Estudo Técnico Preliminar para Aquisição de Switches Departamentais

Versão 1.3

Dezembro/2023

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
27/06/2023	1.0	Revisão e atualização	Elias
29/06/2023	1.1	Revisão e atualização	Elias
05/07/2023	1.2	Revisão e atualização	Elias
07/12/2023	1.3	Revisão e atualização	Elias

INTRODUÇÃO

No âmbito desta 3ª Região, as crescentes demandas na área de Tecnologia da Informação, principalmente dos sistemas processuais eletrônicos, requerem cada vez mais ferramentas e soluções que proporcionem segurança, disponibilidade, eficiência e escalabilidade.

Existe uma cadeia de ferramentas e soluções que se combinam para prover as características acima. Neste projeto, trataremos da camada de acesso à rede de dados, que compreende, basicamente, os dispositivos de rede (como switches) que conectam os dispositivos finais (câmeras, desktop PCs, impressoras, catracas de acesso, televisores, etc) e até mesmo outros dispositivos de rede, como access-points.

Este estudo discutirá uma proposta de modernização da rede e atendimento de necessidade essencial para aquisição de switches de acesso para distribuição às unidades da SJSP e SJMS. Discutiremos a modernização do parque de switches nos edifícios da Torre Norte e Torre Sul com switches Cisco que contemplem entradas redundantes de energia (fonte de alimentação) e maior densidade de portas (switches modulares e switches empilháveis). Estenderemos a discussão para abordar a atualização do estoque de switches de acesso de forma estratégica.

1. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

1.1. Identificação das necessidades de negócio

1.1.1. Visão macro

Garantir a continuidade dos negócios através da modernização do parque de switches de acesso em unidades estratégicas e atualização do estoque desses equipamentos para atendimento às necessidades da SJSP e SJMS. Os switches da fabricante Cisco utilizados como switches de acesso da LAN da JF3R têm como função principal a comunicação dos dados dos dispositivos finais lateral e verticalmente. A continuidade dos negócios diz respeito à ampliação do estoque de switches para reposição, se necessário. A modernização diz respeito à substituição dos switches mais antigos por modelos mais novos, de forma estratégica. Os switches antigos voltarão para estoque aguardando remanejamento.

Adicionalmente, é importante que a contratação tenha previsão para suporte e garantia de todos os componentes de hardware (equipamentos) e software pela vigência

mínima de 60 meses contados a partir do aceite da solução. Essa vigência deve ser alinhada entre contratada e fabricante para que o início da vigência do suporte e garantia para os componentes registrados junto à fabricante não tenham discrepância. Tal exigência pretende evitar situação em que o início e fim de vigência no portal da fabricante encerrem-se antes dos 60 meses, causando prejuízo à Administração em caso de necessidade de suporte e/ou acionamento da garantia da fabricante.

1.1.2. Visão detalhada

Atualmente, na Justiça Federal da 3ª Região, todo (100%) o parque de switches é do fabricante Cisco, sendo que existe uma variedade de modelos de equipamentos. Do total, a instituição também mantém um estoque de switches de acesso para substituição de equipamentos defeituosos ou em caso de ampliação de fóruns e varas da instituição (aumento da quantidade de pontos de rede nas instalações).

Além disso, por se tratarem de equipamentos eletrônicos, seus componentes são suscetíveis a falhas. Equipamentos que ainda possuem garantia do fabricante podem ser substituídos mediante acionamento de uma revenda contratada. Em nossa infraestrutura, porém, existem diversos switches de modelos que já não possuem suporte do fabricante. Parte dos modelos existentes avançaram no ciclo de vida e estão perto do fim de suporte ou já foram descontinuados. A figura a seguir ilustra parte dessa situação:

By Platform

Vendor	Model	Count
Net-SNMP	linux	2
cisco	295024G	1
cisco	2960G48	149
cisco	29xx Stack	257
cisco	37xx Stack	29
cisco	65xx Virtual Switch	1
cisco	887Va	2
cisco	ASR1001X	1
cisco	Cat9300 Fixed Switch Stack	22
cisco	CatWSC2960L48PSLL	9
cisco	IGESM	2
cisco	N5KC56128P	5
cisco	N9KC92160YC	4
cisco	N9Kc9504	4
cisco	WsC2960s24tsS	11
unknown	enterprises.28557.1.332	14
unknown	enterprises.28557.1.408	2

Figura 1 – Resumo de modelos de switches em operação no parque do TRF3. Fonte: Netdisco

Os modelos destacados em amarelo e vermelho na tabela acima são modelos de switches de acesso em operação na rede. Os modelos destacados em vermelho já foram descontinuados pela Cisco e não conseguiremos substituí-los. O caso especial é o modelo 2960L, adquirido na Ata de Registro de Preços de 2018, conforme processo SEI 0033698-04.2018.4.03.8000 (contrato de 60 meses). O contrato de manutenção dessa ata deve se encerrar em 2023. O modelo 2960L foi descontinuado pela Cisco, mas uma empresa com contrato vigente ainda poderia estender a garantia destes produtos e garantir substituição por modelos mais novos, desde que a contratação ocorra até 31/10/2023. A demanda deste estudo não trata de extensão de garantias para switches de acesso, portanto, este tema não será considerado. Além disso, como abordaremos neste documento, existem modelos mais novos e relevantes para uma arquitetura futura que podem ser considerados para aquisição, em vez de

se investir na extensão de garantia desses equipamentos que já tiveram anúncio do encerramento do seu ciclo de vida.

Os equipamentos destacados em amarelo são equipamentos que ainda estão cobertos por contrato de suporte e garantia com vencimento este ano, pois foram adquiridos na mesma ata de registro de preços. Contudo, para a continuidade desse contrato, a renovação deveria ocorrer até 31/10/2023.

A Figura 1 acaba misturando modelos de switches sem suporte da Cisco (2960E, 2960S) e com suporte vincendo (2960X, adquiridos em 2018). O total de equipamentos em operação identificados como “29xxStack” pelo Netdisco é de 257 switches. Conforme pesquisa no ITOP, porém, identificamos que a instituição possui apenas 47 modelos 2960X. Destes, 43 estão em operação e 4 estão em estoque na Torre Sul, sob cuidados da RGAS. As figuras a seguir ilustram melhor o raciocínio de que:

- dos 257 switches “29xxStack”, 210 switches já são obsoletos e não possuem condições de reposição;
- dos 257 switches “29xxStack”, 47 switches são do modelo 2960X, <u>restando apenas 4 no estoque</u>

Pesquisa para objeto Dispositivo Rede — Based on your preferences, obsolete data are hidden

Adicionar novos critérios + | Dispositivo Rede contém SWC and | Management IP: qualquer and | Organização: qualquer and | Modelo: WS-C2960X-48LPS-LB, ...

Total: 43 objetos. | Novo... | Outras ações

Dispositivo Rede	Organização	Estado	Criticidade negócio	Localidade	Fabricante	Modelo	Número serial
SWCAMER05	SJSP	Produção	Baixa	Americana	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ACLM
SWCASSI04	SJSP	Produção	Baixa	Assis	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ACSJ
SWCAVAR03	SJSP	Produção	Baixa	Avaré	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AKSN
SWCBARR03_BB	SJSP	Produção	Baixa	Barretos	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ADLL
SWCBRAG04	SJSP	Produção	Baixa	Bragança Paulista	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AJUD
SWCCATA03	SJSP	Produção	Baixa	Catanduva	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2247AFFD
SWCCGRD05	SJMS	Produção	Baixa	Campo Grande - Fórum	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AKUH
SWCCGRD14	SJMS	Produção	Baixa	Campo Grande - Fórum	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244AGMU
SWCCIVE100	SJSP	Produção	Baixa	São Paulo - Fórum Cível	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ACMH
SWCCORU03	SJMS	Produção	Baixa	Corumbá	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ADGU
SWCCOXI03	SJMS	Produção	Baixa	Coxim	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AKNP
SWCFCAM81	SJSP	Produção	Baixa	Campinas - Fórum	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AJUC
SWCFDRD05	SJMS	Produção	Baixa	Dourados - Fórum	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2247AFGB
SWCFISC103	SJSP	Produção	Baixa	São Paulo - Fórum Fiscal	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AKPS
SWCFUNC04_01	SJSP	Produção	Baixa	São Paulo - Torre FUNCEF	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AMDU
SWCGARA05	SJSP	Produção	Baixa	Guaratinguetá	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ACLF
SWCGARU04	SJSP	Produção	Baixa	Guarulhos	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242AKPF
SWCITAPBB	SJSP	Produção	Baixa	Itapeva	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ABJK
SWCJDRD03	SJMS	Produção	Baixa	Dourados - JEF	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ACKS
SWCJUND20	SJSP	Produção	Baixa	Jundiaí	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ABHL
SWCMARI04	SJSP	Produção	Alta	Marília	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2247AFFF
SWCNAVI03	SJMS	Produção	Baixa	Naviraí	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ADFF
SWCOURIBB	SJSP	Produção	Baixa	Ourinhos	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2242ALBD
SWCPGOM01	SJSP	Produção	Baixa	São Paulo - Adm - Peixoto Gomide	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244AGNU
SWCPGOM04	SJSP	Produção	Baixa	São Paulo - Adm - Peixoto Gomide	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2247AFFK

Figura 2 – Switches 2960X em operação na JF3R. Fonte: ITOP

TSP2244ACKP	TRF3	Suporte	Baixa	São Paulo - TRF CPD_Torre_Sul	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ACKP
TSP2244ACTC	TRF3	Suporte	Baixa	São Paulo - TRF CPD_Torre_Sul	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ACTC
TSP2244ADTJ	TRF3	Suporte	Baixa	São Paulo - TRF CPD_Torre_Sul	Cisco Systems Inc	WS-C2960X-48LPS-LB	TSP2244ADTJ
FCW2112A3AP	TRF3	Suporte	Baixa	São Paulo - TRF CPD_Torre_Sul	Cisco Systems Inc	WS-C2960X-48LPS-LB	FCW2112A3AP

Figura 3 - Switches 2960X em estoque no TRF3. Fonte: ITOP

Em resumo, estimamos que 80% do parque de switches não poderá ser substituído pelo fabricante. Os outros 20% também se encontram sob risco de falta de cobertura de

suporte e garantia após final de 2023, pelo prazo praticamente impossível de se efetuar contrato de extensão dessa garantia até outubro de 2023, bem como de previsão orçamentária na JF3R para esta finalidade.

A ata de registro de preços do processo SEI 0033698-04.2018.4.03.8000 resultou na aquisição total de 130 switches (modelos 2960X, 2960L e 9300, conforme figura abaixo), adquiridos ao longo dos últimos 60 meses (aproximadamente). Apenas quatro (4) destes switches encontram-se disponíveis em estoque. Em consulta à seção RGAS, o total de switches em estoque novos e remanejados de outras localidades não chega a 10 equipamentos.

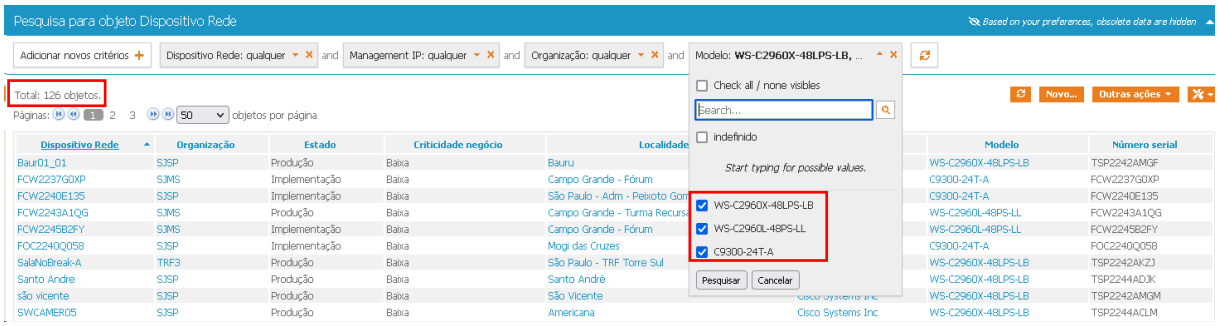

Figura 4- Amostra das aquisições de switches desde 2018 (cerca de 130)

Portanto, acreditamos que uma nova ata de registro de preços precisa ser elaborada para aquisição de, pelo menos, 150 switches de acesso novos, com suporte e garantia para os próximos 60 meses, conforme orientação legal do CJF (Res. 477/2,18, Art 3º, §1). O modelo desses switches será discutido ao longo do documento.

Cabe ainda ressaltar um caso especial na infraestrutura da Torre Sul, a rede do Centro de Controle Operacional (CCO). O CCO é uma estrutura sob responsabilidade da SSEG (Secretaria de Segurança Institucional), responsável pela segurança física dos prédios do TRF3, incluindo controle de acesso implementado por catracas, que possuem controladoras conectadas à rede de dados, câmeras de segurança e telefones com conectividade IP.

A rede de dados que implementa essas soluções é um legado que as secretarias de TI (SETI) e de segurança (SSEG) almejam abandonar, conforme processo SEI 0026683-42.2022.4.03.8000; a intenção da SETI é implementar uma única rede de dados no TRF3, capaz de atender as necessidades de acesso à rede específicas de cada secretaria. Fisicamente, os cabos e switches compartilham as infraestruturas como tubulações e salas técnicas para os switches. Mas, logicamente, a rede de dados que atende o CCO é uma rede totalmente apartada que não conversa diretamente com a rede do TRF3.

A Figura 5 abaixo ilustra o maior problema dessa rede: loops físicos acima do limite aceitável. O protocolo STP (Spanning-tree protocol) é o responsável por manter, no plano lógico, caminhos livres de loop numa rede com redundância física e vários caminhos possíveis para tráfego de pacotes. “Esse protocolo, por sua vez, utiliza parâmetros conhecidos como temporizadores (timers) para implementar o algoritmo de escolha do melhor caminho livre de loops numa rede Ethernet como a da Figura 1. Contudo, existe um parâmetro chamado “diâmetro” que é pouco observado nas implementações, mas pode ser o fator determinante para o problema. A recomendação do IEEE para redes Ethernet é que o diâmetro máximo seja 7, ou seja, um ping entre dois computadores não deve passar por mais do que 7 switches. Na Figura 5, percebemos que o diâmetro da rede do CCO é muito superior: se contarmos a quantidade de switches em cascata a partir do backbone (inclusive): são 21 switches no loop maior (quadrado) e 9 switches no loop menor. Utilizamos o switch de backbone como referência porque ele foi configurado para ser a raiz da topologia STP da rede do CCO.” (extraído do documento Relatório Visita CCO, constante no documento SEI 8885224). O “X” em vermelho desenhado na figura indica uma conexão que precisamos (RCOD) desfazer logicamente (via configuração no switch) para estabilizar a rede na época do incidente.

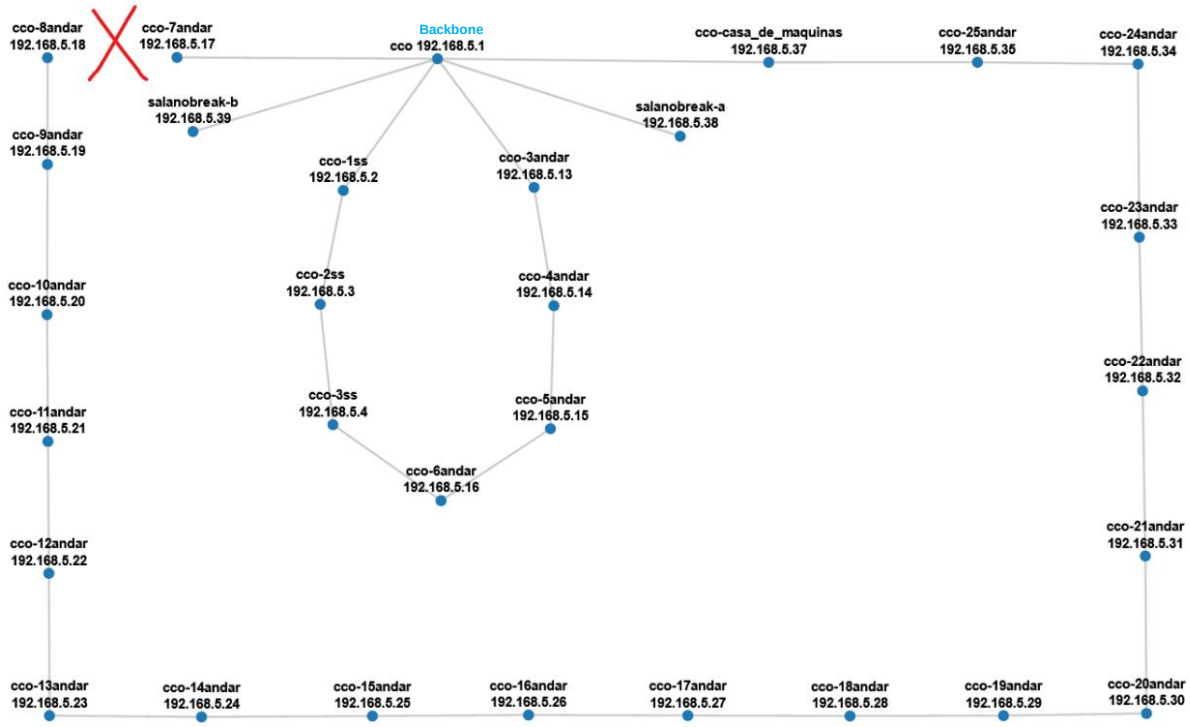

Figura 5 – Mapa de topologia física da rede de computadores do CCO (SSEG)

Portanto, este projeto também deverá levar em consideração a necessidade de absorção da rede de dados do CCO na nova infraestrutura de rede da Torre Sul. Parte desse

levantamento precisa ser considerado durante a fase de dimensionamento da solução (pontos de rede, necessidade de PoE, largura de banda necessária nas portas de acesso e uplinks). A outra parte do levantamento precisa ser melhor investigada durante o planejamento da migração da rede de dados do CCO para a rede do TRF3, particularmente as necessidades específicas de endereçamento IP e protocolos em operação nos switches.

1.2. Identificação das necessidades tecnológicas

Os equipamentos em uso atualmente estão, em sua grande maioria, perto de vencimento da garantia do fabricante ou já foram descontinuados. Além disso, todo o estoque adquirido nos últimos 5 anos foi praticamente consumido na JF3R.

O estoque atual precisa ser reforçado com novos equipamentos e remanejamento dos equipamentos existentes ainda em funcionamento.

Além disso, os prédios da Torre Norte e Torre Sul precisam de switches com maior densidade de portas e redundância de fonte de energia, tendo em vista a alta demanda de pontos de rede nesses prédios e a criticidade dos trabalhos desenvolvidos na sede da JF3R.

As duas demandas (modernização do parque de Sede e recomposição do estoque) podem ser atendidas de forma estratégica e com benefícios para a Administração nos quesitos financeiros, operacionais e experiência para o usuário. Analisaremos essas demandas a seguir.

1.2.1. Modernização do parque na sede do TRF3 (Torres Sul e Norte)

A proposta para a sede do TRF3 é substituir os switches de acesso existentes, da linha Catalyst, por outros switches com maior densidade de portas. Em geral, os switches de acesso existentes são modelos 2960-G, 2960-S, 2960-X ou 2960-L, todos da família Catalyst, trabalhando de forma independente. Esses switches possuem 48 portas UTP para conectar dispositivos finais e, geralmente, 2 portas de fibra para agregação em switches de distribuição da família Nexus linha 9000.

O presente estudo contou com ajuda de um parceiro indicado pela Cisco (empresa NTT) para desenho de cenários e estimativa de preços.

Em nossa pesquisa, consultamos as melhores opções dentre as famílias Nexus e Catalyst. De forma resumida, a família Nexus é mais indicada para switches de acesso na área de datacenter, principalmente para conexão de servidores. Ambientes de datacenter (redes de Storage Area Network – SAN) necessitam de alta performance, privilegiando tráfego entre aplicações e bancos de dados. Esse tipo de tráfego é comercialmente denominado de tráfego lateral ou tráfego leste-oeste.

A família Catalyst, por outro lado, possui foco em tráfego denominado vertical ou norte-sul[1]. Esse tipo de comunicação diz respeito ao tráfego de aplicações para fora da rede local, geralmente tráfego com a Internet. Obviamente, os dispositivos finais também necessitam acessar serviços na rede de datacenter, mas, com o passar do tempo, o acesso a aplicações em nuvem cresceu demasiadamente, reforçando o comportamento de maior consumo de dados na Internet. Esse comportamento engloba, inclusive, aplicações como correio eletrônico e serviços de diretório, aplicações historicamente acessíveis na rede local das organizações e que atualmente são acessadas na modalidade em nuvem.

Nesse sentido, o projeto atual considerou a família Catalyst para o projeto. A decisão não é apenas conceitual (se a rede é ou não no datacenter dos servidores), mas de arquitetura, propósito e estratégias para médio-longo prazo. A opção pela família Catalyst considerou, principalmente:

- necessidade de conexão de usuários e dispositivos de acesso, como os dispositivos IoT (Internet of Things , que incluem ar condicionado, PLC nos elevadores), impressora, desktop PCs. Esses dispositivos, geralmente, necessitam de mecanismos de controle na rede, como microsegmentação, controle de banda, QoS;

- pré-existência de switches Catalyst na infraestrutura, em especial a linha 9300;

- manter um gerenciamento centralizado (possibilidade de utilização do Cisco DNA Center) que possibilite uniformização de IOS do parque. A antiga linha IOS (sistema operacional dos switches) está sendo substituída pela linha IOS-XE nos equipamentos atuais da Cisco. Esse sistema operacional é diferente do sistema NX-OS, que está presente em switches Nexus.

Em reunião com a diretoria ocorrida em 04/05/2023, a NTT mostrou um comparativo de duas soluções e preços de switches do tipo chassi (modulares) e empilháveis (stack).

No aspecto financeiro, a solução mais adequada é a solução de switches empilháveis. Os modelos equivalentes, para fins de comparação, são a linha Catalyst 9400 (chassi) e a linha Catalyst 9300 (stack). Abaixo temos comparativo de preço unitário entre esses dois produtos numa estimativa para atender o 22º. andar da Torre Norte:

Item	Mfr Part #	Description	Qty	Unit Price	Total Price
	22 ANDARComments:				
10	C9300-48UXM-A	Catalyst 9300 48-port(12 mGig, 36 2.5Gbps) Network Advantage	3	R$ 104,533.43	R$ 313,600.29
10.0.1	CON-SSSNT-C93A048M	SOLN SUPP 8X5XNBD Catalyst 9300 48-port(12 mGig36 2.5Gbps	15	R$ 6,427.83	R$ 96,417.45
10.10.1	CON-SSTCM-C93A48	SOLN SUPP SW SUBC9300 DNA Advantage	15	R$ 910.69	R$ 13,660.35
11	C9300-NM-8X=	Catalyst 9300 8 x 10GE Network Module, spare	2	R$ 11,218.05	R$ 22,436.10
12	SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	4	R$ 2,934.01	R$ 11,736.04
Product					R$ 347,772.43
OEM Maintenance					R$ 110,077.80
SECTION GRAND TOTAL (22 ANDAR)					R$ 457,850.23
Item	Mfr Part #	Description	Qty	Unit Price	Total Price
	C9407 - SUBSTITUIÇÃO DO 22 ANDAR / N9K-C92160YCComments:				
13	C9407R	Cisco Catalyst 9400 Series 7 slot chassis	1	R$ 785,753.06	R$ 785,753.06
13.8.1	CON-SSTCM-C94A	SOLN SUPP SW SUBCisco Catalyst 9400	5	R$ 3,101.28	R$ 15,506.40
14	CON-SSSNT-C9407R	SOLN SUPP 8X5XNBD Cisco Catalyst 9400	5	R$ 21,508.90	R$ 107,544.50
15	SFP-10G-SR-S=	10GBASE-SR SFP Module, Enterprise-Class	16	R$ 2,934.01	R$ 46,944.16
16	SFP-10G-LR-S=	10GBASE-LR SFP Module, Enterprise-Class	4	R$ 8,382.85	R$ 33,531.40
Product					R$ 866,228.62
OEM Maintenance					R$ 123,050.90
SECTION GRAND TOTAL					R$ 989,279.52

Figura 6 – Comparativo de preços switches Catalyst 9300 (Stack) x 9400 (Chassi). Fonte: NTT

Destacamos em azul os preços unitário e total para aquisição de uma solução para conectividade do 22º. Andar da Torre Norte usando a linha Catalyst 9300 (switches empilháveis). Em verde, temos a mesma informação para a linha Catalyst 9400 (switch de chassi). Visivelmente, a linha C9300 é mais econômica para a Administração com o mesmo benefício técnico.

Em termos *operacionais*, ambas as linhas funcionam com IOS-XE, portanto, trata-se do mesmo sistema operacional para os switches. Fisicamente, há diferenças entre os equipamentos. Podemos destacar as mais características de cada modelo: no modelo 9400, será necessário instalar módulos (lâminas) no switch, sendo que para cada conjunto de módulos de portas de dados, precisaremos de pelo menos um módulo conhecido como supervisor (supervisora). Já no modelo 9300, a instalação física compreende instalação de cabos stackwise (dados) e stackpower (energia) para, respectivamente, empilhamento e redundância de fonte de energia.

Por fim, com a modernização dos switches nos prédios da Torre Norte e Sul, os switches existentes deixarão de ser utilizados nesses prédios e, por estarem em funcionais, serão reconduzidos ao estoque de switches, conforme exposto no subitem 1.1.1 e discutido em detalhes no subitem 1.2.2 a seguir.

Além disso, ambos os switches são compatíveis com a tecnologia Cisco DNA Center. Essa tecnologia apresenta uma modernização da infraestrutura que pode trazer diversos benefícios à operação da RCOD e à experiência do usuário final. Isso inclui um monitoramento e gerência de portas em switches de acesso em alto nível de detalhe, com

possibilidade de programação de ações para resoluções de problemas. Todo o processamento de protocolos como STP (Spanning-tree protocol) deixa de ser realizado no equipamento e ocorre na gerência centralizada. Além disso toda a configuração do switch passa a ser feita de forma automática pela controladora (conhecida como DNA Center). O processo de implantação de um switch ficará muito semelhante ao que ocorre com os access points da Cisco atualmente: basta conectar o equipamento à rede, para obtenção de um endereço IP válido na rede local e comunicação com a controladora. Com a comunicação estabelecida, toda a lógica de controle (plano de controle) do equipamento será obtida da controladora, dispensando atuação manual da RCOD. A própria controladora fará o papel de calcular os caminhos redundantes e evitar loops na rede. Esse comportamento trará benefícios para a operação da RCOD e para a experiência do usuário remoto responsável pelo CPD na localidade, que passará a se preocupar apenas com a conexão física do equipamento e menos com a espera da configuração e envio de um switch do TRF3 até a localidade. Detalharemos esse caso mais adiante.

1.2.2. Ampliação do estoque de switches

Na última aquisição de switches, foram consumidos cerca de 130 switches (modelos Catalyst 2960X, 2960L e 9300) ao longo dos 60 meses de vigência contratual. Atualmente, restam apenas 4 desses switches (modelo 2960X). Com a modernização discutida no subitem 1.2.1, os switches de acesso em operação serão removidos dos racks e retornarão ao estoque do TRF3, sob cuidados da RGAS. Estimamos um número perto de 120 switches que serão substituídos tanto na Torre Norte quanto na Torre Sul.

Além disso, a diretoria estimou que um número de 100 switches novos seria o suficiente para reforçar o estoque, considerando que haverá remanejamento de equipamentos em operação na sede após a substituição.

Dentre as opções para switches em estoque, existem dois modelos candidatos que sugerimos para aquisição, ambos da família Catalyst: C9200 e C9300.

Em reunião entre a NTT, RCOD, DRED, UARI e SETI, ocorrida em 04/05/2023, a diretoria optou pela linha C9200 por uma questão de custos. A linha C9200 não suporta a tecnologia de stackpower (redundância de energia), apenas stackwise (redundância de dados). Esses switches devem ser, prioritariamente, posicionados na borda da rede de unidades remotas, substituindo switches existentes e mais antigos nessa função (linha 3750, provavelmente).

A Figura 4 (ver item 2 – Situação Atual) exibe um modelo da linha Catalyst 9300 (C9300-24-T) compatível com a tecnologia SD-Access, é necessário ressaltar a vida útil desses

equipamentos. A Figura 7 foi obtida com ajuda da NTT em reunião ocorrida em 26-05-2023. A linha 7 da planilha informa que os switches 9300 em operação atualmente terão sua garantia encerrada em 22/janeiro/2024. A partir dessa data, porém, eles continuarão operacionais, mas perderão o benefício da integração com a tecnologia SD-Access (automatização de configuração, por exemplo).

	A	B	C	D	E	F
1	Subscription and/or Service Contra					
2						
3	CCO USER ID	00u61re7ijivwc5vb5d7				
4	Date	19/05/2023				
5						
6	Product /Offer Name	Description	Start Date	End Date	PAK/Serial Number	Major/Minor
7	C9300-24T-A	Catalyst 9300 24-port data only, Network Advantage		22-jan-2024	FOC2237Q0VH	Major
8	S9300UK9-168	^UNIVERSAL		30-set-2023		Minor
9	CAB-TA-NA	North America AC Type A Power Cable		22-jan-2024		Minor
10	NM-BLANK-T1	Cisco Catalyst Type 1 Network Module Blank		22-jan-2024		Minor
11	PWR-C1-BLANK	Config 1 Power Supply Blank		22-jan-2024		Minor
12	PWR-C1-350WAC	350W AC Config 1 Power Supply		22-jan-2024	ART2238FLEF	Minor
13	DISTI-STOCKING	OPT OUT SKU FOR DISTI STOCKING USE ONLY		22-jan-2024		Minor
14	C9300-NW-A-24	C9300 Network Advantage, 24-port license		22-jan-2024		Minor
15	C9300-24T-A	Catalyst 9300 24-port data only, Network Advantage		22-jan-2024	FCW2237G0XP	Major
16	S9300UK9-168	^UNIVERSAL		30-set-2023		Minor
17	PWR-C1-BLANK	Config 1 Power Supply Blank		22-jan-2024		Minor
18	DISTI-STOCKING	OPT OUT SKU FOR DISTI STOCKING USE ONLY		22-jan-2024		Minor
19	PWR-C1-350WAC	350W AC Config 1 Power Supply		22-jan-2024	ART2238FLEE	Minor
20	CAB-TA-NA	North America AC Type A Power Cable		22-jan-2024		Minor
21	C9300-NW-A-24	C9300 Network Advantage, 24-port license		22-jan-2024		Minor
22	NM-BLANK-T1	Cisco Catalyst Type 1 Network Module Blank		22-jan-2024		Minor
23	C9300-24T-A	Catalyst 9300 24-port data only, Network Advantage		22-jan-2024	FCW2237C1BD	Major
24	DISTI-STOCKING	OPT OUT SKU FOR DISTI STOCKING USE ONLY		22-jan-2024		Minor
25	NM-BLANK-T1	Cisco Catalyst Type 1 Network Module Blank		22-jan-2024		Minor

LineDetails

Figura 7- Vencimento da cobertura da garantia dos switches 930-24 portas em operação na JS3R

Portanto, pensando na continuidade do negócio, ressaltamos duas considerações sobre esses switches existentes:

1. A Administração precisa considerar substituí-los por outros 9200 (capacidades equivalentes), pensando em aproveitar melhor o investimento previsto para os próximos 5 anos;
2. A Administração precisa considerar possibilidade de um plano de extensão de garantia para esses switches de acesso após 22/01/2024, por mais 5 anos, para preservar o investimento atual na arquitetura SD-Access. Essa alternativa pode ser comparada com a estratégia de aquisição de modelos mais novos de switches para decisão da opção mais vantajosa.

Os itens 1 e 2 acima poderiam ser planejados considerando a evolução da rede para uma plataforma de automatização como a Cisco SD-Access, discutida mais adiante. O intuito dessa sugestão é evitar que ao final de 5 anos tenhamos switches operacionais sem licença válida para funcionar em conjunto com a tecnologia SD-Access.

Para os demais andares nas unidades remotas da SJSP e SJMS, haverá ainda o estoque ampliado conforme discutido no subitem 1.2.1.

1.2.3. Necessidades da rede de dados no CCO

Em conversar com o servidor Sr. Umberto (RINA) e investigação nos switches de acesso, identificamos que existem 2 câmeras IP do tipo PTZ em operação, ambas sendo eletricamente energizadas pelo switch através da tecnologia PoE. De forma semelhante,

identificamos que existem quatro (4) telefones IP do tipo PoE para emergências conectados à rede. O Sr. Umberto informou que a SSEG comprou cerca de 180 câmeras que devem ser instaladas em 2023, a maioria do tipo PoE. Essas necessidades são relevantes para o dimensionamento da solução.

Os servidores da SSEG também utilizam softwares específicos em estações de trabalho para acesso a câmeras e sistemas de catracas. Essas necessidades deverão ser mapeadas em maior detalhe na fase de implantação do subitem 1.2.1, para garantir uma transição sem indisponibilidade de serviços aos usuários.

À medida que a etapa de modernização da rede avançar, os switches em desuso poderão ser movidos para o estoque de switches, conforme trata o subitem 1.2.2.

1.2.4. Cisco DNA + ISE

A visão sobre arquitetura de redes evolui nos últimos anos com a concepção de redes definidas por software (ou SDN, na sigla em inglês). Para switches de acesso, a Cisco implementa essa visão inovadora por meio de uma tecnologia conhecida como SD-Access (Software Defined-Access). Nessa visão, a rede física passa a ser responsável pelo tráfego de dados, enquanto a inteligência sobre dados e operação dos switches é realizada por outro dispositivo, conhecido nessa solução como DNA Center.

A plataforma DNA Center implementa a estrutura necessária de comunicação com os dispositivos físicos (switches de acesso). Através dessa comunicação, os switches recebem da controladora SD-Access (DNA Center) toda a configuração necessária para sua operação, incluindo perfis de acesso à rede, portas ativas e inativas, caminhos livres de loop. Essa última aplicação é uma das maiores mudanças dessa nova solução, pois significa que o protocolo STP (protocolo de camada 2) não será mais executado pelo harware e software dos switches; todo o processamento irá ocorrer no DNA Center. Outros protocolos, como OSPF, EIGRP (protocolos de camada 3) também serão processados no DNA Center. A figura a seguir resume a mudança de paradigma da arquitetura de redes de computadores corporativas tradicionais para a arquitetura com SD-Access.

Figura 8 – Comparativo macro de redes tradicionais e redes com arquitetura SD Access. Fonte: NTT

Conforme adiantado no subitem 3.3.2, uma das grandes vantagens que essa nova abordagem pode trazer para o ambiente de redes do TRF3 é a possibilidade de configuração automatizada de switches. Atualmente, a RCOD é a responsável por configurar switches de acesso Cisco, de forma 100% manual, para envio preparado ao destino. Se esse switch necessitar ser reconfigurado após o envio, o equipamento deverá ser conectado via cabo console a um PC ou notebook conectado à rede, acessível remotamente para a RCOD realizar a reconfiguração. Com a automatização da configuração, todo esse processo seria simplificado:

- a configuração seria pré-criada dentro do DNA Center;
- dentro do DNA Center, teríamos perfis de configuração por tipo de dispositivos (ex.: switch de acesso empilhável, swtich de acesso de andar, switch de acesso de borda/backbone);
- o switch de acesso necessitaria apenas de acesso à rede para estabelecer comunicação com o DNA Center e receber as configurações de forma automatizada.

Esse modelo de implantação existe na rede wireless (WLAN) do TRF3. O mesmo access-point (AP) que é usado na Torre Sul pode ser remanejado para uma localidade em Mato Grosso do Sul. Assim que o AP obtém um endereço IP, ele se conecta via túnel com a controladora Wireless e recebe toda a configuração necessária. O mesmo procedimento pode ser implementado para switches compatíveis com a tecnologia SD-Access. A vantagem disso

seria ainda maior nas localidades remotas, principalmente em locais com maior dificuldade de acesso (como Corumbá, em Mato Grosso do Sul). Na eventualidade de um switch defeituoso, bastaria que o CPD local conectasse um switch compatível com SD-Access para ser reconfigurado de forma automática e se tornar pronto para uso.

A tecnologia SD-Access apresenta maior benefício quando a rede possui switches compatíveis com SD-Access. Contudo, essa não é a realidade de curto prazo do TRF3, em que a grande maioria dos switches do parque não modelos sem compatibilidade com SD-Access. Mesmo assim, é possível implantar switches gerenciados pelo DNA Center para operação em conjunto com os switches não compatíveis. Estes últimos, porém, funcionarão da forma convencional, sem o benefício da automatização. A figura a seguir ilustra um pouco desse cenário; nós intermediários ("underlay") representam switches não gerenciados pela solução DNA Center e nós tipo edge do fabric representam switches gerenciados pela solução DNA Center.

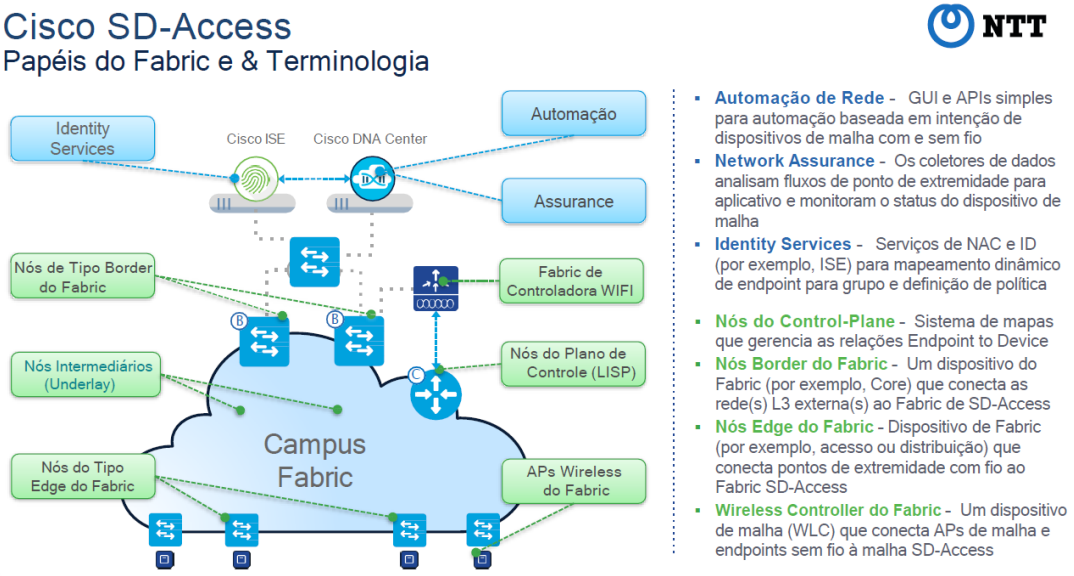

Figura 9 – Resumo de uma rede com arquitetura SD Access completa (arquitetura "Fabric")

Adicionalmente, a figura acima mostra outras vantagens da solução SD-Access. Com ela, é possível termos uma solução integrade de NAC (Network Access Control) e Wireless, todas com o benefício da automatização, segmentação da rede (por usuário, nível de acesso, localização) e identificação do dispositivo de usuário. Esses itens são integrados, porém, não necessitam ser adquiridos numa única aquisição. Contudo, como área técnica, é interessante termos uma visão de médio-longo prazo para a arquitetura de rede e planejarmos a evolução da rede para os próximos anos, em conjunto as priorizações da diretoria e disponibilidade de orçamento.

Adicionalmente, existem outros níveis de automatização necessários à organização, principalmente tendo em vista o ataque ransomware efetuado contra a rede do TRF3 em abril/2022.

Como investimento mínimo recomendável, nos parece mais vantajosa a aquisição da solução de DNA Center em conjunto com Cisco ISE, pensando na modernização da rede discutida anteriormente e preparando o ambiente de redes para implantação de uma solução de NAC da Cisco, tendo em vista que a solução DNA Center é proprietária da Cisco.

Com a solução ISE, da Cisco, poderíamos implementar um controle maior de acesso físico à rede, identificando usuários (quem), dispositivos (o quê) e tempo (quando). A granularidade de controle de acesso que a solução permite implementar na rede depende da compatibilidade dos switches de acesso, principalmente. Além disso, a solução ISE também provê interface para comunicação com outros fornecedores para troca de informações a fim de enriquecer a análise do que está ocorrendo na rede.

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

Levando em consideração que a administração necessita de equipamentos (switches) com fontes redundantes, para um melhor aproveitamento da redundância da solução, identificamos como requisito revisão das salas técnicas onde esses switches serão instalados, providenciando réguas elétricas distintas se possível, para que cada fonte seja ligada em régua elétrica distinta. Essa demanda deve ser direcionada à administração e engenharia de cada unidade (TRF3/SJSP/SJMS).

Adicionalmente, é requisito que as fibras óticas de interligação entre os equipamentos estejam em perfeito estado de funcionamento. Essa demanda deve ser encaminhada ao setor responsável pela estrutura de cabeamento de cada unidade (TRF3/SJSP/SJMS).

1.3.1. Adequação à realidade orçamentária

Durante o planejamento da solução, com base na estimativa de preços inicial fornecida pela NTT para os modelos das linhas de switches 9200 e 9300 sugeridos pela empresa, a diretoria observou a impossibilidade de execução dos preços da ata, em valor muito superior ao orçamento estimado, considerando tanto o preço unitário habitualmente pago por aquisições semelhantes no TRF3 nos últimos anos quanto o custo total com base no quantitativo estimado no subitem 2.1, descrito adiante neste mesmo documento.

Com base nisso, a empresa (NTT) e fabricante (Cisco) foram convocadas para discutir a proposta e entender o que poderia ser ajustado. A diretoria encontrou um edital[2] (PE 82/2022) da Câmara dos Deputados com demandas similares à do TRF3, ou seja, switches

com maiores densidades de portas, redundância de fontes, com solução de gerência centralizada e capacidade de automatização de tarefas. Para aquela licitação, houve disputa acirrada de preços entre fabricantes distintos (Cisco e Huawei), vencendo, por fim, a representante Cisco. Na proposta da empresa, encontramos o modelo 9200-L (48 portas, POE+) que, após negociações durante o pregão, conseguiu ser vendido por cerca de 25 mil reais (preço unitário). Na estimativa de preços da NTT, os preços unitários foram de 87 mil reais para o modelo 9200-48PXG-A e cerca de 100 mil reais para modelos 9300-UXM-A (24 e 48 portas).

Após diversas conversas técnicas e comerciais entre RCOD, DRED, UARI, NTT e Cisco, o projeto original foi redesenhado da seguinte forma:

- o modelo de switch escolhido para a solução, incluindo sites da Torre Norte, Torre Sul (incluindo absorção da rede do CCO/SSEG), SJSP e SJMS foi o Catalyst **9200L-48P-4X-A**. Este modelo atende às necessidades da seguinte forma:
  - permite alta densidade de portas através da técnica de empilhamento (stackwise);
  - suporte fonte redundante;
  - possui 48 portas UTP de 1 Gbps, todas com PoE habilitado;
  - possui 4 portas de uplink com capacidade de 1Gbps ou 10Gbps, a depender do transceiver (GBIC) instalado;
  - está habilitado para SD-Access com a licença Network Advantage;
- a renovação de licença de subscrição, bem como suporte e garantia dos switches 9300-24-T adquiridos na ata de 2018 também será mantida para estender o benefício do investimento com a nova arquitetura SD-Acess, conforme apontado no subitem 1.2.2;
- os appliances Cisco DNA Center serão adquiridos na modalidade appliance físico;
- os appliances Cisco ISE serão adquiridos na modalidade appliance virtual;
- treinamentos oficiais de Cisco DNA Center e Cisco ISE serão mantidos para a equipe RCOD;
- suporte, garantia e licenciamento de toda a solução por 60 meses;
- iremos alterar a estratégia de abastecimento dos switches nas seções judiciárias em SP e MS: em vez de redistribuir os switches da Sede conforme intenção original discutida no subitem 1.2.2, iremos adquirir um quantitativo maior de switches 9200L-48P-4X-A, compatíveis com as soluções DNA e ISE;
- serviço de instalação e configuração da solução também permanece no escopo;
- a diretoria optou por descartar os investimentos:
  - tecnologia de stackpower (redundância fonte e compartilhamento de energia via cabo de força) para switches da Torre Norte e Torre Sul;
  - requisitos de alta potência de alimentação dos switches para dispositivos PoE, como câmeras e access-points. As câmeras PoE devem ser bem suportadas pela

fonte existente no modelo selecionado e, em caso de insuficiência de energia, a ata de registro de preços vai prever um quantitativo de fontes adicionais para aquisição, além do fato de ser possível remanejar pontos de rede entre switches da pilha para balancear o consumo de energia por switch. As demandas relacionadas a access-points (portas mGig e UPOE) serão tratadas no futuro, no desenho do projeto de atualização da rede wifi da JF3R.

2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

2.1. Estimativa do desenho original

O quantitativo estimado observou o seguinte escopo inicial:

1. quatro (4) andares ocupados prédio Torre Norte (andares 11º., 13º. 19º. E 22º.);

2. 24 andares na Torre Sul, do 1º. ao 24º. O 25º. andar será atendido pela sala técnica do 24º. andar;

3. três (3) andares de subsolo na Torre Sul

4. solicitação da diretoria de atender a necessidade de absorção da rede do CCO para a rede do TRF3 (afeta apenas o edifício Torre Sul);

5. localidades da SJSP e SJMS que não receberam um switch 9300 da última aquisição de switches em 2018, sendo 23 localidades na SJSP e 11 localidades na SJMS;

6. quantidade de switches em uso atualmente nas Torres Norte e Sul.

Para a Torre Sul, estimamos uma média de 4 switches por andar, já que existem andares 1 switch a menos ou a mais. Dessa forma, considerando a escolha por switches stack (9300), temos um total de 96 switches (24 x 4) estimados para atender os 24 andares. Adicionalmente, teremos uma média de 2 switches por andar nos 3 subsolos da Torre Sul, num total de 6 switches. Ao todo, para atender as necessidades da Torre Sul, estimamos um total de 104 switches 9300 fazendo uso de stackwise e, quando possível, da tecnologia stackpower também.

Atualmente temos a seguinte distribuição por andar no edifício Torre Norte:

seis (6) switches de acesso no 11º. andar;

quatro (4) switches de acesso no 13º andar;

sete (7) switches de acesso no 19º andar;

dois (2) switches de acesso no 22º andar.

Considerando um provisionamento para aumento da demanda futura, acrescentamos 1 switch por andar na Torre Norte. Sendo assim, sugerimos aquisição e distribuição de 23 switches 9300 (stackwise + stackpower) nesse edifício da seguinte forma:

sete (7) switches de acesso 9300 empilhados no 11º. andar;

cinco (5) switches de acesso 9300 empilhados no 13º. andar;

oito (8) switches de acesso 9300 empilhados no 19º. andar;

três (3) switches de acesso 9300 empilhados no 22º. Andar.

Para conexão dos switches em pilhas nas Torres Norte e Sul, também deverão ser adquiridos cabos stackwise, fontes de energia e cabos stackpower. Para cada switch, deverá ser comprado, no mínimo, 1 cabo stackwise, 1 módulo stackwise, 1 fonte de energia, 1 cabo de stackpowe, além de *2 (dois) módulos* SFP de 10Gbps e *2 (dois) transceivers* de 10Gbps *para cada pilha de switches* interligada ao switch de distribuição. Para redundância das fontes na pilha, alguns dos switches precisarão ter 2 fontes de energia e 2 cabos de força para ligação cruzadas do módulo de energia entre dois switches (a fonte de 1 switch ligada na fonte de outro switch). Portanto, estimamos um mínimo de 104 cabos stackwise, 104 módulos stackwise, 104 fontes de energia, 104 cabos stackpower e 54 módulos SFP de 10 Gbps (27 andares/subsolo x 2 SFP) para a Torre Sul. Para a Torre Norte, o mínimo estimado seria de 8 módulos SFP 10 Gbps (4 andares x 2 SFP) e 96 unidades para os demais itens.

Ainda, necessitaremos de uma (1) solução licenciada do produto Cisco DNA Center e uma (1) solução licenciada do produto Cisco ISE.

Por fim, será necessário adquirir um mínimo de 34 switches 9200 para atender 23 localidades da SJSP que ainda não possuem um switch habilitado para Cisco DNA. Para a SJMS, o quantitativo será de 11 switches com essa mesma finalidade. Porém, com base na aquisição da ata de registro de preços de 2018, a área técnica e diretoria entendem que o quantitativo de entre 100 e 150 switches deva ser um número mínimo razoável para o prazo dos próximos 5 anos. Dessa forma, é possível planejar aquisição de um número entre 34 e 150 switches 9200.

Outro fator relevante para o quantitativo é o prazo de entrega. Segundo a NTT, a estimativa de prazo de entrega da Cisco é a seguinte (previsão obtida em junho/2023):

- **Switch C9300:**
  - Catalyst Switch tipo Fixo, modelo C9300-48UXM-A (sem stackwise, sem stackpower, sem o módulo de Uplink) – aprox. 45 dias para fabricar + 30 dias para chegar no TRF3
  - Catalyst Switch tipo Fixo, modelo C9300-24UX-A (sem stackwise, sem stackpower, sem o módulo de Uplink) – aprox. 50 dias para fabricar + 30 dias para chegar no TRF3
  - Módulo de Uplink C9300 com 08 portas 10Gbps – aprox. 50 dias para fabricar + 30 dias para chegar no TRF3
  - Fontes redundantes C9300 – aprox. 70 dias para fabricar + 30 dias para chegar no TRF3
  - GBICs/Transceivers – aprox. 14 dias para fabricar + 30 dias para chegar no TRF3

- **Switch C9200**:
  - Catalyst Switch tipo Fixo, modelo C9200-48PXG-A (sem stackwise e sem o módulo de Uplink) - 70 dias para fabricar + 30 dias para chegar no TRF3
- **DNA Center:**
  - Opção de Appliance Físico de Gerência do DNA Center modelo DN2-HW-APL - 70 dias para fabricar + 30 dias para chegar no TRF3;
  - Opção de Máquina virtual de Gerência do DNA Center - aprox. 1,5 semana para obtenção de licença na Cisco e entrega ao TRF3.
- **Solução Cisco NAC**:

Máquinas virtuais do Cisco ISE - aprox. 1,5 semana para obtenção das licenças na Cisco e entrega ao TRF3.

Todos esses quantitativos são estimativas para auxiliar a diretoria na definição do orçamento para compra de equipamentos. Os equipamentos adquiridos deverão ter suporte e garantia pelo prazo de 60 meses. Porém, a ata de registro de preços terá validade de 12 meses. Nesse prazo, todos os quantitativos acima deverão ser atualizados respeitando o orçamento existente e prioridades de implantação da solução, ou seja, qual necessidade será atendida primeiro, de acordo com o que foi apresentado nos subitens 1.2.1 a 1.2.4.

2.2. Estimativa após redesenho da solução:

Em relação ao quantitativo de switches para Torre Norte e Torre Sul, houve atualização (ampliação) do número estimado apontado anteriormente, porém, considerando apenas o modelo 9200L-48P-4X-A, conforme apontado no subitem 1.3.1. Além disso, com exceção dos cabos stackpower e dos módulos de uplink, o quantitativo de todos os demais acessórios para estes dois prédios (cabos stackwise, fontes, transceivers) foi mantido após o redesenho de solução.

Netdisco | Inventory | Reports | Admin | Find Anything

By Platform

Vendor	Model	Count
Net-SNMP	linux	2
cisco	295024G	1
cisco	296024PC	26
cisco	2960G48	176
cisco	29xxStack	310
cisco	37xxStack	32
cisco	65xxVirtualSwitch	1
cisco	Cat9300FixedSwitchStack	28
cisco	CatWSC2960L48PSLL	12
cisco	cevChassisN5KC56128P	1
cisco	IGESM	2
cisco	N5KC56128P	5
cisco	N9KC92160YC	4
cisco	N9Kc9504	5
cisco	WsC2960s24tsS	14
unknown	enterprises.28557.1.332	10
unknown	enterprises.28557.1.408	2
Unknown	unknown	1

Figura 10 – Resumo atualizado de modelos de switches em operação no parque do TRF3. Fonte: Netdisco. Dez/2023

Atualmente, o parque de switches de acesso ultrapassa o número estimado de 600 switches. A Figura 10 mostra um retrato atualizado da Figura 1. Alguns equipamentos não estão contabilizados na imagem acima ou por estarem ausentes de configuração de SNMP ou inacessíveis no momento do processo de descoberta da ferramenta Netdisco. Pelos mesmos prováveis motivos, eles também não foram contabilizados no levantamento da Figura 1, cujo levantamento ocorreu entre junho e julho de 2023. Isto posto, cabe aqui atualização sobre o aumento do quantitativo estimado de cerca de 80% do parque de switches, ou seja, em comum

acordo com a diretoria, optamos por registrar em ata um quantitativo de 480 switches 9200-L-48P-4X-A. A estratégia foi atualizada para contemplar requisitos de segurança e eficiência na conectividade das unidades remotas, principalmente as mais distantes e de difícil acesso. Essa estratégia se mostrou mais produtiva e realista, pois os switches inutilizados na sede não serão compatíveis com a solução Cisco DNA e, a grande maioria, não deve ser compatível com a solução Cisco ISE. Todos os demais quantitativos de acessórios (fontes, kits de empilhamento, transceivers) também seguiram a atualização do quantitativo de switches. O ponto de atenção aqui é que, embora tenhamos a intenção de registrar preço para esse quantitativo, a estratégia será limitada pela barreira orçamentária, ou seja, a JF3R só poderá comprar até o limite de seu orçamento.

Para a solução de DNA Center, a decisão final foi de 3 appliances físicos DNA Center com 2 interfaces 10Gbps SFP+ cada um, além de 6 transceivers 10Gbps para suportar conectividade desses 3 appliances. A RGAS possui 12 transceivers em estoque remanejados de um antigo projeto da RADM. Embora estes transceivers possam ser utilizados no projeto da RCOD, é responsabilidade deste setor também as necessidades e sugerir registro para 6 transceivers de 10Gbps SFP+. A conexão destes appliances deveria ser feita no switch Core, porém, não há portas SFP disponíveis nos equipamentos Nexus 9504, apenas portas UTP. Sendo assim, optamos por manter a ligação destes appliances nos switches Nexus 92160YC da Torre Sul, que possuem interfaces 10Gbps SFP disponíveis. Essa arquitetura será revista em projeto futuro de substituição dos Nexus Core e Distribuição (agregação) da arquitetura de redes. Possivelmente, estes equipamentos serão substituídos por switches Catalyst das linhas 9500, 9400 ou 9300 nas funções de switch core e agregação. Em relação ao licenciamento, manteve-se a licença DNA Advantage.

Para a solução de NAC, a decisão foi de 2 appliances virtuais Cisco ISE com licença do tipo Advantage, suportanto até 10.000 dispositivos. Pensando em futura expansão de dispositivos, incluindo eventuais acessos de visitantes (rede wifi e cabeada) à rede corporativa, também faremos registro de licença adicional de 5.000 dispositivos (uso futuro).

Os servidores da RCOD farão treinamento oficial das 2 soluções (Cisco ISE e Cisco DNA Center), da forma que for mais conveniente (remoto ou presencial, sendo possível dividir o treinamento em mais de uma turma, se necessário).

3. ANÁLISE DE SOLUÇÕES POSSÍVEIS

3.1. Identificação das Soluções

ID	Descrição da solução (ou cenário)
1	Aquisição de switches 9200 em 2023
2	Aquisição de switches + DNA Center, em 2023
3	Aquisição do ISE + Treinamento das ferramentas, em 2023
4	Aquisição de todos os itens em 2023/2024
5	Aquisição de switches 9200L para todo o parque + DNA Center + ISE +Treinamento

3.2. Análise Comparativa de Soluções

3.2.1. Cenário 1

A implantação desses switches só pode se mostrar possível para modelo C9200, em virtude de prazo de entrega desses equipamentos no fabricante. Condicionada ao orçamento da direção para essa finalidade em 2023. A linha C9300 tem um prazo muito alto de entrega e, portanto, é mais provável que seja adquirida em 2024.

Esses equipamentos poderiam ser configurados e enviados para o interior, com a finalidade de substituição dos switches 3750 de borda (função de backbone).

Prazo para implantação: Mínimo de 100 dias para recebimento de equipamentos C9200, conforme item 2 (Estimativa da demanda) deste documento.

Vantagens: Switches mais modernos para exercer a função de switch de borda em localidades remotas da SJSP e SJMS, principalmente as mais distantes.

Desvantagens: O prazo de entrega é uma estimativa do fabricante e pode sofrer alterações, o prazo do processo de análise e publicação do edital de licitação (pregão) e assinatura de contrato com um licitante arrematante também podem se estender além do previsto. Esses fatores podem influenciar na viabilidade desse cenário. Usualmente, a contratada tem cerca de 60 dias para entregar os equipamentos e esse prazo deveria decorrer ao longo do exercício de 2023, considerando o pagamento por parte da contratante (JF3R).

3.2.2. Cenário 2

A implantação desses switches só pode se mostrar possível para modelo C9200, em virtude de prazo de entrega desses equipamentos no fabricante. Condicionada ao orçamento da direção para essa finalidade em 2023. A linha C9300 tem um prazo muito alto de entrega e, portanto, é mais provável que seja adquirida em 2024.

Esses equipamentos poderiam ser configurados e enviados para o interior, com a finalidade de substituição dos switches 3750 de borda (função de backbone).

Prazo para implantação: Mínimo de 100 dias para recebimento de equipamentos C9200, conforme item 2 (Estimativa da demanda) deste documento.

Vantagens: Switches mais modernos para exercer a função de switch de borda em localidades remotas da SJSP e SJMS, principalmente as mais distantes.

Desvantagens: O prazo de entrega é uma estimativa do fabricante e pode sofrer alterações, o prazo do processo de análise e publicação do edital de licitação (pregão) e assinatura de contrato com um licitante arrematante também podem se estender além do previsto. Esses fatores podem influenciar na viabilidade desse cenário. Usualmente, a contratada tem cerca de 60 dias para entregar os equipamentos e esse prazo deveria decorrer ao longo do exercício de 2023, considerando o pagamento por parte da contratante (JF3R).

3.2.3. Cenário 3

O ISE permitiria um nível de automação de funcionalidades de segurança extremamente robusto, que incrementa o nível de segurança da instituição e complementa a plataforma de segurança discutida no subitem 1.2.4.

Adicionalmente, sabemos que haverá necessidade de treinamento para a equipe RCOD implementar as soluções de conectividade e segurança. Portanto, é uma solução que pode ser adquirida ainda com o orçamento de 2023 e com menor risco de perda de prazo para pagamento.

Prazo para implantação: No mínimo 1 semana para provisionar licenciamento do ISE e recebimento no TRF3 e mínimo de 50 dias para implantação e configuração.

Vantagens: Aproveitamento de orçamento 2023 para aquisição de switches com uma solução de curtíssimo prazo de recebimento pela contratante e de treinamento da equipe, preparando-a para a operação das novas ferramentas que serão adquiridas (DNA Center e ISE).

Além disso, pode ser vantajoso ter o treinamento antes mesmo da fase de implantação e operação das novas ferramentas.

Por fim, o ISE é concebido como uma solução integrante de uma sugestão apresentada à diretoria para evolução da rede em quesitos mais robustos, como a adição de um NAC. Essa plataforma seria integrada à rede futuramente com os demais componentes, como switches

9200 e 9300 adquiridos na mesma ata, além do DNA Center, essenciais à construção da infraestrutura atual.

Temos alguns modelos[3] de switches no parque que poderiam se beneficiar da integração com o ISE, como o modelo 2960L (10 unidades).

Desvantagens: Estaremos limitados à aplicação do ISE nos switches compatíveis existentes no parque.

3.2.4. Cenário 4

Iniciar implantação do projeto em 2023/2024, tendo em vista que o pagamento só ocorreria em 2024, com o prazo de entrega alto para os switches alvo desta contratação (Catalyst 9200 e 9300), conforme item 2 (Estimativa da demanda) deste documento.

Prazo para implantação: No mínimo 1 semana para provisionar licenciamento do ISE e recebimento no TRF3 e mínimo de 50 dias para implantação e configuração.

Vantagens: Aproveitamento de orçamento 2023 para aquisição de switches com uma solução de curtíssimo prazo de recebimento pela contratante e de treinamento da equipe, preparando-a para a operação das novas ferramentas que serão adquiridas (DNA Center e ISE).

Além disso, pode ser vantajoso ter o treinamento antes mesmo da fase de implantação e operação das novas ferramentas.

Por fim, o ISE é concebido como uma solução integrante de uma sugestão apresentada à diretoria para evolução da rede em quesitos mais robustos, como a adição de um NAC. Essa plataforma seria integrada à rede futuramente com os demais componentes, como switches 9200-L e DNA Center, essenciais à construção da infraestrutura atual.

Temos alguns modelos[2] de switches no parque que poderiam se beneficiar da integração com o ISE, como o modelo 2960L (10 unidades).

Desvantagens: Estaremos limitados à aplicação do ISE nos switches compatíveis existentes no parque.

3.2.5. Cenário 5

Aquisição de switches 9200-L, Cisco DNA Center, Cisco ISE e treinamentos no exercício 2024, considerando o prazo de entrega dos equipamentos e, principalmente, o orçamento da SETI. Nesse cenário, não consideramos a aquisição de 100% do quantitativo registrado, mas

especialmente para que a arquitetura SD-Access seja implantada, existe um quantitativo mínimo que precisa ser respeitado, como cerca de 10 switches 9200-L, solução DNA Center, solução NAC (Cisco ISE) e treinamentos oficiais. Dessa forma, seria possível que contratar o serviço de instalação e configuração inicial para que a empresa especializada instale todo o ambiente para a equipe técnica, faça um repasse do conhecimento e suporte o ambiente por um período de 30 a 60 dias após a implantação, para ajustes emergenciais comuns em projetos deste porte. Em paralelo, a equipe técnica (RCOD) terá condições de iniciar os treinamentos nas soluções Cisco DNA Center e Cisco ISE, para adquirir capacitação necessária para suporte ao ambiente.

Prazo para implantação: No mínimo 90 dias, considerando fabricação e entrega dos appliances DNA Center, switches de acesso e acessórios.

Vantagens: A Administração já terá uma porção da rede implantada na nova arquitetura. Ainda

Desvantagens: Depende de orçamento disponível e do tempo de entrega. Não permitirá usar o orçamento em 2023.

3.3. Pesquisa de Preços de Mercado

A pesquisa de mercado foi redesenho da solução, conforme apontado no subitem 1.3.1. Dessa forma, buscamos editais de soluções semelhantes, a saber:

PE 82/2022 realizado pela Câmara dos Deputados;

Pregão Eletrônico Nº 160/2022 do Ministério da Defesa

Pregão Eletrônico Nº 136/2021 do SERVIÇO NACIONAL DE APRENDIZAGEM RURAL DO MATO GROSSO

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Soluções que não contemplem switches Cisco podem ser competitivas em relação ao custo, a exemplo do que ocorreu no edital de licitação da Câmara dos Deputados, mas para a realidade da JF3R, que utiliza 100% de switches Cisco, poderia haver incompatibilidade técnica entre equipamentos de fabricantes distintos, trazendo instabilidade no acesso à rede dos usuários, atrapalhando a atividade jurisdicional.

5. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

5.1. Cálculo dos Custos Totais de Propriedade

Os principais custos estimados, são:

Serviço de instalação ISE e DNA Center: R$ 586.393,33 (estimativa NTT de maio/2023)

Appliances de licença Cisco DNA + ISE: R$ 1.281.075,18 (estimativa NTT de maio/2023)

Aquisição de switches 9200-L: R$ 18.882,60 (preço unitário) x aprox. 300 switches. Total de R$ 5.664.780,00 (estimativa do PE 82/2022 da Câmara dos Deputados)

Treinamento: R$ 74.937,50 (preço unitário) x 4 servidores RCOD. Total de R$ 299.750,00.

6. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

A solução a ser contratada deverá ser capaz de conectar dispositivos finais, como impressoras, câmeras IP, notebooks e computadores, bem como dispositivos intermediários, como access-points e outros switches. O modelo 9200L-48P-4X-A será adquirido para abastecimento do estoque de switches para envio ao interior de SP, de MS e também para a sede do TRF (Torres Norte e Sul). No interior, esse switch não contará com SFP adicional, tendo em vista que a largura de banda dos links remotos, atualmente, não ultrapassa 1 Gbps. Na sede do TRF3, porém, os switches serão empilhados em grupos de 4 switches na Torre Sul, sendo que os switches topo e base da pilha terão conexões de 10Gbps nas portas de uplink. Para tanto, será necessário adquirir transceivers SFP de 10Gbps em quantidades suficientes, respeitando o quantitativo apontado no item 2 deste estudo. Para a Torre Norte, as pilhas terão tamanhos variados, conforme explicado no subitem 2.1, mas também contarão com uplinks de 10Gbps no switch topo e base de cada pilha. Em reunião de acompanhamento de projetos com toda da diretoria, a decisão foi de registrar um total aproximado de 300 switches desse modelo, para atender SJSP, SJMS e TRF3.

Para aumentar a eficiência e segurança da rede, também serão contratadas uma solução de gerenciamento e automatização, conhecida como Cisco DNA Center, e de controle de acesso à rede – NAC -, conhecida como Cisco ISE. Ambas as tecnologias trabalham de forma integrada e única para compor uma solução, em conjunto com os demais equipamentos. Em consulta ao engenheiro da Cisco, obtivemos a sugestão de aquisição de quatro appliances virtuais (a sugestão da NTT foi de duas máquinas virtuais), sendo duas máquinas desempenhando o papel (“persona”) de PSN (Policy Service Nodes) e duas máquinas desempenhando dois papéis (“persona”) simultaneamente de Policy Administration Node (PAN) e Primary Monitoring Node (MnT). Em relação ao DNA Center, mantivemos a sugestão da NTT

de três appliances físicos. Cada appliance necessitará, também, de dois transceivers SFP de 10Gbps, num total de seis para toda a solução DNA Center.

Com o intuito de aproveitar o investimento anterior em equipamentos compatíveis com essas duas soluções, também necessitamos de extensão de garantia para switches 9300-24-T em operação na nossa infraestrutura, bem como licenças de subscrição para DNA Advantage para esses mesmos equipamentos.

Toda a solução acima deverá ter validade de 60 meses para os aspectos de suporte, garantia e licenciamento.

A equipe técnica (RCOD) necessitará de capacitação para operar essa nova solução e, portanto, também necessitaremos de treinamento oficial de Cisco DNA Center e Cisco ISE.

Também reforçamos a importância de mantermos o foco na renovação do parque Cisco e modernização tecnológica deste mesmo fabricante:

- Do ponto de vista financeiro, trata-se de opção mais econômica, tendo em vista que aproveitaremos parte dos equipamentos existentes e o conhecimento da equipe técnica;
- Do ponto de vista operacional, trata-se de opção essencial, tendo em vista que a experiência e conhecimento da equipe técnica (RCOD) é completamente voltada a tecnologias Cisco. A curva de aprendizado para equipamentos de outros fabricantes seria enorme, em especial para switches de acesso, que são amplamente utilizados em toda da JF3R e que atendem diretamente os usuários finais em suas estações de trabalho. Estimamos um custo adicional de aquisição de operação assistida significativo para acompanhar a equipe técnica;
- Do ponto de vista técnico, manter uma infraestrutura de TI homogênea, utilizando equipamentos do mesmo fabricante, permite o uso de ferramentas de gerenciamento e monitoramento integradas e otimizadas para esses equipamentos, tendo em vista que introduzir equipamentos de fabricantes distintos dificultam tecnicamente a gestão da rede, pois pode ser necessário utilizar múltiplas plataformas de gerenciamento, aumentando a complexidade operacional.
- Do ponto de vista tático, a manutenção desses equipamentos também preserva investimento de contratação efetuada em 2023 para suporte especializado Cisco. O processo SEI 0006750-49.2023.4.03.8000 (contrato no. 04.050.10.2023)

detalha a contratação (prorrogável), por 12 meses, de dois profissionais terceirizados especializados em soluções Cisco, principalmente de conectividade (switches). Este contrato teve por base a totalidade de switches Cisco sob administração da RCOD e foi a motivação para contratação de profissionais com especialização Cisco CCNP.

Por se tratar de um estudo para uma ata de registro de preços, porém, observamos que o quantitativo irá variar com base no preço máximo registrado e no orçamento do TRF3.

7. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

O custo total estimado da contratação é o somatório dos custos individuais apontados no subitem 5.1, ou seja, R$ 586.393,33 + R$ 1.281.075,18 + R$ 5.664.780,00 + R$ 299.750,00. Portanto, a estimativa de custo total é de R$ 7.831.998,51. Esse custo deverá ser distribuído ao longo dos 60 meses, considerando aquisição de equipamentos e licenças e prestação de serviço de suporte e garantia.

8. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Considerando as necessidades de negócio e necessidades tecnológicas, bem como os benefícios da automatização de tarefas com solução DNA Center, além do nível de segurança e controle da rede possíveis com Cisco ISE, entendemos que a contratação é viável e de interessa da administração.

Reforçamos que, por se tratar de uma solução composta por vários elementos independentes, mas que irão compor uma arquitetura unificada, não deverá haver parcelamento do objeto (solução) em mais de uma empresa.

9. REFERÊNCIAS

1. https://blog.nec.com.br/a-importancia-da-segmentacao-da-rede-na-seguranca-da-informacao
2. https://www.camara.leg.br/licitacoes-e-contratos/licitacoes/18646
3. https://www.cisco.com/c/en/us/td/docs/security/ise/nad_capabilities/nad_capabilities_with_ise.html#Cisco_Reference.dita_3456b3da-c198-439e-bb7c-d1ca839e1751

10. APROVAÇÃO E ASSINATURA

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Técnico	**Integrante Requisitante**	**Autoridade Máxima de TI**
Elias Meira dos Santos:3811 Assinado de forma digital por Elias Meira dos Santos:3811 Dados: 2023.12.11 10:45:53 -03'00'	VINICIUS SOUZA BARBOSA:3341 Assinado de forma digital por VINICIUS SOUZA BARBOSA:3341 Dados: 2023.12.11 11:29:46 -03'00'	DANIEL HENRIQUE GUIMARAES:3624 Assinado de forma digital por DANIEL HENRIQUE GUIMARAES:3624 Dados: 2023.12.11 12:12:21 -03'00'

Integrante Administrativo:

Anderson Alves Chieregat:4057

Digitally signed by Anderson Alves Chieregat:4057
DN: C=BR, O=ICP-Brasil, OU=Autoridade Certificadora da Justica - AC-JUS, OU=Cert-JUS Institucional - A3, OU=44264331000104, OU=Presencial, OU=Tribunal Regional Federal da 3a Regiao-TRF3, OU=Servidor, CN=Anderson Alves Chieregat:4057
Reason: I am the author of this document
Location:
Date: 2023.12.11 11:39:05-03'00'
Foxit PDF Reader Version: 2023.3.0