Essa Nota Técnica também reforça, em seu item 4.2, a necessidade de uma arquitetura tecnológica de rede de dados capaz de prover sustentação ao p Analytics:

> ...
>
> *A implantação da nova infraestrutura de equipamentos dedicados ao projeto Big Data implicará também na necessidade de expansão da infraestrutu disponível nos datacenters do MJSP. A intensidade de tráfego que é característica de aplicações que realizam processamento e armazenamento distribuída demanda que sejam providos equipamentos de rede de garantir a conectividade e a largura de banda entre todos os nós componente baixíssima latência e inexistência de oversubscription (ou seja, a capacidade de cursar tráfego dos switches de rede deve ser igual ou superior a transferência de todas as suas interfaces somadas).*
>
> ...

3.6.5. Cabe destacar que, em 17/12/2019, não sendo possível continuar com o projeto descrito e planejado no processo 08006.000621/2019-63, foi ins SEI 08006.001367/2019-11 com a finalidade de materializar o novo planejamento de contratação considerando a demanda existente, confor 709/2019/CGISE/DTIC/SE/MJ (10421490):

> ...
>
> *Restando mantida a necessidade detalhada no Documento de Oficialização da Demanda 8740327 e não tendo sido possível atendê-la por meio da con processo atual, deverá ser iniciado novo processo de contratação com a mesma finalidade, havendo, no entanto, espaço para amadurecimento e redefir de acordo com eventual alteração do cenário.*
>
> *Foi instituído o processo SEI 08006.001367/2019-11 com a finalidade de materializar o novo planejamento de contratação considerando a demanda exist*
>
> ...

3.6.6. Diante disso, e tendo como perspectiva a continuidade da contratação de solução de Big Data Analytics, a prevenção de eventuais falhas no ambiente prospecção de um ambiente seguro com suporte e garantia dos ativos de redes, a garantia dos requisitos de expansibilidade, assim como a reestruturação necessá projeto de Big Data Analytics e as futuras demandas e projetos, se faz necessária a aquisição de equipamentos ativos de rede para a Camada Central do MJSP, que c de redundância e contingência constituídos por uma série de ações e procedimentos que visam soluções e dispositivos de recuperação relacionados com essas falh

3.7. Alinhamento aos objetivos estratégicos

3.7.1. Como pode ser observado, após a explanação das topologias de rede do Data Centers do MJSP, formada pelos Data Centers do núcleo central e pelo Data Integrado de Comando e Controle Nacional de Brasília – CICCN-DF, além do exposto quanto à necessidade de equipamentos de segurança da informação voltados que a estrutura de rede do MJSP é complexa e demanda ações de atualização tecnológica para o correto dimensionamento técnico e atendimento dos obje Importante salientar o mapa estratégico 2015-2019, que possui os seguintes objetivos estratégicos:

a) reduzir homicídios e outros crimes violentos;

b) fortalecer o enfrentamento à criminalidade, com enfoque em organizações criminosas, corrupção, lavagem de dinheiro e atuação na faixa de fr

c) promover o acesso à justiça e proteger os direitos do cidadão;

d) aperfeiçoar a coordenação estratégica e a integração dos órgãos de segurança pública;

e) aperfeiçoar a gestão do sistema prisional;

f) promover a gestão e a alienação do produto de crimes de tráfico de drogas;

g) ampliar a escala e a efetividade das ações de defesa da concorrência e do consumidor;

h) aprimorar mecanismos de gestão e de disseminação do conhecimento com foco no público externo;

i) promover a valorização e o desenvolvimento dos servidores;

j) aprimorar e integrar a gestão e a governança institucional;

k) fortalecer a ampliar a estrutura e os serviços de TIC.

3.7.2. Cabe destacar que para a viabilização dos objetivos estratégicos, vários projetos estão sendo propostos pelas áreas de negócio do Ministério. Os projetos pro processo 08000.011558/2019-41, e devem ser considerados no planejamento de aquisições de Tecnologia da Informação. Como exemplo, pode-se destacar o pro analítica aplicada no combate à corrupção, à lavagem de dinheiro e em ações de segurança pública.

3.8. Compatibilidade Tecnológica e Conclusão

3.8.1. É uma premissa fundamental para a supracitada contratação que a aquisição dos equipamentos possua total compatibilidade tecnológica com os equipamer meio dos Processos Administrativos nº (08006.001074/2014-29), nº (08006.001634/2016-15) e nº (08006.001282/2018-51).

3.8.2. Um ponto importante a ser observado é a compatibilidade entre alguns equipamentos atuais, como os switches Cisco Nexus 56128P e Fabric Extenders Cisco com a solução a ser adquirida nesta contratação. Essa é uma medida essencial e requisito fundamental ao funcionamento do parque de ativos do MJSP, equipamentos da solução como switches, transceiver, e cordões ópticos devem ser totalmente compatíveis com os ativos atuais, não possuindo qualquer tipo de ligações.

3.8.3. Destaca-se que o cenário de compatibilidade tecnológica se faz necessário devido às contratações já realizadas, e, por representar uma infraestrutura considerável, tanto em quantidade de equipamentos quanto em valores de aquisição.

3.8.4. A compatibilidade tecnológica de equipamentos em uma mesma infraestrutura apresenta diversos benefícios, tanto de caráter técnico quanto de caráter ec quais destacamos as seguintes:

a) Todos os equipamentos ativos de rede são configurados e administrados sob um único Sistema Operacional (SO), o que significa que a mesma sinta utilizada em todos os equipamentos, sendo isso um fator importante, também, nos custos para treinamentos dos colaboradores, pois um único SO tem capacitação do que se forem implementados vários SOs na rede;

b) A interoperabilidade entre todos os equipamentos, mesmo que de gerações diferentes, é garantida, não apenas no que tange a protocolos padroniza mas também no que tange a protocolos proprietários, que tipicamente existem dentro do escopo da linha de equipamentos de cada fabricante;

c) A documentação relativa aos procedimentos adotados pelo MJSP para configuração e instalação dos equipamentos é única, não sendo necessárias para equipamentos que realizem a mesma função, mas que sejam de diferentes fabricantes;

d) Viabilização da unificação de contratos de manutenção para os equipamentos de rede cuja garantia já foi expirada.

e) Facilidade no procedimento de backup e restauração de configurações dos equipamentos.

3.8.5. Por fim, cabe ressaltar que uma indisponibilidade da Camada Central, além da não implementação e reestruturação da Camada de Agregação na infraes MJSP, pode gerar alto impacto nas atividades das áreas de negócio do Ministério, comprometendo, inclusive, o cumprimento de sua missão e o atingimento dos ob do MJSP.

3.8.6. Portanto, são necessárias ações para substituição, expansão e atualização de equipamentos com o objetivo de mitigar os riscos e evitar impactos na rotina d do MJSP, que se traduzem nas necessidades abaixo listadas:

a) Manter parque de ativos de switches com suporte, manutenção e garantia;

b) Prover a infra-estrutura necessária para suportar, de forma otimizada e flexível, as demandas de informações e serviços das áreas finalísticas;

c) Implantar um método de gestão e comunicação de toda a infra-estrutura de Tecnologia da Informação de forma a agilizar a sua operação;

d) Suportar a demanda futura por largura de banda de rede requeridas por novas tecnologias;

e) Implementar mecanismos de alta disponibilidade de comunicação de dados com otimização de banda entre os equipamentos do Data Center;

f) Garantir soluções voltadas à segurança em redes de computadores;

3.8.7. Diante dos motivos expostos e das necessidades apresentadas, se faz necessário a aquisição de equipamentos de rede de dados para a modernizaç capacidade, incluindo novos ativos de núcleo e de camada de agregação, além de soluções de segurança da informação voltados à rede, contemplando os serv suporte técnico e garantia.

4 – ANÁLISE DE SOLUÇÕES DE ATIVOS DE REDES

4.1. Solução 1 - Ativos de Redes: Contratação de serviço de garantia e suporte técnico para os ativos existentes

4.1.1. O presente cenário tem o objetivo de analisar a possibilidade da contratação dos serviços de manutenção e suporte para os equipamentos existentes verificando sua viabilidade.

4.1.2 Atualmente, no Data Center do edifício Sede sala 201, está concentrada a convergência de todos os enlaces de fibra óptica que fazem a interligação dos andares do edifício Sede, Anexo II e Anexo I com o núcleo da rede. Salienta-se que atualmente existe uma limitação de velocidade na conexão entre os andares e o núcleo da rede, tendo em vista que os cabos de fibra óptica são do padrão monomodo e ainda funcionam com *transeivers* antigos, também monomodo.

4.1.3 No mesmo Data Center estão concentrados os switches Core da rede, que formam dois VSS (*Virtual Switching System*): VSS-LAN e VSS-DC. No VSS-LAN são configuradas todas as interfaces de rede que recebem as fibras dos andares, já no VSS-DC, são concentradas as fibras ópticas de interligação do outro Data center do INFOSEG, que fica localizado no térreo do Anexo II. Importante ressaltar que os quatro equipamentos que formam os dois VSS's, estão sem contrato de manutenção, suporte e garantia do fabricante, além de estarem defasados tecnologicamente com o mercado, sendo esses o modelo Cisco 6500 adquiridos em 08 de dezembro de 2014, tendo seu suporte e garantia finalizados em 08 de dezembro de 2018. A Figura 13 ilustra a situação em questão:

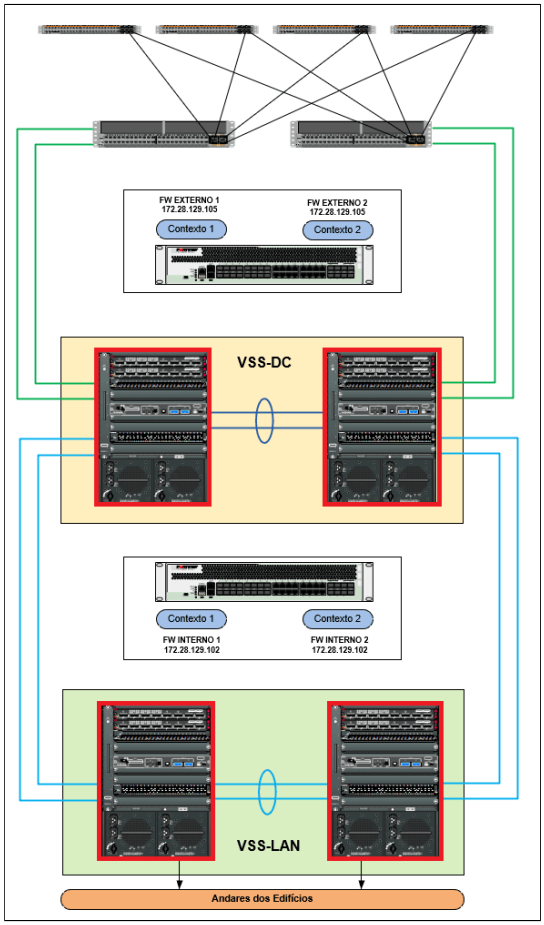

Figura 13 - Topologia Core Edifício Sede

4.1.4. Nessa topologia, encontram-se 4 (quatro) switches core:

- 02 (dois) switches core 6500 (VSS-LAN) são configuradas todas as interfaces de rede que recebem as fibras dos andares e interligados para atender às camadas de distribuição e as de acesso, além de realizarem conexão junto ao *Firewall.*
- 02 (dois) switches core 6500 (VSS-DC) são concentradas as fibras ópticas de interligação do outro Data center que fica localizado no térreo do Anexo II, que abriga 02 (dois) switches Cisco Nexus 56128P, 48 portas, sendo esses ligados aos Extensores de fabric Cisco Nexus 2348 com 48 portas, para conexões que utilizam UTP.

4.1.5. Importante salientar que os 02 (dois) switches Cisco Nexus 56128P de 48 portas, bem como os 04 (quatro) Extensores de fabric Cisco Nexus 2348 com 48 portas, para conexões que utilizam UTP, estão cobertos por contrato de suporte e garantia até 16/02/2022, por meio do contrato 19/2016 (3422816).

4.1.6. No caso dos 04 (quatro) switches core modelo 6500, o fabricante dos equipamentos definiu datas específicas para descontinuidade dos produtos expostos (*end of life*), que se deu em 31/01/2018, conforme pode ser observado no site do fabricante do equipamento: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/eol_c51-697975.html.

4.1.7. A topologia core do CICCN é formada por 02 (dois) switches Extreme Networks, modelo Black Diammond 8810 (RACK 02) e por 02 (dois) switches Extreme Networks Summit X440-24t, interligados para atender às camadas de distribuição e as de acesso do edifício (bloco H), além de realizarem conexão com os servidores e *firewalls* da sala cofre. A Figura 14 demonstra esses ativos:

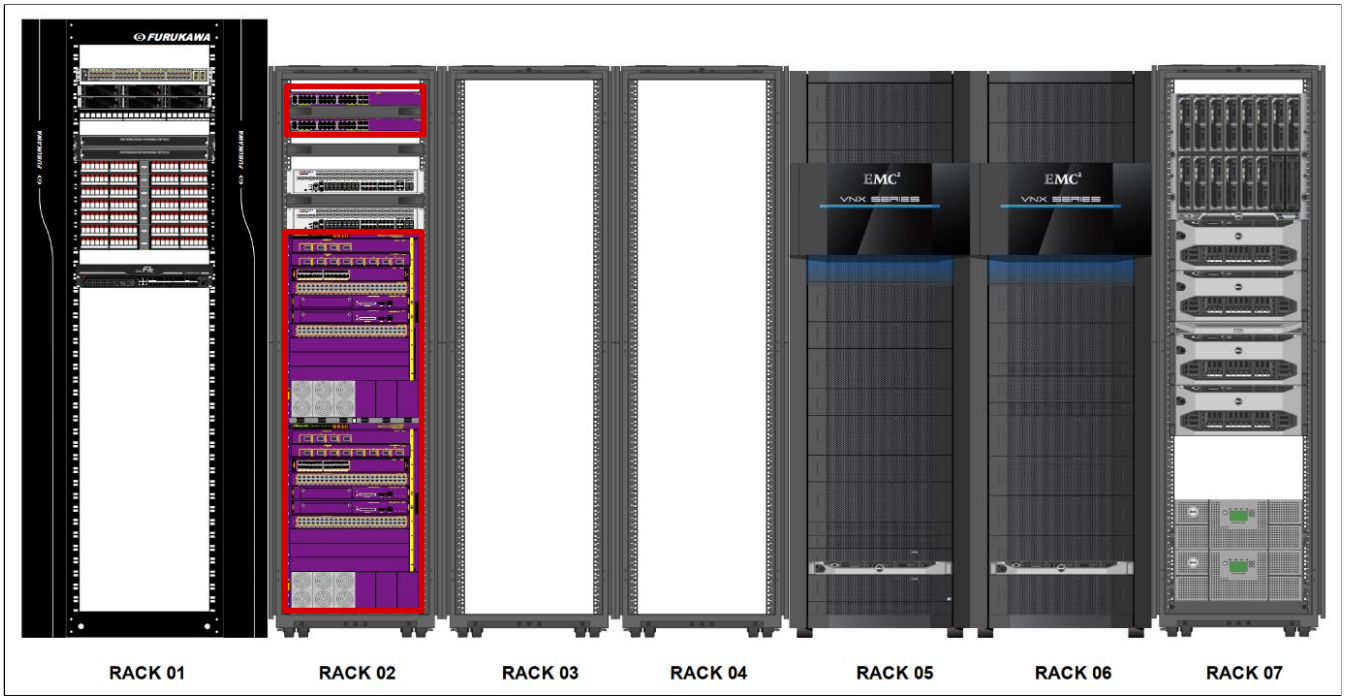

Figura 14 - Sala Cofre - CICCN

4.1.8. Tais equipamentos atingiram seu tempo de vida útil estando desatualizados tecnologicamente. Logo, há um comprometimento na contratação de garantia e suporte, além de se caracterizar como uma solução sem sustentabilidade a médio e longo prazo.

4.1.9. Importante ressaltar que o fabricante dos equipamentos define datas específicas para descontinuidade dos produtos expostos (*end of life*) em seu sítio, conforme pesquisas realizadas em: https://www.extremenetworks.com/support/end-of-sale-and-end-of-support-products/. Com isso, os switches Extreme Networks, modelo Black Diammond 8810 e os switches Extreme Networks Summit X440-24t, estão descontinuados e o fabricante não disponibiliza serviços de suporte e garantia.

4.1.10. Cabe destacar, que além do fato de os referidos equipamentos, tanto do Data Center do núcleo central do Ministério, quanto da sala cofre do CICCN, se encontrarem em estado de obsolescência, estando descontinuados pelo fabricante, ainda a de se considerar as Práticas e Acórdãos que tratam sobre o tema para embasar de forma positiva ou negativa o cenário proposto.

4.1.11. Salienta-se ainda que corroborando com as pesquisas feitas, existem as BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4 (Link), do Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação do STI/MP, que cita a contratação de manutenção dos ativos de TIC fora de garantia como mais onerosa para a Administração Pública, assim como define o ciclo de vida para esses equipamentos:

> ....
>
> *1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de* ***manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração*** *do que quando o bem é adquirido com garantia para toda sua vida útil. (grifo nosso)*
>
> ....
>
> *1.4. ORIENTAÇÕES ESPECÍFICAS SOBRE CICLO DE VIDA*
>
> *1.4.4. ATIVOS DE REDE*
>
> *1.4.4.1 Para aquisição de ativos de rede, tipo equipamentos wi-fi, switches de centro e de borda, roteadores, etc, deve-se considerar* ***o tempo de vida de 5 (cinco) anos*** *para fins de posicionamento da tecnologia e de garantia de funcionamento.(grifo nosso)*

4.1.12. Assim como a apreciação da Egrégia Corte de Contas que exarou entendimento no sentido de condenara prática de atualizações tecnológicas em detrimento da aquisição de novos equipamentos. Para ilustrar cita-se o Acórdão TCU nº 2400/2006 que assim discorreu sobre os serviços de atualização tecnológica e suporte técnico:

"Acórdão TCU n. 2400/2006 – Plenário

> ...
>
> *2.9.2.4 .... do ponto de vista técnico, o fato de existir garantia para os equipamentos que sofrerem atualização nos mesmos níveis que os prestados a equipamentos novos não garante vantagem técnica ao upgrade. Pelo contrário, não se pode esperar que um servidor em gabinete desmontado e remontado em um rack com substituição de quase todos os componentes (ver listagem dos componentes que serão substituídos à fl. 70 do anexo 2), com a permanência de alguns componentes antigos, possa ter menor probabilidade de falha que um equipamento novo que, dependendo do fornecedor, pode ser montado e testado em fábrica. A garantia não diminui o risco de falha e necessidade de substituição de componentes (mais provável no caso do upgrade do que no caso de aquisição de novos servidores), caso em que os equipamentos, mesmo que por pouco tempo, permaneceriam indisponíveis. "*

4.1.13. Dessa forma, seguindo as BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4, do Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação do STI/MP, o acórdão TCU *n. 2400/2006*, além da necessidade de expansão e atualização dos ativos de TIC, a equipe de planejamento contratação entende que a aquisição do serviço de garantia e suporte técnico para os ativos existentes, **não é uma solução viável**, além de implicar em risco elevado para a operação dos serviços críticos de tecnologia da informação providos pelo MJSP devido à indisponibilidade de suporte aos equipamentos por parte do fabricante.

4.2. Solução 2 - Ativos de Redes: Contratação de ativos novos contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses

4.2.1. O presente cenário tem o objetivo de demonstrar a reestruturação e modernização necessária da topologia de ativos de redes (switch core) dos atuais ambientes do Data Center MJSP (núcleo central) e Sala cofre do CICCN-DF (setor policial sul). O objetivo principal da análise é a possibilidade de aquisição de novos switches, expandindo e reestruturando arquitetura da rede MJSP e CICCN-DF, de forma a implementar uma topologia moderna, escalável e de alto desempenho nos Data Centers.

4.2.2. A Figura 15 demonstra quais switches serão desativados no Data Center MJSP - SEDE para reestruturação da arquitetura de redes:

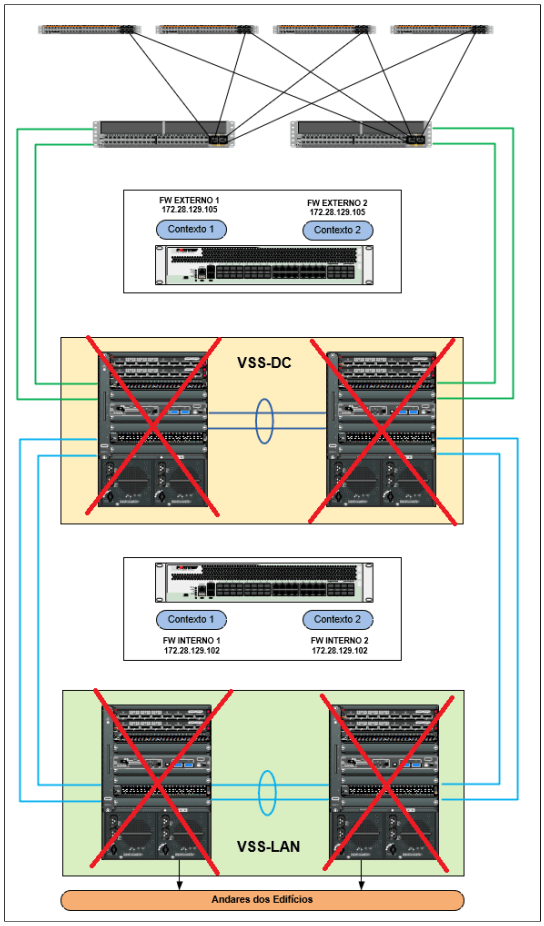

Figura 15 - *Topologia Core Edifício Sede*

4.2.3. Nesse cenário (Figura 15), pretende-se desativar 4 (quatro) switches core 6500 (VSS-LAN) e (VSS-DC) - sem garantia e desatualizados tecnologicamente - todos instalados no Data Center do MJSP (núcleo central), além de reaproveitamento dos demais equipamentos (com suporte e garantia).

4.2.4. Topologia SPINE-LEAF - conceitos e vantagens

4.2.4.1. Para a reestruturação da topologia do presente projeto, pretende-se utilizar o conceito ***Spine-Leaf,*** que consiste em uma espinha dorsal, formada pelo SPINE, e os LEAF, que servem de entrada dos diversos subsistemas de rede. A arquitetura proposta, irá formar um único *Fabric,* que funcionará de forma redundante, em camada 3 e com a utilização de roteamento dinâmico interno ao Data Center.

4.2.4.2. Nessa nova topologia, os switches SPINE funcionam essencialmente como o núcleo da estrutura e os switches LEAF como borda do Fabric, fornecendo conectividade aos servidores e se interligando por meio dos uplinks dos switches Spines. Com isso se permite uma maior velocidade no Fabric, na medida em que são adicionados mais SPINES, ou maior quantidade de portas na medida em que são adicionados mais LEAFES.

4.2.4.3. Esse tipo de arquitetura pode fornecer uma conectividade em camada 2 ou em camada 3 para o Data Center, o que traz um design favorável ao uso dos protocolos TRILL, SPB e FabricPath para balanceamento de tráfego entre os links ativos ao invés do Spanning-Tree. Nesse caso, os servidores já estão conectados ao Fabric, que oferece uma topologia de camada 3 livre de loops.

4.2.4.4. Uma característica importante dessa arquitetura é que, preferencialmente, cada switch LEAF deve se conectar com cada SPINE sem *oversubscription*. Esse ponto é o que resolve o problema do modelo tradicional, já que agora não importa em qual switch um servidor está conectado, ele sempre precisa atravessar a mesma quantidade de dispositivos até chegar a outro servidor. Isso faz com que a latência se mantenha em um nível previsível, pois o tráfego só precisa atravessar um switch SPINE e um LEAF para chegar ao destino.

4.2.4.5. A camada LEAF consiste nos switches de acesso que conectam servidores, *firewalls*, roteadores e demais elementos de rede computacionais, sendo assim não existe comunicação direta entre os Leafs sem passar pelo Spine.

4.2.4.6. A camada do SPINE consiste na interconexão dos LEAFS, nenhum outro equipamento é conectado diretamente ao SPINE.

4.2.4.7. Outro fator importante na implementação dessas topologias é a sua compatibilidade com o conceito de redes definidas por software, mais conhecido como Software Defined Networking (SDN). Essas soluções surgiram para favorecerem a automação e a disponibilização dinâmica por software de recursos de rede através do uso de novos padrões e protocolos, além de oferecerem mais níveis de controle e permitirem o crescimento simplificado da rede.

4.2.4.8. O MJSP está implantando, como solução de SDN, o VMware NSX, que é a plataforma de virtualização e segurança de rede.

4.2.4.9. O NSX, utilizado em arquitetura SPINE-LEAF, possui a possibilidade de criar uma rede com, no máximo, dois saltos da origem ao destino com múltiplos caminhos sendo utilizados simultaneamente. Essa arquitetura ainda reduz o tempo de atraso na entrega do tráfego, reduz o tempo de convergência, a possibilidade de falhas e aumenta o desempenho da rede.

4.2.5. A Figura 16 demonstra como a nova topologia de switches core no Data Center MJSP pode ser estruturada utilizando a arquitetura SPINE-LEAF:

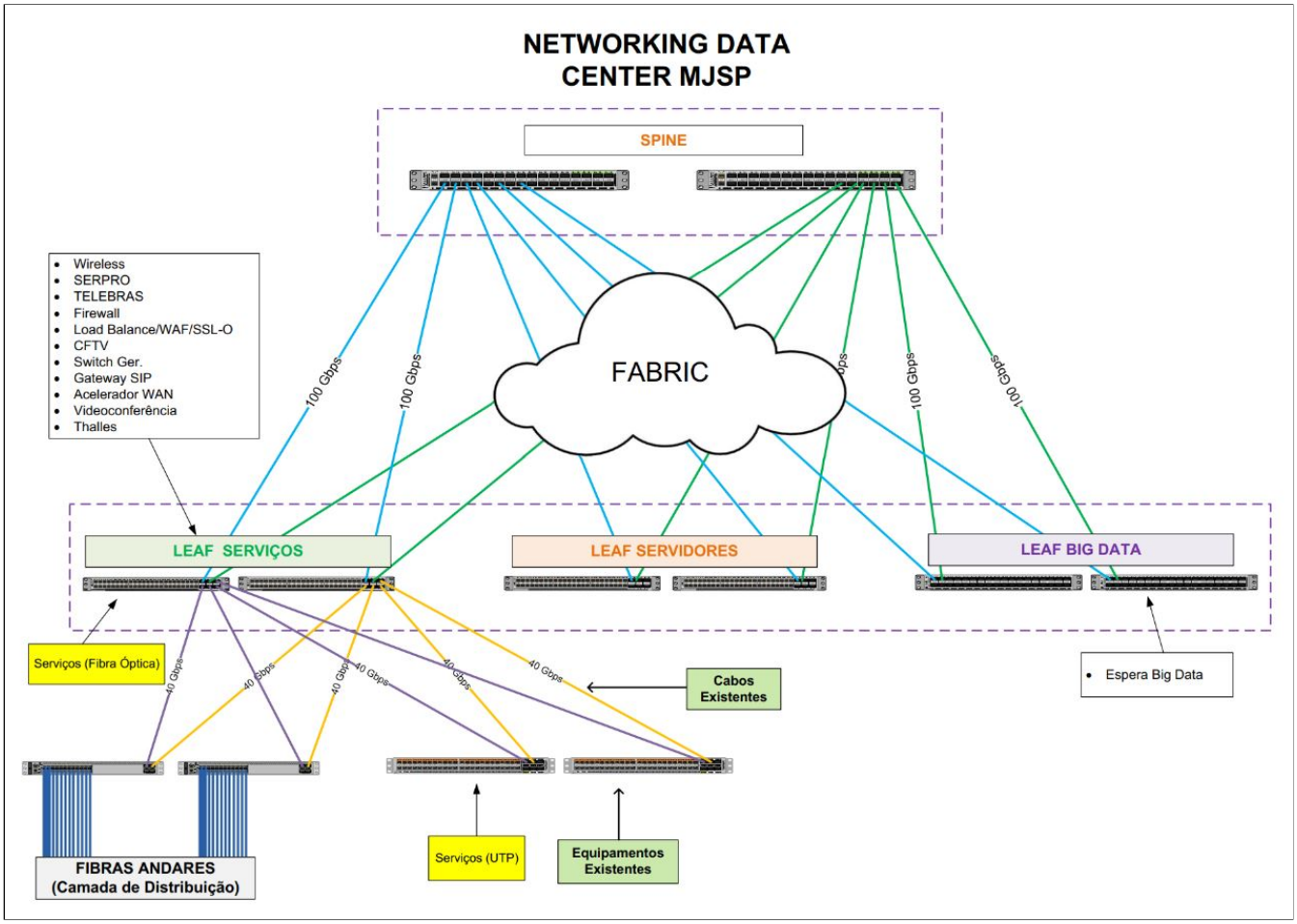

Figura 16 - Previsão da Nova Topologia Core - Data Center MJSP (SPINE LEAF)

4.2.6. A aquisição de novos switches proporcionará a expansão e substituição de equipamentos sem garantia e suporte do fabricante, por equipamentos com maior capacidade de trafego de links, além de permitir a construção de um ambiente simétrico e de alta disponibilidade.

4.2.7. Com o projeto de reestruturação da Camada Core do Data Center MJSP, algumas vantagens serão evidentes, como por exemplo:

- Economia de espaço físico;
- Gerenciamento centralizado;
- Redução de custos de energia e refrigeração pelo uso de menos equipamentos físicos, além do fato de serem mais modernos e eficientes;
- Maior disponibilidade e facilidade na recuperação, em caso de desastres;
- Suporte e manutenção simplificados;
- Melhor aproveitamento do hardware;
- Facilidade de migração de ambientes.

4.2.8. Essas vantagens também colaboram em outra contratação em desenvolvimento pelo MJSP. Trata-se da contratação de empresa para construção de Solução de Ambiente de Alta Disponibilidade para Sistemas Críticos, processo 08006.000180/2019-08, principalmente no que se refere à economia de espaço, à redução de custos de energia e refrigeração pelo uso de menos equipamentos físicos e ao suporte e manutenção simplificados.

4.2.9. A Figura 17 demonstra quais switches serão desativados na Sala Cofre - CICCN:

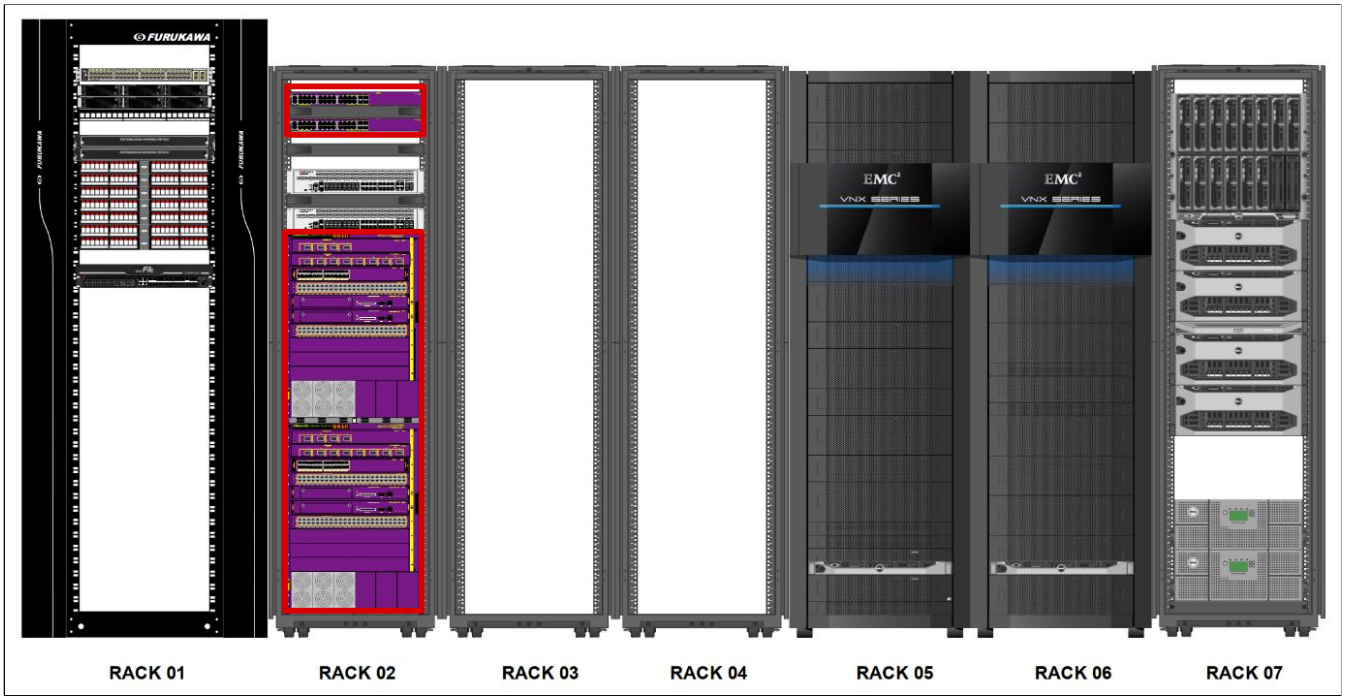

Figura 17 - Sala Cofre - CICCN-DF

4.2.10. Neste cenário (Figura 16), pretende-se desativar 2 (dois) switches Extreme Networks, modelo Black Diammond 8810 (RACK 02) e 02 (dois) switches Extreme Networks Summit X440-24t - sem garantia e desatualizados tecnologicamente - instalados na Sala Cofre do CICCN-DF.

4.2.11. A Figura 18 ilustra como a nova topologia de switches core na Sala Cofre do CICCN-DF será reestruturada:

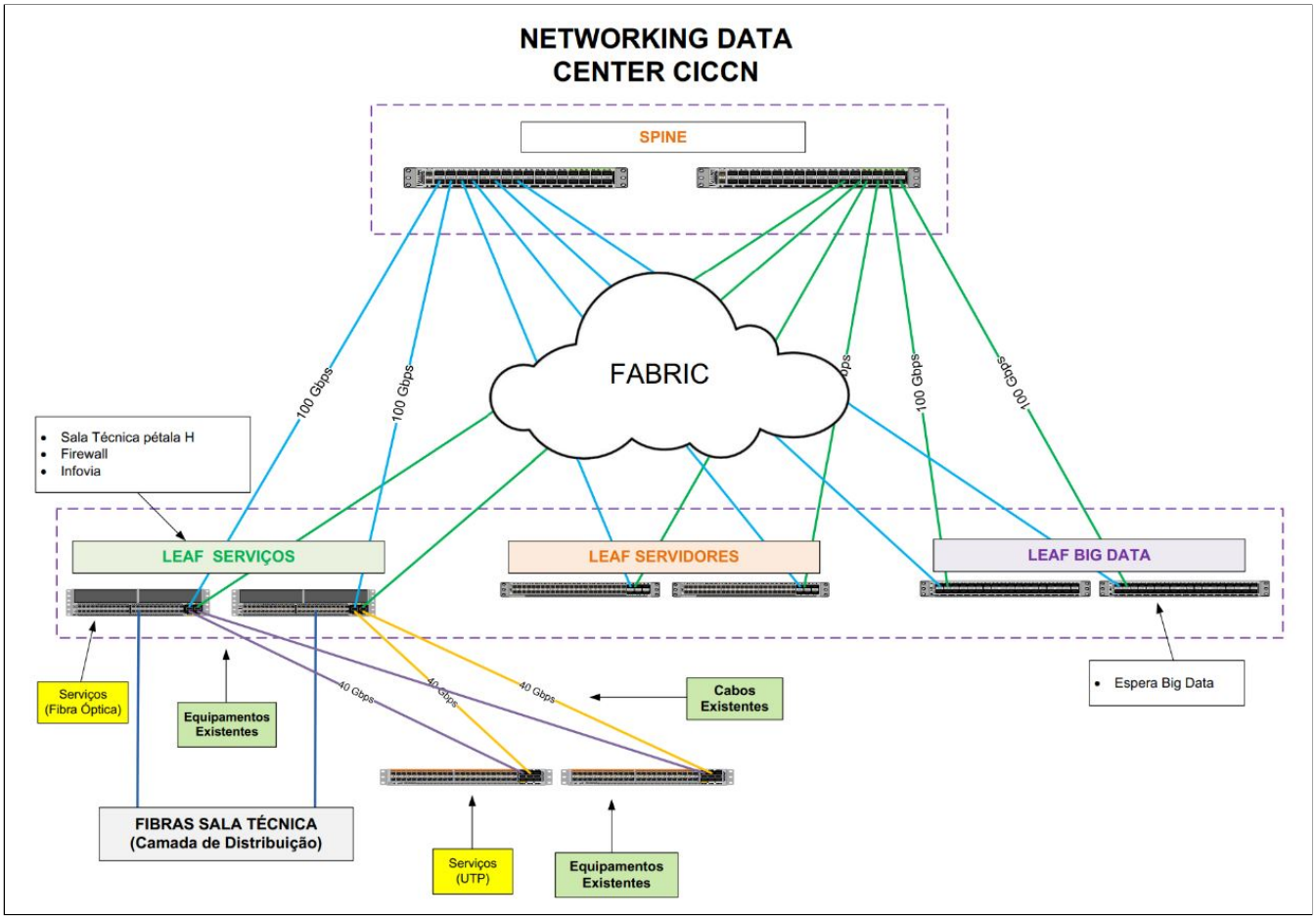

Figura 18 - Previsão da Nova Topologia Core - Sala Cofre CICCN-DF (SPINE LEAF)

4.2.12. Em virtude dos argumentos e vantagens citadas, fica claro o benefício na implementação da arquitetura SPINE-LEAF no ambiente de rede, sendo essa totalmente integrada e compatível tecnologicamente, trazendo como benefício a uniformidade de procedimentos e rotinas de acompanhamento, assistência e suporte técnico, possibilitando uma gestão menos onerosa e complexa para o MJSP, além de prover um serviço com maior disponibilidade aos usuários do Ministério.

4.2.13. Com isso, a fim de prevenir eventuais falhas e oferecer alternativas que evitem que estas acarretem em maiores prejuízos, se faz necessária a aquisição de equipamentos ativos de rede para o ambiente do MJSP, que contemplem planos de redundância e contingência constituídos por uma série de ações e procedimentos que visam soluções e dispositivos de recuperação relacionados com essas falhas.

4.2.14. Diante do exposto, a equipe de planejamento da contratação entende que a contratação de equipamentos ativos de rede novos e compatíveis tecnologicamente com o parque de TIC atual **é o cenário mais viável**, com vistas a mitigar os possíveis riscos da não continuidade dos serviços prestados às áreas de negócio do Ministério da Justiça e Segurança Pública.

5. ANÁLISE DE SOLUÇÕES DE BALANCEAMENTO DE CARGA E SEGURANÇA APLICADA A REDES

5.1. Considerações gerais

5.1.1. Esta análise tem como objetivo demonstrar as possibilidades de aquisição para Solução de Segurança e Balanceamento de Carga. A referida solução traz benefícios significativos para o Ministério da Justiça e Segurança Pública (MJSP) relacionados principalmente ao desempenho, robustez, resiliência, escalabilidade, gerenciabilidade e segurança ao ambiente computacional que está sendo remodelado.

5.1.2. Uma Solução de Balanceamento de Carga, desde a sua concepção, era destinada a ampliar o desempenho de aplicações web pela mera adição de nós de processamento, agrupados sob a forma de uma entidade lógica que passou a ser referenciada como servidor virtual. O serviço básico de SLB (*Server Load Balancing*) utiliza o conceito de Virtual IP, recebendo tráfego de aplicação do lado cliente da conexão e o encaminhando, seletivamente, para cada um dos nós existentes, conforme critérios estabelecidos nas regras de distribuição de carga configuradas.

5.1.3. Os balanceadores, como eram comumente conhecidos, evoluíram, passando a incorporar uma série de outras tarefas associadas ao tratamento de aplicações, que transcendem os aspectos de disponibilidade e desempenho. Essa expansão de escopo de atuação foi tão relevante, que culminou na criação de uma nova categoria de dispositivos denominados *Application Delivery Controllers* (ADCs). Dentre as múltiplas funções disponíveis em um ADC moderno, merecem destaque:

a) ***Server Load Balancing*** **(SLB)** – apesar do foco em disponibilidade e desempenho dos serviços tradicionais de balanceamento, a porção SLB do ADC pode contribuir muito para Segurança (controle nativo de ataques de negação de serviço baseados em TCP SYN Flood, por exemplo).

b) ***Global Server Load Balancing*** **(GSLB)** – peça essencial para permitir alta disponibilidade entre sites, pois permite a seleção do Data Center (DC) que atenderá uma determinada requisição. Após a escolha do DC, o SLB tradicional entra em ação, distribuindo carga entre os servidores (daquele site), conforme algoritmo configurado para o serviço específico. Vale notar que o serviço GSLB é usado entre dispositivos de um mesmo fabricante de ADC, se apoiando nas informações de *health check* providas pelo ADC instalado em cada Data Center. Tal serviço traz outra dimensão para o gerenciamento de tráfego, pois permite promover distribuição não igualitária de carga entre sites geograficamente dispersos, garantindo que os recursos do Data Center Secundário estejam constantemente acessíveis.

c) ***Web Application Firewall*** **(WAF)** – enquanto os web proxies geralmente atuam no lado cliente da conexão, os dispositivos WAF foram concebidos para prover proteção para os servidores Web, funcionando como uma espécie de proxy reverso que pode incluir regras de controle em conversações Web. O WAF complementa a atuação dos firewalls tradicionais, podendo evitar ataques associados a falhas de segurança no desenvolvimento de aplicativos Web, tais como *cross-site scripting* (XSS), *SQL injection* e inclusão de arquivos indevidos na conexão. Nas ofertas mais avançadas de um tal tipo de solução, as atualizações de padrões de ataques (assinaturas) são disponibilizadas, de forma automática, pelo fabricante do WAF para os clientes que possuem contrato de manutenção ativo.

d) **SSL *Offload* –** Dado o peso computacional associado ao tratamento de conexões SSL (necessidade de abertura de SSL), o ADC pode ser configurado para realizar esse trabalho e encaminhar para os servidores reais os pacotes já decriptografados (ou recriptografados com uma chave de tamanho inferior). Como isso, economiza-se processamento dos servidores reais, não havendo a necessidade de renunciar aos aspectos de privacidade da comunicação (mesmo nas conexões locais ao Data Center), uma vez que são mantidas as conexões criptografadas para fora do Data Center. Os ADCs modernos possuem hardwares dedicados para otimizar tais operações.

e) **Visibilidade e Inspeção de SSL** – além da capacidade de realizar o *offload* das conexões SSL dos servidores, o ADC também pode ser utilizado para abrir, de forma centralizada e seletiva, tais conexões criptografadas, de modo a aliviar a exigência de processamento também dos dispositivos clássicos de segurança (Firewall, NG Firewall, IPS, WAF, proxy web, dentre outros). Desta forma, tais elementos especializados podem direcionar seus recursos computacionais para realizar as tarefas de inspeção de tráfego para as quais foram concebidos e otimizados. Além de dar uma sobrevida, no que diz respeito a desempenho, aos equipamentos existentes, tal abordagem aumenta a segurança da rede, contribuindo para eliminar "pontos cegos" decorrentes da onipresença dos canais SSL criptografados. Tal função, dado ao processamento exigido, também é feita com recursos de hardwares dedicados.

f) ***Single Sign On/Multi Factor Authentication*** **(SSO/MFA) –** outra função incorporada aos ADCs é a capacidade de prover, de forma organizada e consistente, controle de acesso a múltiplos sistemas, sem que isso gere um peso adicional de operação. Além disso, permite exigir autenticação e autorização mais elaborada, baseada na validação de múltiplos atributos, antes de conceder o acesso dos usuários a sistemas críticos.

5.1.4. O ambiente do MJSP possui 2 (dois) *sites* sendo um deles o Data Center principal e o segundo, atualmente, com a função de Data Center redundante e backup, funcionando como sistema ativo-*standby*. Em caso de falha do Data Center primário, os principais serviços passam a funcionar no ambiente secundário (backup).

5.1.5. Para analisar as possibilidades de implementação das funcionalidades de um ADC moderno no ambiente do MJSP, existem, porém, pontos específicos a serem considerados quando tratamos tecnicamente de tipos diferentes de Data Center (sendo um principal e um *backup*). Como trata-se de dois ambientes com prioridades diferentes, ou seja, o site principal provê todos os serviços oferecidos pelo MJSP, enquanto o site backup atua fazendo redundância e também em caso de falhas e para serviços pontuais (SEI e Exchange, por exemplo), a escolha da solução para cada um dos Data Centers deve também levar tais pontos em consideração.

5.1.6. Neste cenário, após o estudo de possibilidades existentes no mercado para aquisição da Solução de Balanceamento de Carga e Segurança, optou-se pela aquisição da solução sob a forma de *appliance* físico para o Data Center principal, dada a exigência de hardware dedicado para o tratamento das conexões SSL. Já para o Data Center secundário, não há, num primeiro momento, tal exigência, podendo a solução adotada ser entregue sob a forma de *appliance* virtual. Cabe ainda enfatizar que nem todas as funções de um ADC a serem executadas no Data Center principal exigem hardware dedicado, de modo que possa montar, no Data Central principal, um cenário misto com *appliance* físico e virtual.

5.1.7. Nos próximos itens deste estudo, serão abordados os cenários possíveis de acordo com as melhores práticas de mercado e no âmbito da APF.

5.2. Solução 1 - Balanceamento de Carga e Segurança: Aquisição de appliances físicos para o Data Center Sede e Aquisição de Licenciamento de Software (modelo tradicional) para o CICCN

5.2.1. Este cenário é uma **Aquisição de Solução Física** para o Data Center Sede **e Aquisição de Licenciamento de Software (modelo tradicional)** para o CICCN, sendo utilizados para grandes volumes de conexões e aumento de escala de gerenciamento de tráfego corporativo exigente e / ou complexo. Além disso, trata-se de gerenciadores de tráfego global (DNS) para aumentar a disponibilidade entre Data Centers.

5.2.1.1. Data Center Sede

- O Data Center principal tem a necessidade de alta performance, robustez, resiliência, escalabilidade, gerenciabilidade e, principalmente, segurança para que todos os serviços estejam operando ininterruptamente. A solução física, através de um hardware próprio para balanceamento de carga, GSLB, WAF e Visibilidade SSL, permite que os parâmetros exigidos no termo de referência, como *throughput* da caixa com e sem visibilidade SSL, taxa de compressão,

taxa de *offload* SSL, entre outros, possam ser atingidos para todas as funções esperadas, pois, ao contrário da solução virtualizada, não depende da performance alocado em um servidor físico terceiro, que pode não ser suficiente para desempenhar todas as funções citadas acima.

- Além disso, existe possibilidade de executar várias instâncias virtuais em um mesmo appliance físico, permitindo não somente a seleção de serviços em cada instância, mas também a escolha da versão de Sistema Operacional em cada uma das instâncias (Full Virtualization). O uso de instâncias virtuais permite que se criem contextos de homologação e desenvolvimento, de modo que novas funcionalidades possam ser testadas e validadas antes que venham a ser implantadas no ambiente de produção. Desta forma é possível que sejam testadas, em paralelo com o ambiente de produção, e no mesmo conjunto de elementos que o materializa, novas versões de software que possam ser mais adequadas para cada tipo de aplicação disponível.
- No contexto de segregação de atividades e capacidades, surge uma observação quanto aos serviços que não necessitam de *appliances* tão robustos e que podem ser aprovisionados em soluções virtuais. Isso traz benefícios como melhor aproveitamento dos *appliances físicos com* diminuição do processamento com serviços não essenciais e priorizando o tratamento de tráfego SSL.
- Sendo assim, após uma análise da equipe técnica de planejamento, a solução apresentada para o Data Center Sede não atende às necessidades e requisitos em sua plenitude.

5.2.1.2. Sala Cofre CICCN

- Num cenário tradicional de licenciamento, as capacidades de performance da máquina como *throughput* de camada 4, *throughput* SSL, conexões e requisições por segundo (L4 e L7), taxa de compressão, entre outras são fixas e pouco personalizáveis.
- Neste modelo, o MJSP tem que adquirir uma quantidade já especificada de licenças da solução de ADC, definindo os parâmetros esperados (por exemplo, um *throughput* de 5 Gbps).
- Dada a crescente demanda pelos recursos de um ADC na infraestrutura do MJSP, esta não seria a melhor decisão neste momento, uma vez que não se poderia, por exemplo, reutilizar esta máquina virtual com 5 Gbps licenciado em múltiplas máquinas virtuais de menor capacidade, uma vez tratar-se de aprovisionamento único e perpétuo, não sendo possível aplicar uma segmentação do *throughput* de 5 Gbps.
- Cabe ressaltar que a perpetuidade das licenças não significa que, passado o período de suporte contratado, o MJSP poderia continuar usufruindo plenamente da solução, uma vez que sem um contrato de suporte ativo, não há mais garantia de atualização de versão de software por parte do fabricante e, consequentemente, garantia de compatibilidade com os novos recursos instalados.
- Diante disso, entende-se como fator fundamental, para a solução de balanceamento e segurança do CICCN, a capacidade de segmentação, realocação e reutilização de forma que garanta máquinas com *throughput* personalizáveis. Desta forma, a solução apresentada para a Sala Cofre do CICCN Sede não atende a todos os requisitos em sua totalidade.

5.2.1.3. Diante do exposto, levando em conta a crescente demanda pelos recursos de um ADC na infraestrutura do MJSP, assim como considerando a forma de provisionamento estático da solução, além do suporte, garantia e atualizações que, passado o período de suporte contratado, ficariam comprometidos, a equipe de planejamento da contratação entende que a **Aquisição de Solução Física** para o Data Center Sede **e Aquisição de Licenciamento de Software (modelo tradicional) não é uma solução viável** para o Ministério da Justiça e Segurança Pública.

5.3. Solução 2 - Balanceamento de Carga e Segurança: Aquisição de solução Física e Virtual para o Data Center Sede e Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA))

5.3.1. Este cenário é uma aquisição de solução **Física e Virtual** para o Data Center Sede **e Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA))** para o CICCN, sendo utilizados para grandes volumes de conexões e aumento de escala de gerenciamento de tráfego corporativo exigente e / ou complexo. Além disso, também são gerenciadores de tráfego global (DNS) para aumentar a disponibilidade entre Data Centers.

5.3.1.1. Data Center Sede

- Através de um cenário misto de implementação (Física e Virtual), utilizando um ambiente físico para as funções que exigem alto processamento (tratamento de tráfego SSL) e *appliances* virtuais para as demais funcionalidades, pode-se buscar otimizar o tamanho de cada uma das soluções de acordo com a necessidade.
- Da mesma forma que no ambiente totalmente físico, quando utilizada múltiplas instâncias, a solução virtualizada também permite a escolha da versão de Sistema Operacional em cada provisionamento feito, usufruindo dos mesmos benefícios citados anteriormente.
- A utilização da implementação de uma solução virtualizada para as demais funções de uma ADC evita o desperdício de recursos de hardware (CPU, memória e interfaces de rede) nos elementos de serviço, pois é possível alocar tais tipos de recurso para cada máquina virtual provisionada, de acordo com a demanda específica da aplicação que por ela será atendida.

5.3.1.2. Sala Cofre CICCN

- Atualmente, a maioria dos fabricantes possui uma modalidade de aquisição de licenciamento de software, chamado de *Enterprise Agreement* (EA), em que a solução é ofertada sob a forma de um direito de uso, em que o cliente tem a flexibilidade de utilização da solução, nas suas mais variadas métricas, enquanto existir um contrato ativo.
- Com este cenário, o MJSP, ao adquirir um pacote de *throughput* 20 Gbps, que pelas análises técnicas e com a previsão de crescimento, seja o adequado em um primeiro momento, passa a poder utilizar tal capacidade na mesma medida de suas necessidades, podendo ser aprovisionadas quantas e em quaisquer tamanhos de máquinas sejam necessárias desde que somadas utilizem o *throughput* total contratado.

5.3.2 Apresentados os cenários de aquisição do licenciamento para as máquinas virtuais, concluímos que o benefício da flexibilidade e dinamicidade que o modelo de *Enterprise Agreement* oferece é o fator chave para a tomada de decisão, uma vez que, em um ambiente cada vez mais mutável, as máquinas virtuais poderão ser alocadas (e excluídas) sem maiores preocupações com o licenciamento, permitindo, inclusive, que o MJSP utilize de todas as funcionalidades de um ADC tanto no seu Data Center Sede quanto no CICCN-DF, como também, eventualmente, qualquer outro site, inclusive em ambientes de nuvem (pública ou privada).

5.3.3. Em virtude dos fatos mencionados, a solução **Física e Virtual** para o Data Center Sede **e Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA))** para o CICCN **é o cenário mais viável**, com vistas os benefícios de elasticidade, mobilidade e dinamicidade prestados às áreas de negócio do Ministério da Justiça e Segurança Pública.

5.4. Solução 3 - Balanceamento de Carga e Segurança: Utilização da computação em nuvem para suprir necessidade de Balanceamento de Carga e Segurança

5.4.1. O presente cenário tem o objetivo de analisar a possibilidade de utilização da computação em nuvem pública para suprir a necessidade de balanceamento de carga e segurança.

5.4.2. Conforme previsto no item 4, do anexo da INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019, os órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a

inviabilidade em estudo técnico preliminar da contratação.

5.4.3. Cabe destacar que a DTIC/MJSP vislumbra benefícios na adoção de serviços de computação em nuvem nas modalidades infraestrutura e plataforma como serviço, sendo esta uma tendência a médio e longo prazo. No entanto, deve ser considerado que já foram feitos investimentos consideráveis em infraestrutura própria de TIC, por meio da aquisição de servidores, storages e equipamentos de rede de dados.

5.4.4. Destaca-se que existem algumas estratégias iniciais no MJSP para adoção de serviços de computação em nuvem. Atualmente o Ministério conta com o contrato nº 28/2018 (8964029), que disponibiliza créditos na Azure Public Cloud, da Microsoft. No entanto, mesmo considerando o uso atual das soluções de IaaS e Paas do fornecedor, a estratégia do MJSP para a sustentação de serviços de TIC não permite prescindir de infraestrutura *on premise*, por considerar que ainda há grande risco para a sustentação e operação de serviços críticos caso seja feita a opção pela adoção de infraestrutura puramente em nuvem, pois, neste caso, não existiria uma alternativa para manter a sustentação dos sistemas corporativos caso houvesse alterações nas previsões orçamentárias ou na política de preços dos fornecedores. É dentro deste contexto que a instituição considera ser necessário dotar a infraestrutura de ativos de redes e segurança local com recursos mínimos capazes de garantir a alta disponibilidade dos serviços.

5.4.5. O Ministério da Justiça já conta atualmente com contrato de provimento de serviços de computação em nuvem, e possui estratégia de expandir a adoção desses serviços, especialmente em casos em que não houver o tratamento de dados sigilosos. No entanto, tal circunstância não exime a responsabilidade de se manter aderente à legislação no caso de tratamento de dados sigilosos, conforme discutido acima. Além disso, não se vislumbra a computação em nuvem como **alternativa técnica viável para a operacionalização de sistemas legados** que permanecem sendo utilizados no âmbito da instituição, e tampouco há alternativa para a sustentação segura desses sistemas *on premise* sem que haja um reforço e reformulação de estrutura dos ativos de redes, balanceamento de carga e segurança, além do fato que o reforço dessa infraestrutura atua no sentido de preservar os investimentos já realizados.

5.4.6. Além das razões acima, vários aspectos de sigilo, segurança e riscos devem ser avaliados quando se fala em computação em nuvem, principalmente na questão da governança dos dados, pela própria característica institucional e pela sensibilidade das informações tratadas pelo Ministério da Justiça e Segurança Pública. Um aspecto relevante a ser considerado é a natureza das informações com as quais o Ministério da Justiça e Segurança Pública deve lidar para a execução das suas competências, e o nível de sigilo que deve ser a elas assegurado. Em muitos casos trata-se de dados contendo informações sensíveis para as quais o acesso deve ser restrito, como é o caso de informações que dizem respeito à vida privada e intimidade de cidadãos brasileiros e de estrangeiros residentes no Brasil. Em alguns casos, a imposição de sigilo das informações é algo previsto na própria legislação.

5.4.7. Tais características contraindicam, nos termos do item 5.2.2 da Norma Complementar nº 14 da Instrução Normativa nº 01/2008-DSIC/GSI, a utilização de forma irrestrita de recursos de computação em nuvem para esses fins, o que se enquadra nas exceções às recomendações do Ministério da Economia de dar preferência a contratações de serviços de nuvem pública ou privada para suportar os serviços de TIC da Administração Pública Federal. A Norma Complementar nº 14 ainda veda terminantemente a utilização de nuvem para o armazenamento de informações classificadas nos graus de sigilo (ultrassecreta, secreta ou reservada) estabelecidos pelo Art. nº 24 da Lei nº 12.527/2011 (Lei de Acesso à Informação). Todas as essas restrições implicam na necessidade de investimento em ativos de redes, balanceamento de carga e segurança para suportar os projetos do MJSP que irão necessitar de recursos de Tecnologia da Informação, em particular nos projetos que irão lidar com grandes volumes de dados sensíveis, como é o caso do projeto SINESP BIG DATA.

5.4.8. Dessa forma, a equipe de planejamento da contratação entende que o presente cenário **não é uma solução viável** para o momento para a totalidade das necessidades do MJSP, por não se enquadrar nos aspectos legais relativos ao tratamento dos dados sensíveis e ainda por representar risco para a continuidade de negócios caso seja utilizada de forma exclusiva.

6 – IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
	Ativos de Redes
1	Contratação de serviço de garantia e suporte técnico para os ativos existentes
2	Contratação de ativos novos contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses
	Solução de Balanceamento de Carga e Segurança Aplicada a Redes
1	Aquisição de appliances físicos para o Data Center Sede e Aquisição de Licenciamento de Software (modelo tradicional) para o CICCN
2	Aquisição de solução Física e Virtual para o Data Center Sede e Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA))
3	Utilização da computação em nuvem para suprir balanceamento de carga e segurança

7 – ANÁLISE COMPARATIVA DE SOLUÇÕES

Ativos de Redes				
Requisito	**Solução**	**Sim**	**Não**	**Não se Aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1		x	
	Solução 2	x		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			x
	Solução 2			x
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			x
	Solução 2			x

Ativos de Redes				
Requisito	**Solução**	**Sim**	**Não**	**Não se Aplica**
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			x
	Solução 2			x
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			x
	Solução 2			x
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			x
	Solução 2			x

Solução de Balanceamento de Carga e Segurança Aplicada à Redes				
Requisito	**Solução**	**Sim**	**Não**	**Não se Aplica**
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	x		
	Solução 2	x		
	Solução 3		x	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			x
	Solução 2			x
	Solução 3			x
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			x
	Solução 2			x
	Solução 3			x
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			x
	Solução 2			x
	Solução 3			x
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			x
	Solução 2			x
	Solução 3			x

Solução de Balanceamento de Carga e Segurança Aplicada à Redes				
Requisito	**Solução**	**Sim**	**Não**	**Não se Aplica**
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			x
	Solução 2			x
	Solução 3			x

8 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

8.1. **Ativos de Redes**

8.1.1. Solução 1: Entende-se que este cenário não é viável em virtude das BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC - Versão 4, do Departamento de Segurança da Informação, Serviços e Infraestrutura de Tecnologia da Informação do STI/MP, o acórdão TCU *n. 2400/2006*, além da necessidade de expansão e atualização dos ativos de TIC.

8.1.2. Dessa forma, a equipe de planejamento contratação entende que a aquisição do serviço de garantia e suporte técnico para os ativos existentes não é uma solução viável, pois além de os equipamentos possuírem mais de 5 anos de operação, apresenta risco elevado para a operação dos serviços críticos de tecnologia da informação providos pelo MJSP devido à indisponibilidade de suporte aos equipamentos por parte do fabricante (*end of life*).

8.2. **Solução de Balanceamento de Carga e Segurança Aplicada a Redes**

8.2.1. Solução 1: Após uma análise da equipe técnica de planejamento, a solução apresentada para o Data Center Sede não atende às necessidades e requisitos em sua plenitude.

8.2.2. Solução 3: Não é uma solução viável para o momento para a totalidade das necessidades do MJSP, por não se enquadrar nos aspectos legais relativos ao tratamento dos dados sensíveis e ainda por representar risco para a continuidade de negócios caso seja utilizada de forma exclusiva.

9 – ANÁLISE COMPARATIVA DE CUSTOS (TCO)

9.1. **Ativos de Redes**

9.1.1. Não se aplica, pois apenas 1 (uma) solução (Contratação de ativos novos contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 meses) encontra-se viável não sendo possível realizar comparação com outra, conforme previsto no art. 11, § 1º da INSTRUÇÃO NORMATIVA Nº 1, DE 4 DE ABRIL DE 2019.

9.2. **Solução de Balanceamento de Carga e Segurança Aplicada a Redes**

9.2.1. A análise comparativa de custos foi realizada levando em consideração a única solução viável (Aquisição de solução Física e Virtual para o Data Center Sede e Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA).

9.2.2. Nessa solução, a equipe constatou que a Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA) pode ser contratada sob 3 (três) cenários, sendo elas: Contrato de 36 meses com pagamento anual, Contrato de 12 meses com pagamento único (renováveis até 36 meses) e Contrato de 36 meses com pagamento único.

9.2.3. Abaixo, encontra-se a tabela comparativa com cada uma dessas modalidades:

Descrição	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
Contrato de 36 meses com pagamento anual	R$ 1.779.480,00	R$ 1.779.480,00	R$ 1.779.480,00	**R$ 5.338.440,00**
Contrato de 12 meses (renováveis até 36 meses)	R$ 3.118.680,00	R$ 3.118.680,00	R$ 3.118.680,00	**R$ 9.356.040,00**
Contrato de 36 meses com pagamento único	R$ 4.411.800,00	-	-	**R$ 4.411.800,00**

9.2.4. Diante disso, a equipe também pesquisou por contratações que foram realizadas utilizando **Contrato de 36 meses com pagamento único**, cabendo destacar que são contratações com durações iguais ou superiores a 36 meses, com pagamento único, realizados em períodos/anos diferentes e com objeto semelhantes, que podem ter valores diferentes dependendo das especificações técnicas de cada um.

9.2.5 Os seguintes resultados foram encontrados:

ÓRGÃO OU ENTIDADE	CONTRATO/PREGÃO	ITEM/DESCRIÇÃO	DURAÇÃO
MEC -Ministério da Educação	15/2019	Aquisição de Solução de Segurança da Informação Application Delivery Controller (ADC), com funções de balanceador de carga e aceleração web com módulos de Loading Balance, Global Server Loading Balance, Web Application Firewall e SSL offload e inspection (LB/GSLB/WAF/SSL),	36 meses
ANA - Agência Nacional de Águas	18/2019	Aquisição de plataforma de software de geoprocessamento para continuidade das atividades de análise, visualização, layout de mapas, coleta de dados e disponibilização on-line, pela internet de dados geográficos, mapas, imagens de satélite, resultados de análise espacial e geográfica de dados da Agência Nacional de Águas - ANA.	36 meses
Procuradoria Geral do Trabalho	23/2019	Contratação de empresa especializada na renovação da prestação de serviços de manutenção e suporte técnico on site para equipamentos F5 BIG-IP 3600 e ampliação, instalação e configuração desta solução de balanceamento de carga	36 meses
SEGETH-DF	12/2016	Licenciamento Corporativo Esri (ELA) e Suporte Especializado 36 meses	36 meses

ANEEL	62/2018	Contrato de Prestação de serviços de atualização tecnológica das licenças da plataforma ArcGIS	36 meses
CAESB – Companhia de Abastecimento do DF	8672/2016	Licenciamento Corporativo Esri (ELA) e Suporte Especializado 48 meses	48 meses

9.2.6. Sendo assim, observa-se que a vigência do contrato de 36 meses, com pagamento único, é utilizado em contratações com objetos semelhantes.

9.2.7. Desse modo, sob o posto de vista econômico, é mais vantajosa a Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA) com a vigência do contrato de 36 meses com pagamento único, ao invés de renovações a cada 12 meses ou contrato de 36 meses com pagamento anual.

9.2.8. Esta contratação, com a vigência do contrato de 36 meses com pagamento único, se enquadra no inciso IV do art. 57 da Lei 8.666/93 e se dá em virtude da natureza dos serviços contratados, conforme previsto na Orientação Normativa da AGU 38 de 2011:

> *ORIENTAÇÃO NORMATIVA Nº 38, DE 13 DE DEZEMBRO DE 2011 (*)*
>
> *"NOS CONTRATOS DE PRESTAÇÃO DE SERVIÇOS DE NATUREZA CONTINUADA DEVE-SE OBSERVAR QUE: A) O PRAZO DE VIGÊNCIA ORIGINÁRIO, DE REGRA, É DE ATÉ 12 MESES; B) EXCEPCIONALMENTE, ESTE PRAZO PODERÁ SER FIXADO POR PERÍODO SUPERIOR A 12 MESES NOS CASOS EM QUE, DIANTE DA PECULIARIDADE E/OU COMPLEXIDADE DO OBJETO, FIQUE TECNICAMENTE DEMONSTRADO O BENEFÍCIO ADVINDO PARA A ADMINISTRAÇÃO; E C) É JURIDICAMENTE POSSÍVEL A PRORROGAÇÃO DO CONTRATO POR PRAZO DIVERSO DO CONTRATADO ORIGINARIAMENTE." (grifo nosso)*

9.2.9. Diante do exposto, entendemos ser mais vantajoso economicamente e tecnicamente para o Ministério da Justiça e Segurança Pública que a vigência se der pelo prazo de 36 (trinta e seis) meses, nos termos do inciso IV, do art. 57 da Lei 8.666/93.

10 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Ativos de Redes

10.1. **Solução 2** -Trata-se da solução de **Contratação de ativos novos contemplando serviços de instalação e suporte técnico com garantia pelo período de 60 mes** redundância e contingência constituídos por uma série de ações e procedimentos.

10.1.1. A equipe de planejamento da contratação entende que a aquisição de equipamentos ativos de rede novos e compatíveis tecnologicamente com o parque t mais viável, com vistas a mitigar os possíveis riscos da não continuidade dos serviços prestados às áreas de negócio do Ministério da Justiça e Segurança Pública compatibilidade tecnológica com os investimentos já feitos pelo órgão nos anos anteriores.

10.1.2. Os quantitativos foram definidos considerando as necessidades imediatas e futuras do Ministério da Justiça e Segurança Pública (MJSP), levando e características de escalabilidade e desempenho.

10.1.3. Há a previsão de switches com velocidades de portas 10, 25, 40 e 100 Gbps, cujas modularidades foram definidas tomando como base aspectos técnicos co pela área técnica, considerando os mais importantes fabricantes e fornecedores de cada tipo de equipamento. É essencial que esses equipamentos o compatibilidade com ferramentas de gerenciamento existentes no parque de ativos de TIC do MJSP.

10.1.4. Outro ponto que foi levado em consideração na definição dos quantitativos de switches e portas de cada equipamento foi a relação entre SPINE x LE/ minimizar o *oversubscription* na rede, inclusive considerando alguns cenários de múltiplas falhas dos equipamentos e de suas conexões, de modo que se poss grande parte dele) entre as referidas camadas.

10.1.5. Para atender a longevidade prevista do projeto, é vital que os equipamentos de todas as camadas, principalmente a Camada Central e a Camada de possuam redundância, sejam flexíveis (física e funcionalmente) e escaláveis. Isso se reflete na decisão de selecionar switches de núcleo que sejam capazes de sup estratégicas de portas físicas.

Solução de Balanceamento de Carga e Segurança Aplicada a Redes

10.2. **Solução 2** - Trata-se da **Aquisição de solução Física e Virtual para o Data Center Sede e Aquisição de Licenciamento de Software (*Enterprise Agreement* (EA)**

10.2.1. A equipe de planejamento da contratação entende que a aquisição de solução Física e Virtual para o Data Center Sede e Aquisição de Licenciame *Agreement* (EA)) é o cenário mais viável, com vistas a um ambiente cada vez mais mutável, as máquinas virtuais poderão ser alocadas (e excluídas) sem m licenciamento, permitindo, além disso, que o MJSP utilize de todas as funcionalidades de um ADC tanto no seu Data Center Sede quanto no CICCN-DF.

10.2.2. Os quantitativos também foram definidos considerando as necessidades imediatas e futuras do Ministério da Justiça e Segurança Pública (MJSP), levando características de expansibilidade, flexibilidade e desempenho.

10.2.3. Há a previsão de *Appliance* Físico para o Site Principal(com funções de tratamento de tráfego SSL), possibilidade de utilização futura de todas as fun *Appliance* Físico (licenciamento adicional) e Licenciamento compartilhando entre os Data Centers Principal e Secundário sob a forma de *Enterprise Agreement,* definidas tomando como base aspectos técnicos considerados como essenciais pela área técnica, considerando os mais importantes fabricantes e fornecedores.

10.3. Com o objetivo de detalhar e ilustrar a arquitetura SPINE-LEAF, que pretende-se adotar nos sites MJSP e CICCN-DF, a equipe técnica expandiu a visão tanto da geral), quanto dos LEAFS de SERVIÇOS, SERVIDORES, e BIG DATA, assim como da Solução de Balanceamento de Carga e Segurança, conforme exposto abaixo:

10.3.1. Ativos de redes - Detalhamento de topologias e equipamentos para o site do núcleo central do MJSP.

10.3.1.1. Topologia SPINE-LEAF

10.3.1.1.1. A topologia é composta por equipamentos que compõem as camadas de SPINE e LEAF (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA).

10.3.1.1.2. Como pode ser observado na Figura 19, são detalhados, de forma meramente ilustrativa, os equipamentos com suas respectivas quantidade conectividade, formando assim o *Fabric.*

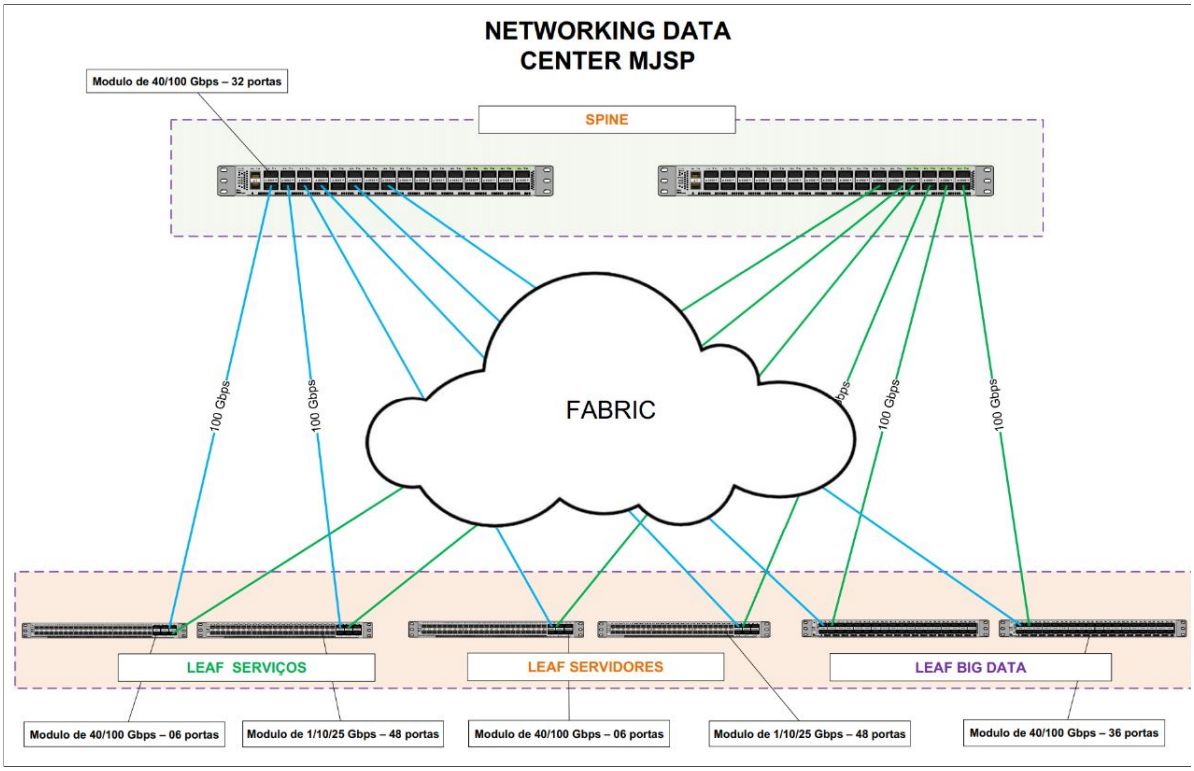

Figura 19 - Topologia SPINE-LEAF

10.3.1.1.3. Para os equipamentos na camada SPINE, há a previsão de switches de 32 portas 40/100 Gigabit Ethernet, cujas modularidades foram definidas tor técnicos considerados como essenciais pela área técnica responsável, assim como características de escalabilidade para uso estimado de 05 (cinco) anos.

10.3.1.1.4. Os switches do SPINE, inicialmente, se conectam com os switches LEAFS (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA) a uma velocidade de cor porta. Para interconexão entre os switches do SPINE e os switches LEAFS estão sendo previstos Cabos de Conexão Direta de 100 Gbps.

10.3.1.1.5. O quantitativo de equipamentos para a camada SPINE, bem como os Cabos de Conexão Direta para conexão dos LEAF, são:

CAMADA SPINE	
Quantidade	**Descrição**
02	Switches de Núcleo (Core Switch), composto por 32 (trinta e duas) portas 40/100 Gigabit Ethernet, em cada switch, para interconexão com os switches Leafs (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA)
12	Cabos de Conexão Direta 100G – (10 metros, mínimo)

Tabela 01 - quantitativos camada Spine

10.3.2. Nos próximos itens serão detalhadas as topologias de cada LEAF, com suas respectivas características.

10.3.1.2. Topologia LEAF SERVIÇOS

10.3.1.2.1. O LEAF SERVIÇOS irá concentrar toda a parte de conectividade externa e interna da rede, bem como serviços acessórios que não estarão diretar SERVIDORES e LEAF BIG DATA. Inicialmente estarão conectados no referido LEAF os seguintes serviços:

a) Controladoras Wi-fi;

b) Roteador Telebras (internet e MPLS);

d) Switch SERPRO (Internet e INFOVIA);

f) Firewalls (interno e externo);

g) Switches de agregação dos andares;

10.3.1.2.2. Além disso, para o provisionamento de portas UTPs, serão reaproveitados dois equipamentos existentes no Data Center, Extensor de fabric Cisco 1/10G, 6 portas de uplink 40G QSFP (PART NUMBER N2K-C2348TQ), que foram adquiridos por meio do Processo Administrativo nº (08006.001634/2016-15). Inicia aos Extensor de fabric Cisco Nexus 2348 os seguintes serviços:

a) Gateway SIP;

b) Aceleradores de WAN;

c) Videoconferência

d) Thalles

10.3.1.2.3. Para conexão entre os novos equipamentos, e os existentes, serão reaproveitados cabos de Conexão Direta de 40 Gbps que acompanham o Extensor de

10.3.1.2.4. Conforme ilustrado na Figura 20, a topologia LEAF SERVIÇOS é composta por equipamentos de alta disponibilidade de banda, baixa latência e expansíve

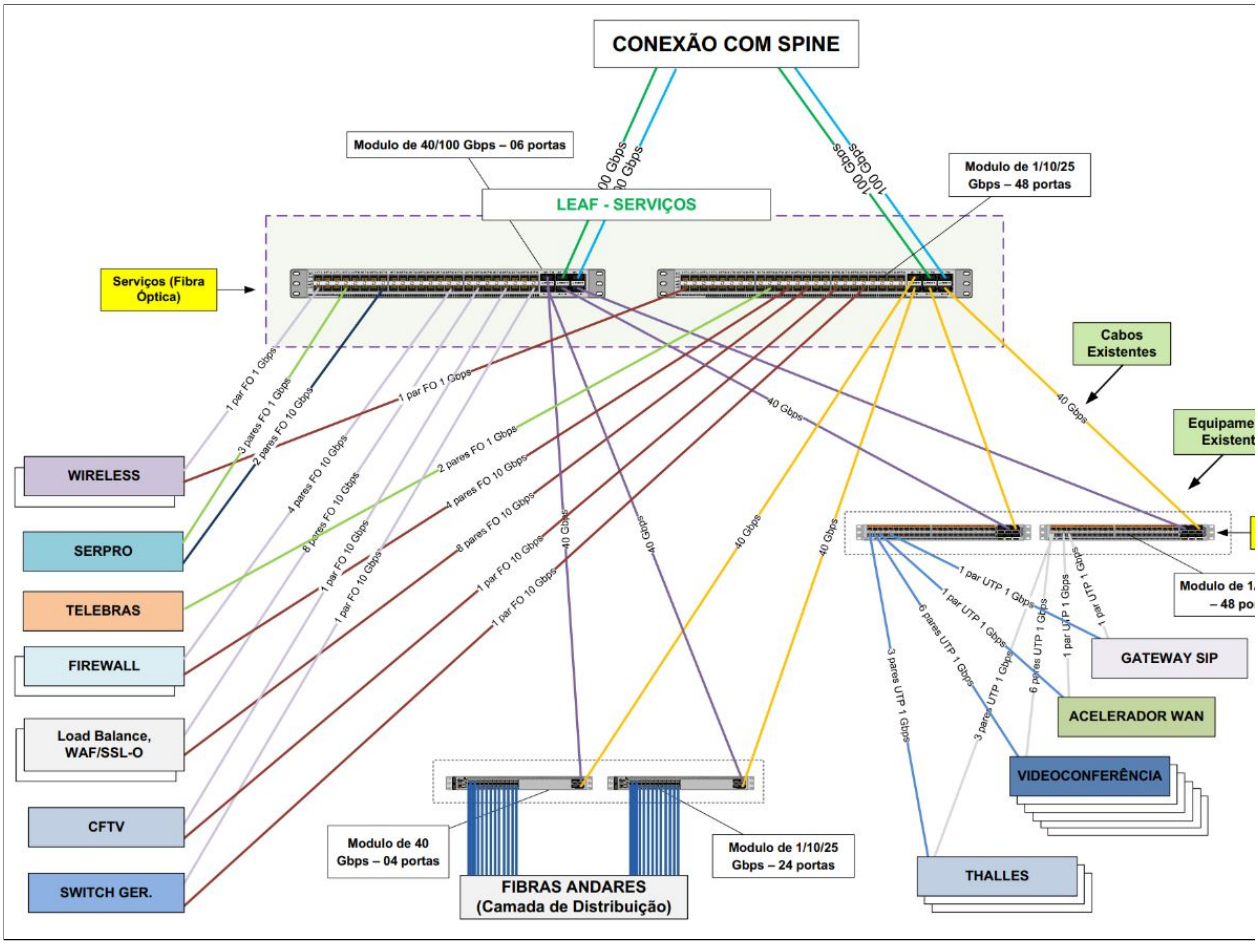

Figura 20 - LEAF SERVIÇOS

10.3.1.2.5. Para os equipamentos do LEAF SERVIÇOS, há a previsão de switches com no mínimo de 48 portas 1/10/25 Gbps, com no mínimo 6 portas de 40/10 aspectos foram definidos tomando como base requisitos técnicos considerados como primordiais pela área técnica responsável, assim como características de cre de 05 (cinco) anos. Deverão ser previstos transceivers, totalmente compatíveis tecnologicamente com os equipamentos, para interconexão dos demai controladoras *Wi-fi*, Aceleradores de WAN e Roteador Telebras, Switch SERPRO e gateway SIP).

10.3.1.2.6. Para os equipamentos de agregação dos andares, há a previsão de switches com no mínimo 24 portas 1/10/25 Gbps, contendo no mínimo 4 portas d fibras dos andares, assim como há previsão de Transceivers para interconexão dos andares, tanto para o lado do Data Center, quanto para as 16 (dezesseis) sala atualmente existentes nas 16 salas técnicas e que fazem a distribuição são do modelo WSC3650-24PD (PART NUMER C1-WS3650-24PD/K9). Aqui, cabe destacar a r serem totalmente compatíveis tecnologicamente com os equipamentos que fazem a distribuição nos andares (Modelo de transceivers atualmente instalados: modificação necessária por incompatibilidade pode causar impacto no acesso dos usuários à rede MJSP.

10.3.1.2.7. É importante também prever conectividade para soluções que serão renovadas em um futuro próximo, como é o caso da Solução de Segurança de Pe 08006.001190/2016-18), e que necessitam de conexões junto ao LEAF SERVIÇOS, sendo um requisito fundamental que essas ligações promovam maiores capaci banda e densidade.

10.3.1.2.8. Nessa linha, após análise técnica, se faz necessário para nova Solução de Segurança de Perímetro (Firewall) que este projeto contemple Transc totalmente compatível com os switches de 48.

10.3.1.2.9. Para interligação dos equipamentos do LEAF SERVIÇOS com o Switches de agregação dos andares, deverão ser previstos Cabos de Conexão Direta de 40

10.3.1.2.10. Sendo assim, projeta-se que esses switches supram os requisitos expostos, com eficiência na comunicação, alta disponibilidade de banda e baixa latênc

10.3.1.2.11. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF SERVIÇOS:

LEAF SERVIÇOS	
Quantidade	**Descrição**
02	Switches de Agregação, composto por, no mínimo, 48 (quarenta e oito) portas, 1/10/25 Gbps, com no mínimo 06 portas de 40/100, em cada switch
02	Switches de Agregação composto por, no mínimo, 24 (vinte e quatro) portas 1/10/25 Gbps, com no mínimo 04 portas de 40G, em cada switch
04	Cabos de Conexão Direta 40G, 10 metros, mínimo
90	Transceivers, 10G Multimodo, LC, totalmente compatível com os switches de 48 e 24 portas
16	Transceivers, 25G Multimodo, LC, totalmente compatível com os switches de 48.
30	Cordões Óptico, 10G Multimodo, LCxLC, 10 metros, mínimo

***Tabela 02 - quantitativos* LEAF SERVIÇOS**

10.3.1.3. Topologia LEAF SERVIDORES

10.3.1.3.1. O LEAF SERVIDORES, como o próprio nome já diz, irá concentrar todos os servidores do Data Center.

10.3.1.3.2. Conforme descrito na Figura 21, a topologia LEAF SERVIDORES também será composta por equipamentos de alta disponibilidade de banda, baixa latênc

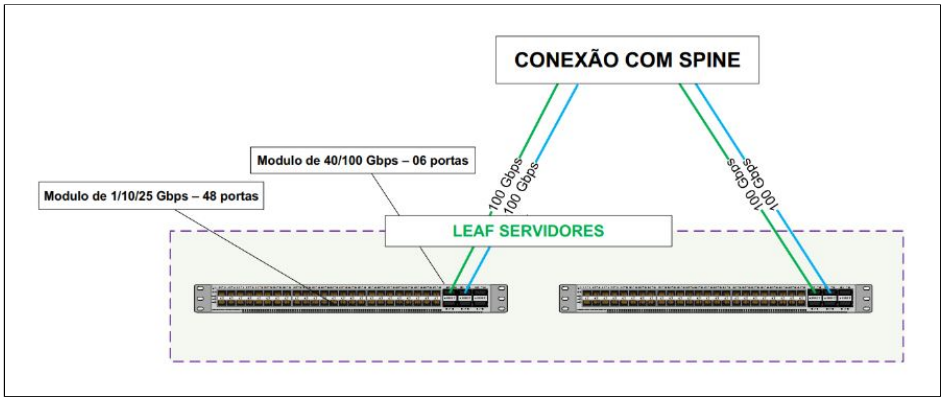

Figura 21 - LEAF SERVIDORES

10.3.1.3.3. Para os equipamentos do LEAF SERVIDORES, há a previsão de switches com no mínimo de 48 portas 1/10/25 Gbps, com no mínimo 6 portas de 40/10 foram determinados com base nos requisitos técnicos considerados fundamentais pela área técnica, assim como características de ampliação para uso estimado ser previstos transceivers, totalmente compatíveis tecnologicamente com os equipamentos, para interconexão dos servidores aos switches do LEAF SERVIDORES.

10.3.1.3.4. Com isso, entende-se que esses switches supram as exigências apresentadas, com aprimoramento de tráfego leste-oeste, eficiência na comunicação, a e baixa latência entre os nós.

10.3.1.3.5. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF de SERVIDORES:

LEAF SERVIDORES	
Quantidade	**Descrição**
02	Switches de Agregação, composto por, no mínimo, 48 portas, 1/10/25, com no mínimo 6 portas 40/100, em cada switch
48	Transceivers, 10G Multimodo, LC, totalmente compatível com os switches de 48 portas

***Tabela 03 - quantitativos* LEAF SERVIDORES**

10.3.1.4. Topologia LEAF BIG DATA

10.3.1.4.1. O LEAF BIG DATA, como o próprio nome já diz, irá concentrar todos os equipamentos da solução Big Data que está sendo prospectada pela CGISE.

10.3.1.4.2. Destaca-se que por meio do processo 08006.000621/2019-63 foi inciada a aquisição de uma solução de Big Data. No decorrer do processo vislumbrou-s da ARP do Pregão nº 11/2018 - CML/MD. No entanto, após a análise mais aprofundada da equipe de planejamento da contratação, optou-se por ini (08006.001367/2019-11), que ainda está sendo prospectada.

10.3.1.4.3. Tendo em vista que o projeto de Big Data é estratégico para o Ministério, e necessitará de conectividade com o restante da rede, quando implant exclusivo para a referida solução. Entretanto a equipe de planejamento do projeto de Big Data deverá incluir em seu escopo equipamentos de rede, transceivers e c compatibilidade com o LEAF BIG DATA que está sendo adquirido no presente processo.

10.3.1.4.4. Sendo assim, projeta-se que esses switches (LEAF BIG DATA) supram a necessidade da solução de Big Data, que demandam otimização de tráfego comunicação, dependendo de uma alta disponibilidade de banda e baixa latência entre os nós.

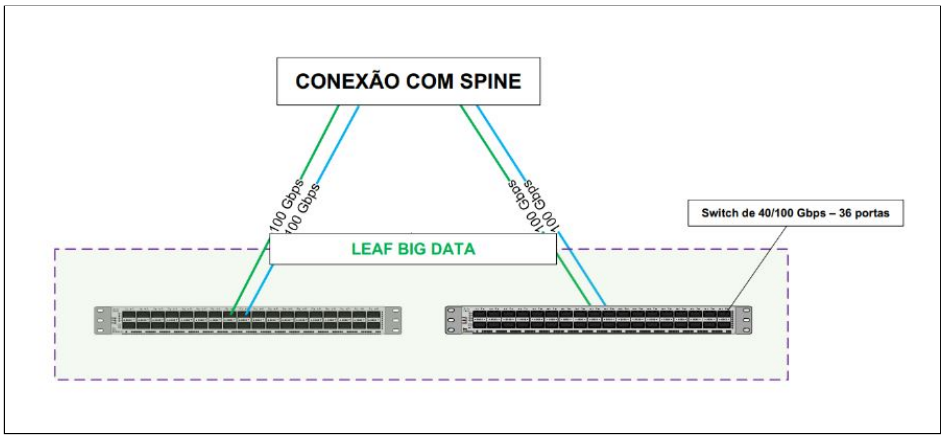

Figura 22 - LEAF BIG DATA

10.3.1.4.5. Conforme detalhado na Figura 22, a topologia LEAF BIG DATA, assim como as demais camadas LEAF, é composta por equipamentos de alta disponibilida e expansíveis.

10.3.1.4.6. Para os equipamentos da LEAF BIG DATA, há a previsão de switches com no mínimo de 36 portas 40/100 Gigabit Ethernet, cujas modularidades fora base aspectos técnicos considerados como essenciais pela área técnica responsável, assim como características de expansibilidade para uso estimado de 05 (cinco)

10.3.1.4.7. Cabe frisar que não há previsão de Switches (topo de rack) para atendimento da solução Big Data, como já exposto, pois isso ficará a cargo da equipe qu

10.3.1.4.8. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF BIG DATA:

LEAF BIG DATA	
Quantidade	**Descrição**
02	Switches de Agregação composto por, no mínimo, 36 (trinta e seis) portas 40/100 Gigabit Ethernet, em cada switch

***Tabela 04 - quantitativos* LEAF BIG DATA**

10.3.2. Ativos de redes - Detalhamento de topologias e equipamentos para o site do CICCN-DF.

10.3.2.1. Topologia SPINE-LEAF

10.3.2.1.1. Como pode ser observado na Figura 23, a topologia SPINE-LEAF CICCN-DF é semelhante a do Site Principal (Figura 19), sendo composta por equipamen LEAF (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA).

10.3.2.1.2. Destaca-se que serão detalhados, de forma meramente ilustrativa, os equipamentos com suas respectivas quantidades de portas, velocidades e cone *Fabric.*

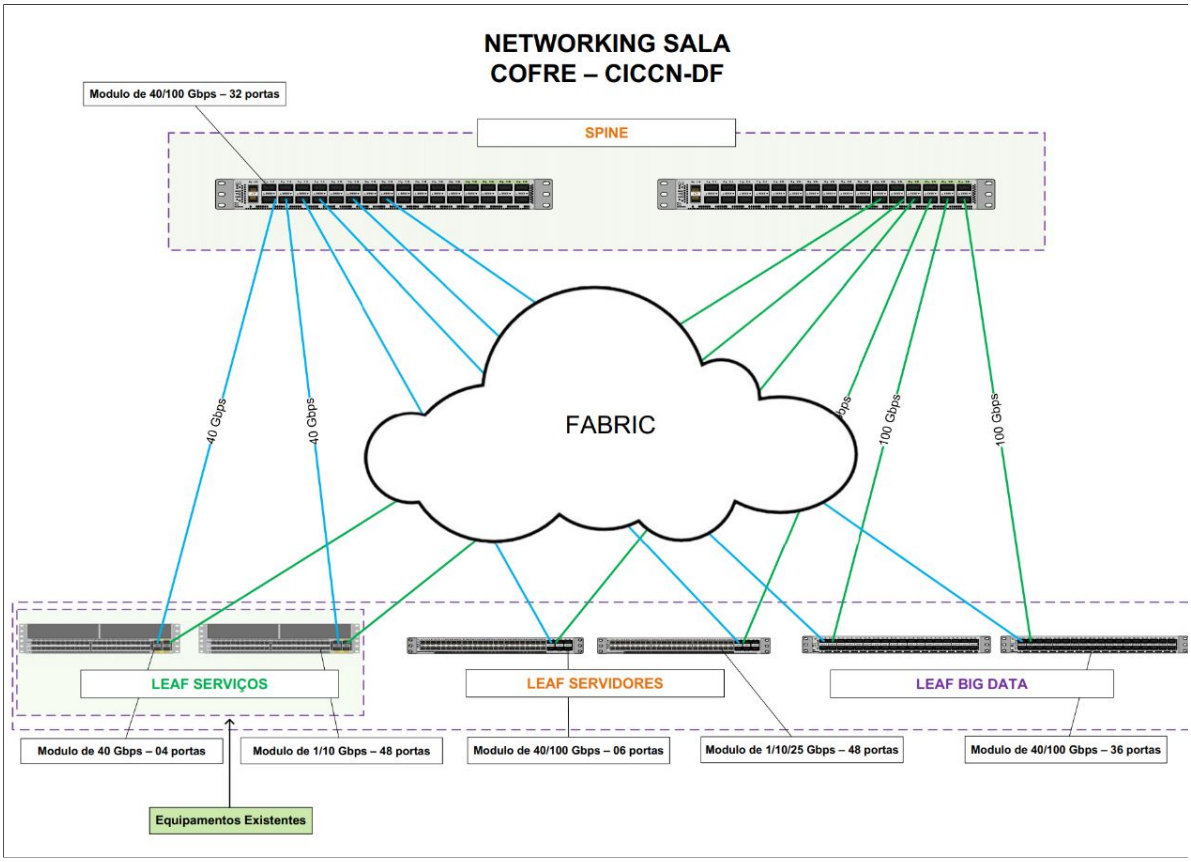

Figura 23 - SPINE LEAF CICCN-DF

10.3.2.1.3. Para os equipamentos na camada SPINE, há a previsão de switches de 32 portas 40/100 Gigabit Ethernet, cujas modularidades foram definidas to técnicos considerados como essenciais pela área técnica responsável, assim como características de escalabilidade para uso estimado de 05 (cinco) anos.

10.3.2.1.4. Os switches do SPINE, inicialmente, se conectam com os switches LEAFS (LEAF SERVIDORES e LEAF BIG DATA) a uma velocidade de conexão de 100 Gb do LEAF SERVIÇOS, será feita a conexão a uma velocidade de 40 Gbps. Para interconexão entre os switches do SPINE e os switches LEAFS estão sendo previstos Cab Gbps, com exceção do LEAF SERVIÇOS que necessitará de Cabos de Conexão Direta de 40 Gbps.

10.3.2.1.5. Por fim, da mesma forma que na definição da arquitetura de rede do núcleo central do MJSP, foi levado em consideração na definição dos quantitati cada equipamento a relação entre Spine x Leaf x servidores, de forma a minimizar o *oversubscription* na rede, inclusive considerando alguns cenários de múltipla de suas conexões, de modo que se possa escoar todo o tráfego (ou grande parte dele) entre as referidas camadas.

10.3.2.1.6. O quantitativo de equipamentos para a camada SPINE, bem como os Cabos de Conexão Direta para conexão dos LEAF, são:

CAMADA SPINE	
Quantidade	**Descrição**
02	Switches de Núcleo (Core Switch), composto por 32 (trinta e duas) portas 40/100 Gigabit Ethernet, em cada switch, para interconexão com os switches LEAFS (LEAF SERVIÇOS, LEAF SERVIDORES e LEAF BIG DATA)
08	Cabos de Conexão Direta 100 Gbps – (10 metros, mínimo)
04	Cabos de Conexão Direta 40 Gbps – (10 metros, mínimo)

Tabela 05 - quantitativos camada Spine CICCN

10.3.2.2. Topologia LEAF SERVIÇOS

10.3.2.2.1. Importante salientar, que pelo fato do Data Center do CICCN-DF estar sendo projetado para redundância do Data Center do núcleo central, além do sala técnica (pétala H do complexo da DPRF), alguns equipamentos estão sendo reduzidos ou adaptados nos LEAFES.

10.3.2.2.2. O LEAF SERVIÇOS da Sala Cofre do CICCN-DF, como pode ser observado na Figura 24, possui menor quantidade de equipamentos que o mesmo LEAF r em vista menor quantidade de serviços a serem atendidos. Inicialmente estarão conectados no referido LEAF os seguintes serviços:

a) Switch SERPRO (INFOVIA);

b) Firewalls (interno e externo);

c) Interligação com a sala técnica a pétala H do complexo da DPRF (DIOP);

10.3.2.2.3. Conforme ilustrado na Figura 24, a topologia LEAF SERVIÇOS é composta por equipamentos de alta disponibilidade de banda, baixa latência e expansíve

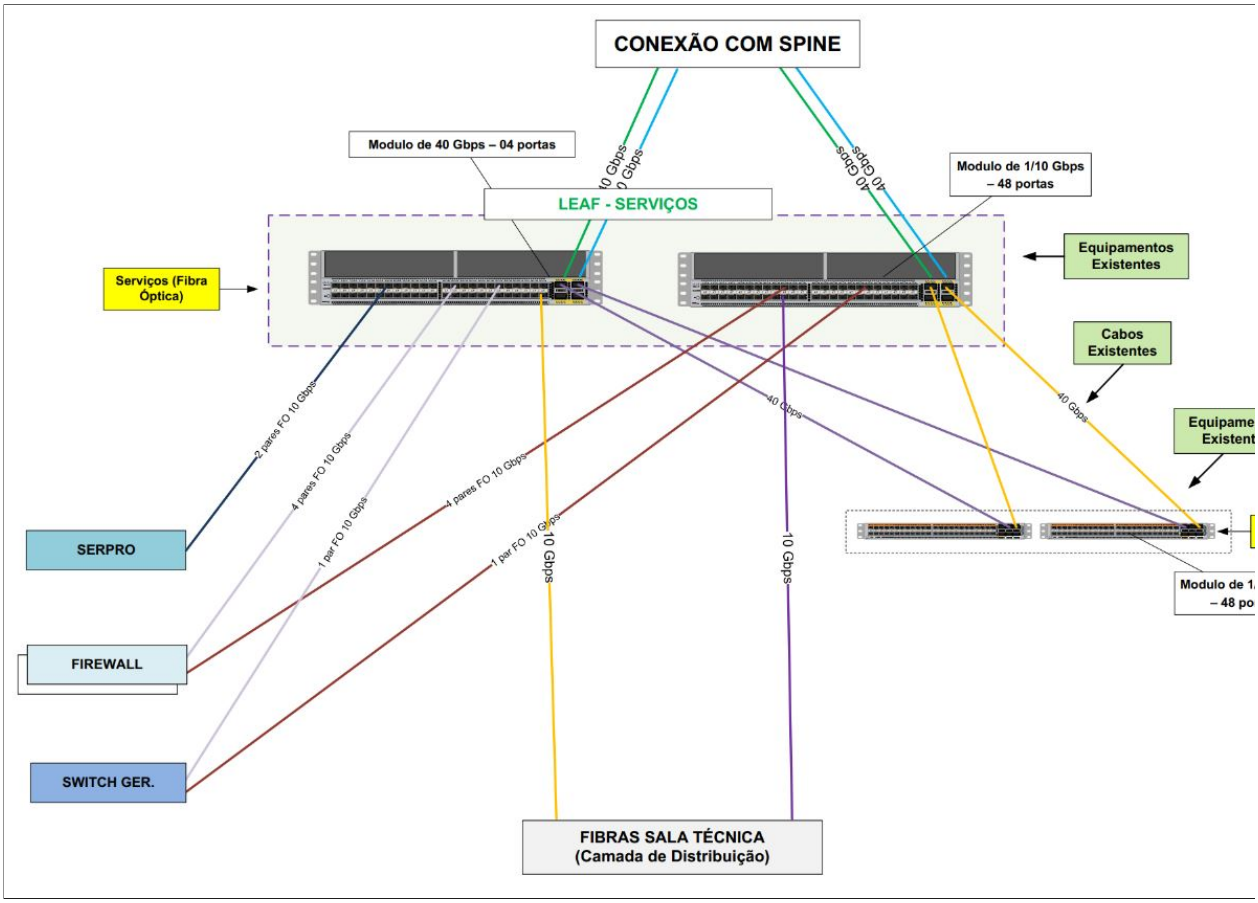

Figura 24 - LEAF SERVIÇOS CICCN-DF

10.3.2.2.4. Destaca-se que os equipamentos que compõe o LEAF SERVIÇOS do CICCN (Switches Cisco Nexus 56128P 48 portas 10G SFP Ethernet - PART NUMBER N fabric Cisco Nexus 2348 com 48 portas 1/10G, 6 portas de uplink 40G QSFP (PART NUMBER N2K-C2348TQ), equipamentos adquiridos por meio do (08006.001634/2016-15), serão reaproveitados, pois atualmente encontram-se instalados no Data Center do INFOSEG e ainda com suporte e garantia do fabricante

10.3.2.2.5. Para os dois Switches Cisco Nexus 56128P será necessária a aquisição licenciamento para que possam permitir a configuração do protocolo Virtual Ex permite a criação de segmentos de redes virtuais e sua extensão através da camada de redes (nível 3) ao encapsular quadros Ethernet em pacotes IP através propiciar a configuração do protocolo de roteamento dinâmico BGPv4 para IPv4 e IPv6.

10.3.2.2.6. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF SERVIÇOS:

LEAF SERVIÇOS	
Quantidade	**Descrição**
12	Transceivers, 10G Multimodo, LC, totalmente compatível com os switches de 48 portas
12	Cordões Óptico, 10G Multimodo, LCxLC, 10 metros, mínimo

***Tabela 06 - quantitativos* LEAF SERVIÇOS**

10.3.2.3. Topologia LEAF SERVIDORES

10.3.2.3.1. O LEAF SERVIDORES da Sala Cofre do CICCN, possui exatamente a mesma topologia (Figura 21), e equipamentos que o LEAF correspondente no Data Cer

10.3.2.3.2. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF de SERVIDORES:

LEAF SERVIDORES	
Quantidade	**Descrição**
02	Switches de Agregação, composto por, no mínimo, 48 portas, 1/10/25, com no mínimo 6 portas 40/100, em cada switch;
20	Transceivers, 10G Multimodo, LC, totalmente compatível com os switches de 48 portas
20	Cordões Óptico, 10G Multimodo, LCxLC, 10 metros, mínimo

***Tabela 07 - quantitativos* LEAF SERVIDORES**

10.3.2.4. Topologia LEAF BIG DATA

10.3.2.4.1. O LEAF BIG DATA da Sala Cofre do CICCN, possui exatamente a mesma topologia (Figura 22), e equipamentos que o LEAF correspondente no Data Center

10.3.2.4.2. Abaixo são expostos os quantitativos necessários para o dimensionamento do LEAF BIG DATA:

LEAF BIG DATA	
Quantidade	**Descrição**
02	Switches de Agregação composto por, no mínimo, 36 (trinta e seis) portas 40/100 Gigabit Ethernet, em cada switch

***Tabela 08 - quantitativos* LEAF BIG DATA**

10.3.3. Detalhamento de topologias e equipamentos de balanceamento de carga para o site do núcleo central do MJSP.

10.3.3.1. Abaixo encontram-se as topologias, meramente ilustrativas, que detalham cada conexão:

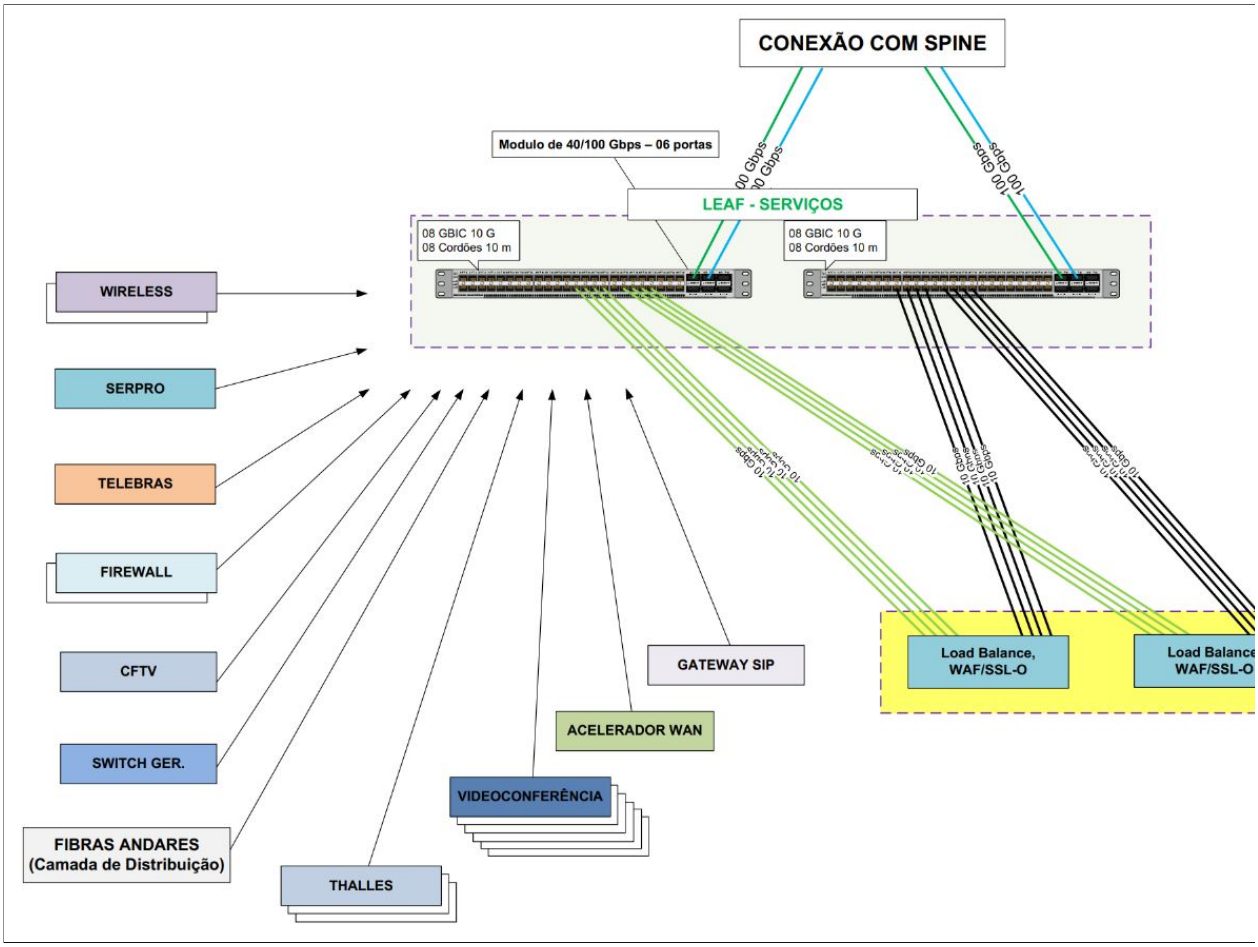

Figura 25 - Balanceamento de carga, SSL-O, WAF

10.3.3.2. Conforme visto na Figura 25, os equipamentos, uma parte da solução de balanceamento de carga e segurança serão instalados no LEAF SERVIÇOS.

10.3.3.3. Com o objetivo de suportar altas cargas de processamento (tratamento de tráfego SSL), vislumbra-se a implementação de solução física (*appliances* físicos

10.3.3.4. Para funcionalidades não triviais, que demandam pouco processamento e recursos de hardware (CPU, memória e interfaces de rede), optou-se pela imp virtualizada.

10.3.3.5. Com o objetivo de solucionar a demanda de um Web Application Firewall (Firewall de Aplicação Web - WAF), a melhor solução escolhida foi a aquisição segurança e balanceamento de carga (GSLB, WAF, DDoS, MFA/SSO), sendo dedicado para proteção efetiva da camada de aplicação.

10.3.3.6. Para realizar as conexões junto ao LEAF SERVIÇOS, serão utilizados Transceiver 10G Multimodo (LC), bem como os respectivos cabos de conexão, com no m

10.3.3.7. Será necessário também um treinamento na solução e Operação Assistida.

10.3.3.8. Abaixo são expostos os quantitativos necessários para o dimensionamento da solução de segurança e balanceamento de carga e segurança:

SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA - LEAF SERVIÇOS - NÚCLEO CENTRAL	
Quantidade	**Descrição**
02	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A
02	Serviço de instalação (Tipo A)
02	Licença para solução de segurança e balanceamento de carga - Visibilidade SSL (Appliance Físico - Tipo A)
02	Licença para solução de segurança e balanceamento de carga - ADC Avançado (Appliance Físico - Tipo A)
16	Transceiver 10G Multimodo LC
01	Treinamento (semana)
04	Operação Assistida (Semana)

Tabela 09 - quantitativos solução de balanceamento de carga e segurança - núcleo central

10.3.4 Detalhamento de topologias de balanceamento de carga e segurança para o site do CICCN-DF.

10.3.4.1. A solução de balanceamento de carga e segurança no Data Center do CICCN-DF, será implementada de forma virtualizada, tendo em vista que demand recursos de hardware (CPU, memória e interfaces de rede).

10.3.4.2. Esta solução deve ser baseada em um serviço de subscrição, com direito de uso pelo período de 12 (doze meses), podendo ser renovado até o máximo de como volume máximo contratado de *throughput* 20 (vinte) Gbps.

10.3.4.3. Além disso, é requisito fundamental que a solução ofereça suporte técnico especializado no ambiente configurado, sendo esses de forma **corretiva, preve**

10.3.4.4. Os serviços de **natureza corretiva** são aqueles efetuados com objetivo de solucionar problemas de funcionamento e disponibilidade da solução e de escla instalação, configuração, uso e atualização dos produtos;

10.3.4.5. Os serviços de **natureza preventiva** são aqueles nas quais a CONTRATADA, mediante visita mensal (on-site), realiza uma checagem da saúde e fu implementada, permitindo um diagnóstico preciso do status atual da rede;

10.3.4.6. Os serviços de **natureza evolutiva** são aqueles em que a CONTRATADA, mediante solicitação da CONTRATANTE, implementará atualizações de softw mantendo a solução em pleno funcionamento e na versão desejada pela CONTRATANTE.

10.3.4.7. Além de serviços de implementação de melhorias da solução implementada, os serviços especializados também poderão ser utilizados para:

- Desinstalação/reinstalação da solução;
- Consultoria Especializada;
- Repasse adicional de conhecimento.

10.3.4.8. Com isso, temos o serviço da Solução de Segurança e Balanceamento de carga – aaS que traz como principal benefício a flexibilidade e dinamicidade *Agreement* oferece, assim como, ao adquirir um pacote de *throughput* (20 Gbps, por exemplo), passa a poder utilizar tal capacidade na mesma medida de suas ne aprovisionadas quantas e em quaisquer tamanhos de máquinas sejam necessárias desde que somadas utilizem o *throughput* total contratado.

10.3.4.9. Com base no mencionado, temos o seguinte dimensionamento:

SOLUÇÃO DE BALANCEAMENTO DE CARGA E SEGURANÇA - CICCN-DF	
Quantidade	**Descrição**
01	Subscrição de licença para solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses
01	Serviço de instalação (Tipo B - Ambiente Virtual)

***Tabela 10 - quantitativos solução de balanceamento de carga e segurança* - CICCN-DF**

10.3.5. Tabela Detalhada dos Quantitativos

TABELA DETALHADA DOS QUANTITATIVOS		
Data Center MJSP - SEDE		
ID	**Descrição**	**Tipo**
1.	Switch SPINE 32 portas	Equipamento
2.	Serviço de instalação e configuração de Switch SPINE	Serviço
3.	Cabo de Conexão Direta 100G – (10 metros)	Equipamento
4.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIÇOS)	Equipamento
5.	Serviço de instalação e configuração de Switch LEAF - Tipo A (LEAF SERVIÇOS)	Serviço
6.	Transceiver 10G Multimodo (LC)	Equipamento
7.	Transceivers, 25G Multimodo (LC)	Equipamento
8.	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	Consumo
9.	Switch de Agregação - 24 portas (LEAF SERVIÇOS)	Equipamento
10.	Serviço de instalação e configuração de Switch de Agregação	Serviço
11.	Cabo de Conexão Direta 40G – (10 metros)	Equipamento
12.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIDORES)	Equipamento
13.	Serviço de instalação e configuração de Switch LEAF - Tipo A (LEAF SERVIDORES)	Serviço
14.	Transceiver 10G Multimodo (LC)	Equipamento
15.	Switch LEAF - Tipo B (BIG DATA)	Equipamento
16.	Serviço de instalação e configuração de Switch LEAF - Tipo B (BIG DATA)	Serviço
Sala Cofre - CICCN		
17.	Switch SPINE 32 portas	Equipamento
18.	Serviço de instalação e configuração de Switch SPINE	Serviço
19.	Cabo de Conexão Direta 100G – (10 metros)	Equipamento
20.	Cabo de Conexão Direta 40G – (10 metros)	Equipamento
21.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIÇOS)	-
22.	Serviço de instalação e configuração de Switch LEAF - Tipo A (LEAF SERVIÇOS)	Serviço
23.	Licenciamento Switches existentes (Cisco Nexus 5600 Series)	Software
24.	Transceiver 10G Multimodo (LC)	Equipamento
25.	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	Consumo
26.	Switch LEAF - Tipo A - 48 portas (LEAF SERVIDORES)	Equipamento
27.	Serviço de instalação e configuração de Switch LEAF - Tipo A (LEAF SERVIDORES)	Serviço
28.	Transceiver 10G Multimodo (LC)	Equipamento
29.	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	Consumo
30.	Switch LEAF - Tipo B (BIG DATA)	Equipamento
31.	Serviço de instalação e configuração de Switch LEAF - Tipo B (BIG DATA)	Serviço
Data Center MJSP - SEDE e Sala Cofre - CICCN		
32	Sistema de Gerenciamento de Equipamentos de Data Center	Software
33	Serviço de instalação e configuração de Sistema de Gerenciamento de Equipamentos de Data Center	Serviço
34	Solução de Controle de Acesso – Virtual Machine	Software
35	Serviço de instalação e configuração de Solução de Controle de Acesso – Virtual Machine	Serviço
36	Treinamento (semana)	Serviço
37	Operação Assistida (Semana)	Serviço
Segurança Aplicada a Redes: Aquisição de Solução de Balanceamento de Carga e Segurança		
1.	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	Equipamento
2.	Serviço de instalação do item 1 (Tipo A)	Serviço
3.	Subscrição de licença para solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	Serviço Mensal
4.	Serviço de instalação do item 3 (Tipo B - Ambiente Virtual)	Serviço
5.	Licença para solução de segurança e balanceamento de carga - Visibilidade SSL - para item 1 (Appliance Físico - Tipo A)	Software
6.	Licença para solução de segurança e balanceamento de carga - ADC Avançado - para item 1 (Appliance Físico - Tipo A)	Software
7.	Transceiver 10G Multimodo LC	Equipamento
8.	Treinamento (semana)	Serviço

9.	Operação Assistida (Semana)	Serviço

Tabela 11 - Detalhamento de quantitativos

11 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

11.1. É importante citar que o MJSP adquiriu Transceivers 10G Multimodo (LC) em licitações realizadas anteriormente (Contrato 74/2014 e Contrato 19/2016). Diante disso, a equipe técnica desta contratação realizou uma contagem minuciosa com o objetivo de verificar a possibilidade de reaproveitar alguns Transceivers neste projeto.

11.2. A quantidade de Transceivers 10G Multimodo (LC) necessária para o projeto é de 172, sendo que após a contagem, para reaproveitamento dos já adquiridos, o número total necessário foi reduzido para 70, conforme exposto no Grupo 1, item 14.

11.3. Na tabela abaixo encontram-se a descrição de todos itens e orçamento estimado da contratação:

Grupo	Item	Descrição	Unidade	Quantidade	Estimativo unitário (R$)	Estimativo total (R$)
1	1	Switch Spine	Unitário	04	238.300,00	953.200,00
	2	Serviço de instalação do item 1(Spine)	Serviço	04	25.200,00	100.800,00
	3	Switch Leaf- Tipo A	Unitário	06	164.400,00	986.400,00
	4	Serviço de instalação do item 3 (Tipo A)	Serviço	06	14.600,00	87.600,00
	5	Switch Leaf- Tipo B	Unitário	04	218.700,00	874.800,00
	6	Serviço de instalação do item 5 (Tipo B)	Serviço	04	14.600,00	58.400,00
	7	Switch de Agregação	Unitário	02	146.100,00	292.200,00
	8	Serviço de instalação do item 7 (Agregação)	Serviço	02	29.900,00	59.800,00
	9	Sistema de Gerenciamento de Equipamentos de Data Center	Unitário	01	50.100,00	50.100,00
	10	Serviço de instalação do item 9 (Sistema de Gerenciamento)	Serviço	01	14.500,00	14.500,00
	11	Solução de Controle de Acesso – Virtual Machine	Unitário	01	44.500,00	44.500,00
	12	Serviço de instalação do item 11 (Solução de Controle de Acesso)	Serviço	01	26.300,00	26.300,00
	13	Licenciamento Switches existentes	Unitário	02	28.100,00	56.200,00
	14	Transceiver 10G Multimodo (LC)	Unitário	70	2.950,00	206.500,00
	15	Transceiver 25G Multimodo (LC)	Unitário	16	4.230,00	67.680,00
	16	Cordão Óptico Duplex, 10G Multimodo,(LC/LC) (10 metros)	Unitário	62	220,00	13.640,00
	17	Cabo de Conexão Direta 100G – (10 metros)	Unitário	20	9.250,00	185.000,00
	18	Cabo de Conexão Direta 40G – (10 metros)	Unitário	08	5.270,00	42.160,00
	19	Treinamento (Semana)	Serviço	01	22.300,00	22.300,00
	20	Operação Assistida (Semana)	Serviço	04	21.600,00	86.400,00
	VALOR ESTIMADO DO GRUPO				**R$ 4.228.480,00**	
2	1	Solução de segurança e balanceamento de carga - Appliance Físico - Tipo A	Unitário	02	768.800,00	1.537.600,00
	2	Serviço de instalação do item 1 (Appliance Físico - Tipo A)	Serviço	02	73.300,00	146.600,00
	3	Licença para solução de segurança e balanceamento de carga - Visibilidade SSL - para item 1 (Appliance Físico - Tipo A)	Unitário	02	213.600,00	427.200,00
	4	Licença para solução de segurança e balanceamento de carga - ADC Avançado - para item 1 (Appliance Físico - Tipo A)	Unitário	02	384.700,00	769.400,00
	5	Transceiver 10G Multimodo (LC) - para item 1 (Appliance Físico - Tipo A)	Unitário	16	9.570,00	153.120,00
	6	Subscrição de licença para solução de segurança e balanceamento de carga - Tipo B (Ambiente Virtual) para 36 meses	Unitário	01	4.411.800,00	4.411.800,00
	7	Serviço de instalação do item 6 (Tipo B - Ambiente Virtual)	Serviço	01	59.500,00	59.500,00
	8	Treinamento (semana)	Serviço	01	24.800,00	24.800,00
	9	Operação Assistida (Semana)	Serviço	04	23.300,00	93.200,00
	VALOR ESTIMADO DO GRUPO				**R$ 7.623.220,00**	
ESTIMATIVA DO CUSTO TOTAL DA CONTRATAÇÃO *(Art. 11, Inciso IV, da IN 01/2019 SGD/ME)* *					**R$ 11.851.700,00**	

* Conforme o "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação" V 3.0 do SISP (pág. 39), o orçamento estimado informado nesse momento é preliminar. **O orçamento detalhado será realizado na confecção do Termo de Referência.**

Tabela 12 - Descrição dos itens

12 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

12.1. O presente Estudo Técnico Preliminar da Contratação evidencia que a forma de contratação que maximiza a probabilidade do alcance dos resultados pretendidos com a mitigação dos riscos e observância dos princípios da economicidade, eficácia e eficiência, seria a realização de processo de contratação de ativos novos com garantia e suporte técnico pelo período de 60 meses, para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

12.2. Como principais objetivos a serem alcançados, entre outros, podem ser citados:

- Alinhamento estratégico com as iniciativas do MJSP, garantindo a entrega de valor para que as áreas finalísticas consigam atingir seus objetivos específicos;

- Melhoria da qualidade dos serviços prestados pela DTIC a sua população cliente, com adoção das melhores práticas de mercado incorporadas à solução tecnológica que se pretende adquirir.
- Manter parque de ativos de switches com suporte, manutenção e garantia;
- Prover a infra-estrutura necessária para suportar, de forma otimizada e flexível, as demandas de informações e serviços das áreas finalísticas;
- Implantar um método de gestão e comunicação de toda a infra-estrutura de Tecnologia da Informação de forma a agilizar a sua operação;
- Suportar a demanda futura por largura de banda de rede requeridas por novas tecnologias;
- Implementar mecanismos de alta disponibilidade de comunicação de dados com otimização de banda entre os equipamentos do Data Center.

12.3. Diante do exposto, a equipe de planejamento declara ser **viável** a contratação da solução pretendida.

13 – APROVAÇÃO E ASSINATURA

13.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria SAA nº 23, de 08 de julho de 2020 (12100374), conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

Integrante Técnico	
Nome	Bruno Alves de Lima
Matrícula/SIAPE	2270209
Integrante Requisitante	
Nome	Leonardo Garcia Greco
Matrícula/SIAPE	1447905
Autoridade Máxima da Área de TIC	
Nome	Rodrigo Lange
Matrícula/SIAPE	0480055

Documento assinado eletronicamente por **Bruno Alves de Lima**, **Integrante Técnico(a)**, em 29/07/2020, às 20:10, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Leonardo Garcia Greco**, **Integrante Requisitante**, em 29/07/2020, às 21:40, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

Documento assinado eletronicamente por **Rodrigo Lange**, **Diretor(a) de Tecnologia da Informação e Comunicação**, em 30/07/2020, às 12:12, conforme o § 1º do art. 6º e art. 10 do Decreto nº 8.539/2015.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **12121843** e o código CRC **E22C3DAF**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.