ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

1. Requisitos de Negócio

1.1. Está sendo montado um *datacenter* secundário (*backup*), localizado no térreo do Edifício Sede do Tribunal de Contas do Distrito Federal – TCDF, para replicar os serviços da sala dos equipamentos de informática da Departamento de Tecnologia da Informação – DTI. Esse sítio secundário terá a capacidade de manter em funcionamento toda a rede local do TCDF no caso do *datacenter* primário, localizado no primeiro andar do Edifício Anexo, ficar inoperante.

1.2. Nesse último ano, alguns serviços passaram a exigir mais recursos, como o *MentoRH* e o *SINJ*. E serviços importantes, como o processo eletrônico, estão sendo muito demandados. Portanto, há a necessidade de maior capacidade computacional para a melhoria no desempenho dos serviços e que permitam a distribuição de carga com redundância dos serviços mais críticos.

1.3. O sistema de segurança da rede local baseia-se em computadores que executam as funções de *firewall*, *proxy* e roteamento. Alguns desses equipamentos são computadores de mesa reaproveitados e precisam ser substituídos.

1.4. O sistema de monitoramento por câmeras de vídeo ocupa 12 TiB [1] (~13,2 terabytes) para armazenamento de imagens, e permite que os vídeos fiquem armazenados por um período de 20 a 24 dias. Para que as imagens fiquem armazenada por cerca de seis meses é necessário aumentar o espaço de armazenamento de 12 TiB para mais de 100 TiB (um aumento de aproximadamente oito vezes).

2. Levantamento das soluções disponíveis

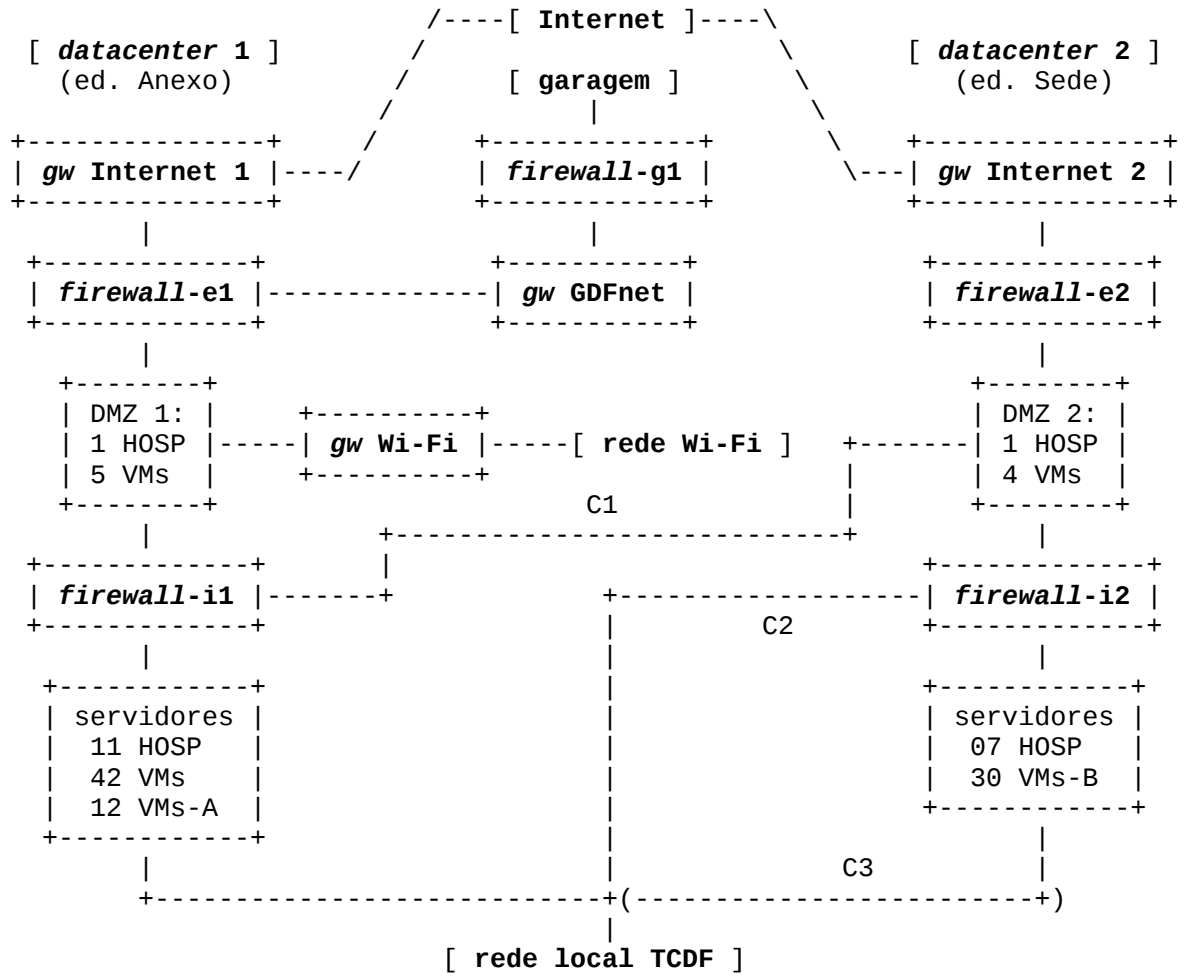
São três os tópicos a serem analisados: (i) a duplicação do *datacenter*, que consiste na aquisição de computadores hospedeiros; (ii) o sistema de *firewall*, que baseia-se em computadores configurados para a função; (iii) o sistema de armazenamento, consistindo de servidores de disco e equipamentos de rede (*switches*).

2.1. Duplicação do *datacenter*

A duplicação do *datacenter* faz parte de um processo de contingenciamente e alta disponibilidade que consiste, basicamente, em duas partes: (i) redundância ativa (*online*) com duplicação de servidores no *datacenter* primário; (ii) redundância passiva (*offline*), com duplicação de servidores no *datacenter* secundário, a serem ativados apenas quando o *datacenter* primário ficar inoperante. Sua implantação começou pela aquisição de equipamentos por meio dos processos de nº 28569/2013 (*switches* e duplicação de fibras ópticas) e de nº 16352/2014 (computadores e sistema de

1 O byte é uma unidade binária não reconhecida pelo SI (Sistema Internacional de Unidades), o qual recomenda que, para este caso, seja usado o padrão ISO-IEC 60027-2:2005 (substituído pelo ISO-IEC 80000-13: 2008). Neste padrão o byte é representado pela letra 'B' e o bit por 'b'. Os prefixos representam potências de 2: para 2^{10} (1024) usa-se o *kibi* (sigla Ki); para 2^{20} o *mebi* (MiB); para 2^{30} o *gibi* (GiB); para 2^{40} o *tebi* (TiB).

armazenamento). A figura 2.1.1 mostra a estrutura proposta para os dois *datacenters* (e inclui a localização lógica da garagem).



HOSP: computador hospedeiro de máquinas virtuais (VMs).
C1: conexão da DMZ do *datacenter* 2 ao conjuntos de servidores da rede local por meio do *firewall-i1*.
C2: conexão dos computadores clientes da rede local à DMZ do *datacenter* 2 para acesso à Internet.
C3: conexão *offline* entre os servidores instalado no *datacenter* 2 à rede local – a ligação somente será ativada manualmente.

Figura 2.1.1: esquema da estrutura proposta para a rede do TCDF.

Neste esquema da rede local do TCDF foram consideradas as seguintes estruturas: (i) três unidades (sítios) de processamento – *datacenter* primário (ed. Anexo), *datacenter* secundário (ed. Sede) e sub-sistema da garagem; (ii) três sub-redes – rede principal (ed. Sede + ed. Anexo), sub-rede da garagem e sub-rede Wi-Fi; (iii) duas redes externas – GDFnet e Internet – esta, com duas conexões independentes[2].

Atualmente, na rede do TCDF, existem 47 servidores virtuais (executando em máquinas virtuais – VMs) instalados em 16 computadores hospedeiros. Dos 47, cinco já são servidores redundantes. Para a

2 O TCDF possui somente uma conexão à Internet. A segunda será contratado em procedimento separado.

implementação do esquema mostrado na figura 2.1.1 são necessários 20 computadores hospedeiros.

O TCDF possui, além dos 10 computadores hospedeiros adquiridos em 2014, um sistema em chassi *HP Blade System* que possui 16 lâminas – nove do modelo *BL460 G1* (adquiridas em 2008) e sete do modelo *BL460 G7* (adquiridas em 2012). Pelo menos três das lâminas G1 e uma G7 apresentam problemas de *hardware*. Considerando-se que os equipamentos do modelo G1 já têm cerca de sete anos de uso, sua manutenção não é recomendada. Os equipamentos do modelo G7 ainda podem ser usados, mas estão sem garantia, portanto podem ser usados seis, por um prazo não superior a dois anos.

Conclui-se que são necessários quatro novos computadores hospedeiros para que a estrutura proposta fique plenamente operacional. Acrescente-se mais um computador para que seja possível instalar alguns servidores (em VMs).

No processo nº 16352/2014 foi mostrado que existem dois sistemas de processamentos de dados quanto à estrutura: (i) em chassi, onde os computadores são lâminas (*blades*) instalados em um gabinete proprietário (o chassi que é o caso do *HP Blade System*); (ii) modular, onde os computadores são equipamentos independentes (caso dos computadores adquiridos por meio do processo nº 16352/2014). A solução modular foi escolhida naquele processo (vide e-DOC 5D8FE67A) e também será adotada aqui.

2.2. Sistema de *firewall*

Um *firewall* é um dispositivo ou um grupo de dispositivos que aplica uma política de controle de acesso entre redes [3]. Faz parte de um sistema de segurança da informação, que por sua vez possui três objetivos básicos [4]: (i) confidencialidade – dados protegidos somente serão acessados por pessoa(s) autorizada(s); (ii) integridade – a informação somente poderá ser alterada por pessoa(s) autorizada(s); (iii) disponibilidade – a informação deve estar sempre (ou quase sempre) disponível para pessoa(s) autorizada(s).

O TCDF possui uma rede local privada que conecta-se à Internet a 100 Mbit/s[5]. Também possui uma conexão Gigabit (1000 Mbit/s) com a GDFnet. Além da rede local, existe uma sub-rede *wireless* (Wi-Fi) para acesso de visitantes e conexão de dispositivos móveis (*smartphones, tablets* e *notebooks*).

Até 2013 o TCDF usava como *firewall* um par de equipamentos fabricados pela empresa *Aker Security Solutions*. Esses equipamentos operavam em modo redundante ativo-passivo[6]. A figura 2.2.1 mostra o

3 Definição fornecida pela RFC 2647 (<https://tools.ietf.org/html/rfc2647>).
4 Veja-se o documento "*Guide to General Server Security*" (disponível em <http://csrc.nist.gov/publications/PubsSPs.html>) do NIST (*National Institute of Standards and Technology*, órgão do governo dos EUA).
5 Neste texto serão usadas as expressões 'Mbit/s' para indicar milhões de bits por segundo e 'Gbit/s' para indicar bilhões de bits por segundo.
6 No modo ativo-passivo os dois equipamentos efetivamente operam como um único dispositivo – um dos equipamentos funciona (dispositivo passivo) como *firewall*, enquanto o outro fica na reserva (dispositivo passivo), entrando em operação automaticamente quando o primeiro pára de funcionar.

esquema de funcionamento daquele ambiente. Um único *firewall* para controlar o tráfego entre diversas redes é denominado "*multi-homed firewall*".

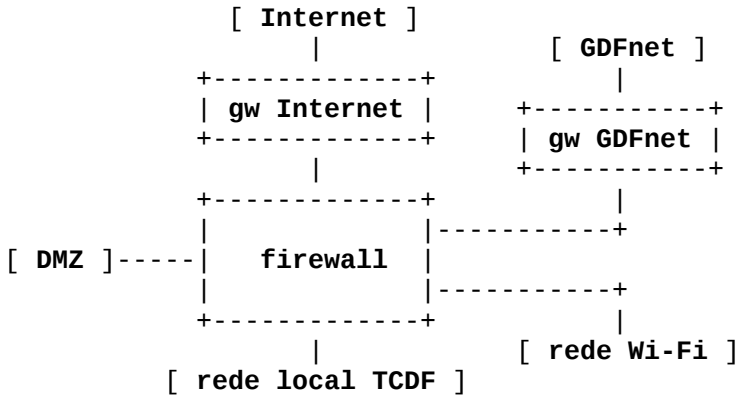


Figura 2.2.1: esquema da antiga estrutura de *firewall* do TCDF.

Na DMZ ("Zona Desmilitarizada") foram disponibilizados os seguintes serviços: (i) um servidor *proxy* reverso apontando para servidores Web na rede local; (ii) servidores DNS primário e secundário do TCDF na Internet; (iii) um *gateway* MTA para recebimento e envio de mensagens de correio eletrônico.

O sistema de páginas Web do TCDF consiste em um conjunto de servidores Web *Apache*, com um servidor *proxy* reverso centralizando a disponibilização dessas páginas, tanto na Internet como na intranet. A função do servidor de *proxy* reverso é receber e reencaminhar as requisições internas (de clientes da rede local) e externas (de clientes na Internet) para os servidores Web internos. Essa estrutura contém um ponto de falha único e um gargalo de processamento e de tráfego de dados. No final de 2013 esse sistema apresentou falhas, por causa da degradação de alguns componentes e por falta de desempenho.

Em dezembro de 2013 o *firewall* da Aker foi substituído por um conjunto de quatro computadores de mesa[7] usados, os quais foram configurados para funcionarem como dispositivos de *firewall*. Em cada computador foi instalado o sistema operacional Linux com *netfilter*e a configuração do *firewall* foi feita pelo aplicativo *iptables*. A estrutura usada é mostrada na figura 2.2.2.

A conexão da Internet ao sítio Web do TCDF foi distribuída entre os dois *firewalls* externos (*firewall-e1* e *firewall-e2* na figura) – os dois servidores de *proxy* reverso (*proxy-r1* e *proxy-r2*) fazem a intermediação entre a Internet e os servidores Web localizados na rede local; os dois servidores DNS (DNS1 e DNS2) conectam-se à Internet, cada um por um *firewall*; o *gateway* MTA (que também funciona como *antispam*) conecta o servidor de correio eletrônico (que situa-se na rede local) à Internet. O *firewall-e2* também liga a rede do TCDF à GDFnet.

7 Um computador de mesa (*desktop*) é um computador mais simples que um servidor de rede. Sua durabilidade é menor e possui menos recursos (embora possa ter maior capacidade de processamento).

Os dois *firewalls* internos (*firewall-i1* e *firewall-i2* na figura) controlam o acesso entre a DMZ e a rede local. O *firewall-i1* conecta os servidores da rede local à DMZ e o *firewall-i2* permite que os usuários da rede local e da sub-rede Wi-Fi acessem a Internet.

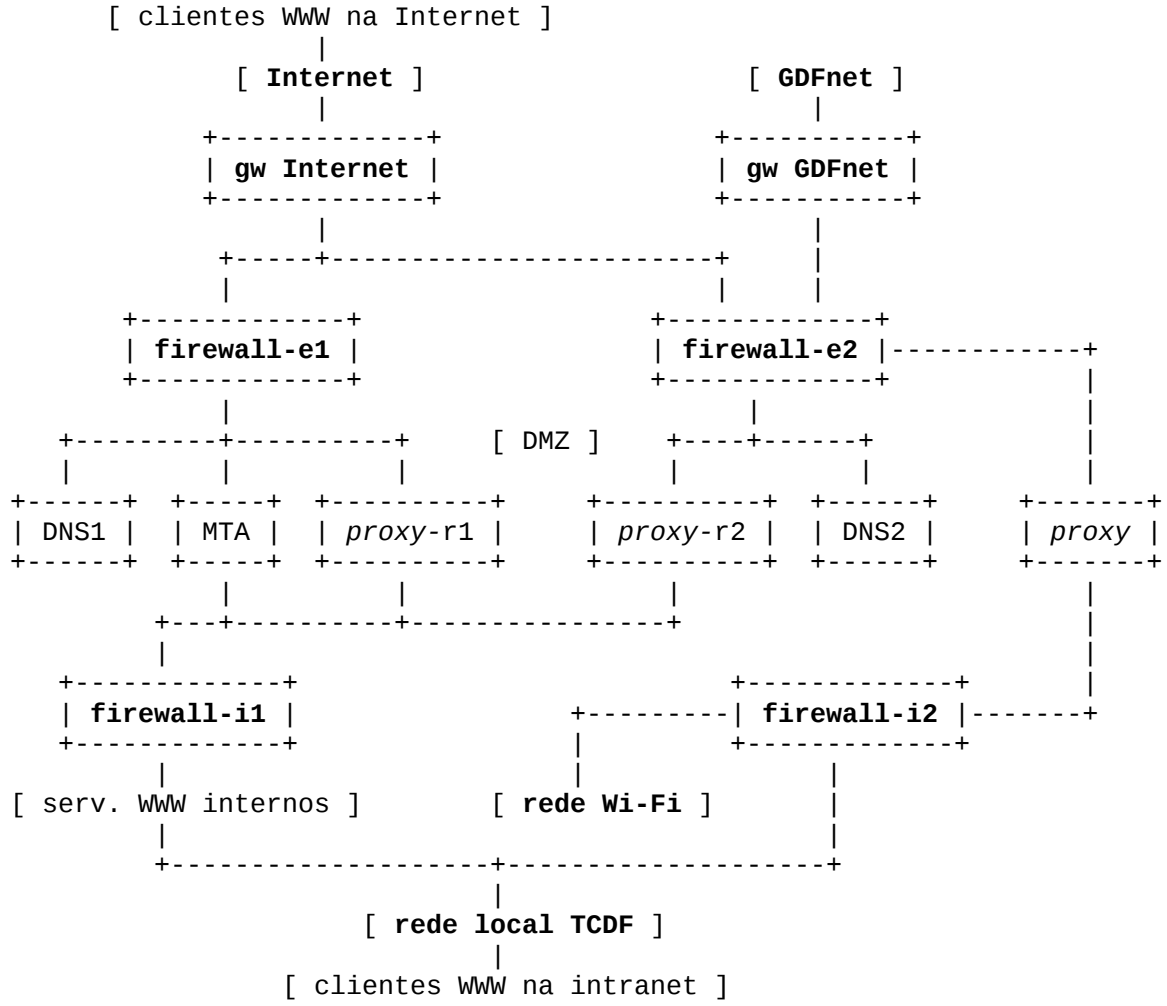
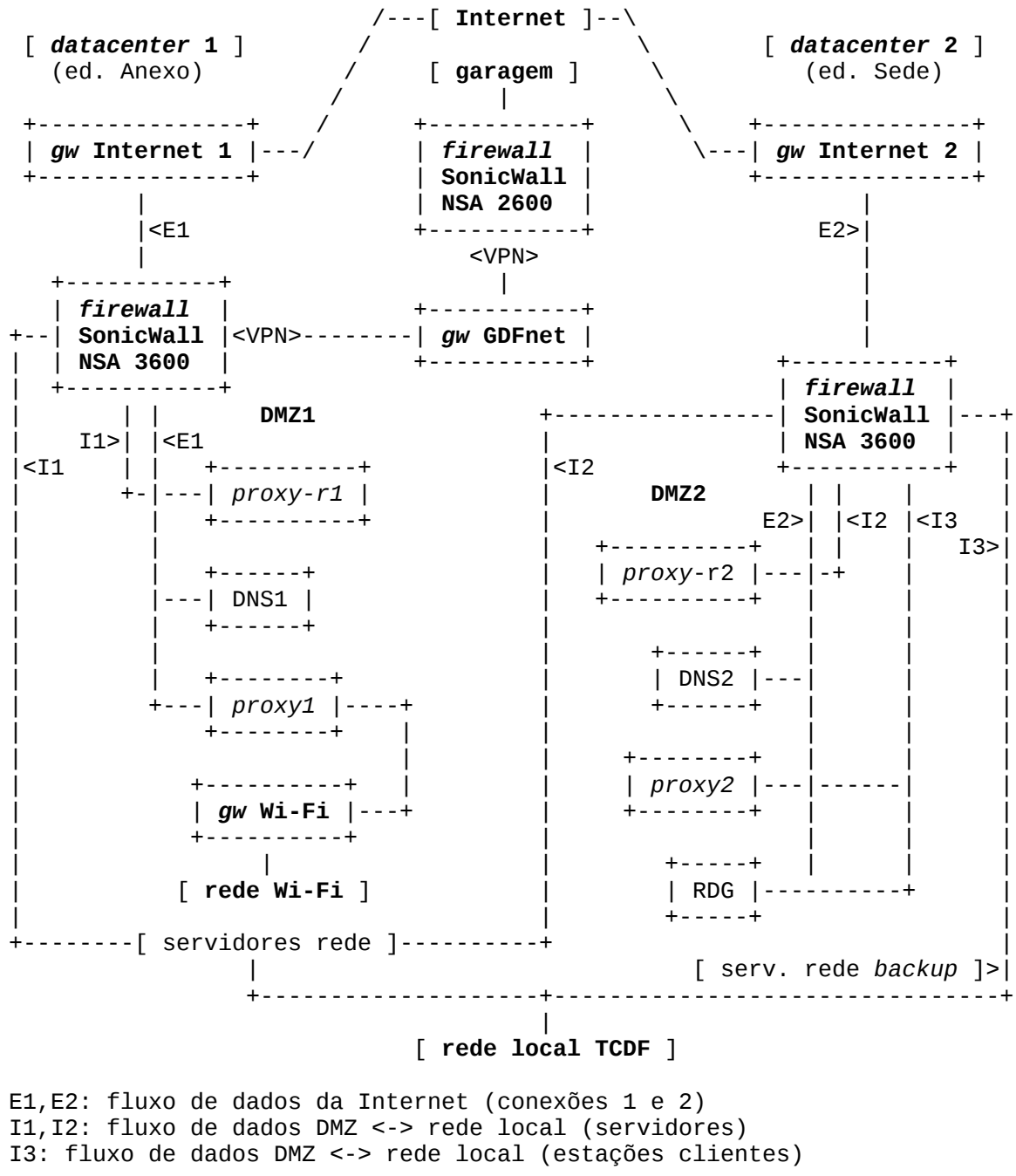


Figura 2.2.2: esquema da estrutura de *firewall* e serviços WWW do TCDF em 2013-2015.

Com a implementação de um segundo *datacenter*, a estrutura deve ser modificada. A figura 2.2.3 mostra um sistema de segurança para dois *datacenters* baseado na utilização de dispositivos de *firewall* da marca *Dell SonicWall*, série NSA. [8]

Na figura são mostradas as duas conexões de acesso à Internet que ainda serão contratadas ("*gw Internet 1*" e "*gw Internet 2*"). A estrutura mostrada é análoga à da figura 2.2.1, pois utiliza apenas um *firewall* (modelo *NSA 3600*) para cada datacenter. Também inclui um *firewall*de menor capacidade (modelo *NSA 2600*) para a garagem.

8 Para este estudo foram analisados equipamentos (computador e *firewall*) da marca Dell pelos seguintes motivos: (i) o TCDF adquiriu recentemente computadores da Dell; (ii) em 2014 o TCDF contratou a aquisição de um conjunto Dell SonicWall 5600 (dois dispositivos em modo ativo-passivo), mas o contrato foi cancelado (Processo nº 11127/2013); (iii) a Dell permite a configuração *online* dos equipamentos, mostrando o valor final em dólar dos EUA.



E1,E2: fluxo de dados da Internet (conexões 1 e 2)
I1,I2: fluxo de dados DMZ <-> rede local (servidores)
I3: fluxo de dados DMZ <-> rede local (estações clientes)

Figura 2.2.3: esquema com *firewall* único na estrutura de segurança da rede do TCDF.

O dispositivo *Dell SonicWall NSA 3600* é, segundo o fabricante, um "*Next-Generation Firewall*" (NGFW) [9], e a principal vantagem da linha NSA é o conjunto de múltiplas tecnologias de segurança em um pacote [10], tais como filtros contra *softwares* maliciosos (*antivirus*, *antispyware*, etc.), sistemas de prevenção de invasão (IPS), e filtro de conteúdo. Também possui um serviço de *antispam.* Por isso, em comparação com a figura 2.2.2, nota-se, além da diferença na organização dos diversos equipamentos, que não há um servidor

9 A Dell SonicWall também fornece o tipo UTM ("*Unified Threat Management*"), mas o recomenda para escritórios e pequenas empresas.

10 "*How Traditional Firewall Fail Today's Networks – and Why Next-Generation Firewall Will Prevail*", 2012; disponível em <http://software.dell.com/documents/how-traditional-firewalls-fail-todays-networks-ebook-24532.pdf>.

de MTA (que inclui o serviço de *antispam*), pois essa função pode ser executada pelo *NSA 3600*.

Embora o *NSA 3600* tenha recursos de DPI (*Deep Package Inspection*), DPI-SSL e filtro de conteúdo, não faz *cache* de páginas acessadas e não possui a capacidade plena para operar como "*Web Application Firewall*" (WAF). Para essa função existe a série SRA [11]. Assim, os servidores de *proxy* (direto e reverso) foram mantidos.

A Fortinet, outro fabricante de equipamentos de segurança de rede, publicou, em 2014, um documento [12] onde mostra que os *firewalls* de próxima geração (NGFW) não têm todos os recursos para um verdadeiro WAF. A tabela 2.2.1 mostra algumas dessas limitações. No mesmo documento, informa que 60% de todos os ataques observados na Internet têm como alvo as aplicações Web.

Tabela 2.2.1: comparação de recursos entre WAF (Fortinet) e NGFW.

Recurso	FortiWeb WAF	NGFW
Bloqueia ataques tais como definidos por "OWASP Top 10" (*SQL injection, XSS, CSRF,* etc.).	sim	não
Controla uma linha base de acessos permitidos: URLs, parâmetros, *cookies* e sessões.	sim	não
Provê modelos de segurança positivo e negativo.	sim	não
Controle de aplicações e funções	não	sim
Limita (controla) o tráfego de aplicações não prioritárias	não	sim
Restringe e protege o acesso de clientes à Internet	não	sim

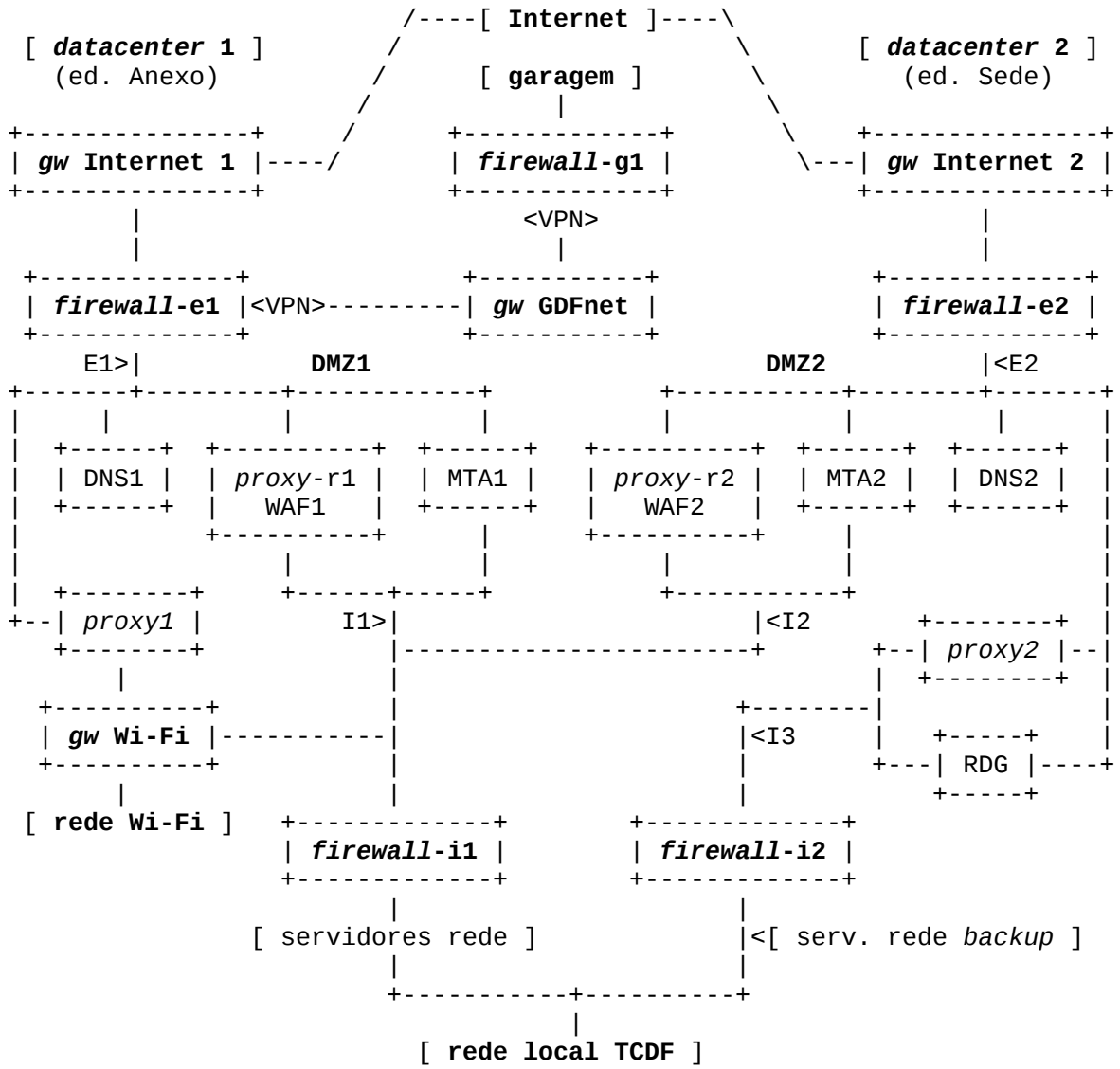
O *OWASP*, citado na primeira linha da tabela, é um projeto (*Open Web Application Security Project*) dedicado a ajudar organizações a desenvolver e manter aplicações que sejam confiáveis. Um dos seus produtos mais notáveis é o documento "*OWASP Top 10*" [13], que lista e descreve os dez maiores riscos às aplicações Web. Os principais *firewalls* de aplicação Web (WAF), sejam em *software* ou dispositivos de *hardware*, usam aquele documento como referência.

O *PCI Security Standard Council* [14] é outra organização que, dentre outras atividades, publica documentos sobre segurança da informação. Um desses documentos é o *Data Security Standard* (PCI DSS). Em um documento de 2008 - "*Information Supplement: Code Reviews and Application Firewall Clarified*"[15] são descritos dois métodos para proteger aplicações Web: (i) revisão do código fonte das aplicações; (ii) utilização de um *firewall* de aplicações Web (WAF).

11 Vide documento "*Web Application Firewall Service*", disponível em: <http://www.sonicwall.com/br/pt/products/SRA-Web-Application-Firewall.html>.
12 Vide "*WAF or IPS?: Why you need more than a Firewall and IPS to protect your applications*", disponível em: <http://www.fortinet.com/resource_center/whitepapers/waf-vs-ngfw.html>.
13 Disponível em: <https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013>.
14 Essa instituição foi fundada por grandes administradoras de cartão de crédito (American Express, Discover Financial Services, JCB International, MasterCard e Visa), mas seus documentos de segurança são usados por empresas que necessitam de segurança na Internet.
15 Disponível em: <https://www.pcisecuritystandards.org/security_standards/documents.php>.

O TCDF usa o *software* livre *Apache* como servidor Web. Um dos mais conhecidos recursos para construir um WAF voltado para o Apache é uma ferramente chamada *ModSecurity*, desenvolvida como *software* livre inicialmente por Ivan Ristic e que é mantida, atualmente, pela empresa *Trustwave Holdings, Inc*. A DTI tem como projeto a implmentação de um WAF usando o *ModSecurity* com o *Apache* em um servidor de *proxy* reverso na DMZ.

A figura 2.2.4 (que é semelhante à figura 2.1.1 e mostra uma estrutura análoga à da figura 2.2.2) mostra um esquema de segurança de rede baseado em *software* livre.




```
E1,E2: fluxo de dados da Internet (conexões 1 e 2)
I1,I2: fluxo de dados DMZ <-> rede local (servidores)
I3: fluxo de dados DMZ <-> rede local (estações clientes)
```

Figura 2.2.4: esquema da estrutura proposta para a segurança da rede do TCDF.

Nesta estrutura são usados dois dispositivos de *firewall* para cada *datacenter* e um para a garagem. Cada dispositivo é um computador servidor

de rede executando o sistema operacional Linux com *netfilter* e *iptables*. Cada *datacenter*, portanto, terá um elemento de segurança duplicado no outro.

Cada *proxy* reverso (*proxy*-r1 e *proxy*-r2) será também um *firewall* de aplicação Web (com o *Apache* e o *ModSecurity*). Estes serviços e os de MTA e DNS funcionarão em modo redundante ativo-ativo com distribuição de carga por *round-robin* por meio de configuração no servidor DNS.

Cada par de serviços conecta-se com os servidores da rede local exclusivamente por meio do *firewall* interno 1. O *firewall* interno 2 faz a conexão dos clientes da rede local à Internet (por acesso direto ou redirecionando o tráfego para o servidor *proxy* 2).

Para VPN acrescenta-se o *software* livre *OpenVPN* [16], com a vantagem de não haver restrição de número de usuários (exceto pela capacidade do *hardware*).

O servidor de *gateway* RDG faz a intermediação de acessos remotos (da Internet) para estações Windows na rede local.

Na estrutura proposta, os servidores da rede local nos *datacenter* 1 e 2 irão operar em modo redundante ativo-passivo, i.e., os servidores no *datacenter* 2 somente serão ativados quando os servidores do *datacenter* 1 estiverem inoperantes.

A tabela 2.2.2 descreve os serviços mostrados na figura 2.2.4, e lista onde esses serviços seriam executados na estrutura da figura 2.2.3.

Tabela 2.2.2: descrição dos serviços providos nas estruturas das figuras 2.2.3 e 2.2.4.

Dispositivo	Serviços da figura 2.2.4	Figura 2.2.3
a) *firewall-e1*	DNAT (servidores na DMZ), filtro IP (*stateless*, *stateful*), IDS, VPN (com a garagem)	NSA 3600
b) *firewall-e2*	SNAT (acesso à Internet pelas estações de trabalho), filtro IP (*stateless*, *stateful*), IDS, DNAT (para acesso remoto, com "*port knocking*")	NSA 3600
c) *firewall-g1*	Filtro IP (*stateless*, *stateful*), IDS, VPN (com o TCDF)	NSA 2600
d) *firewall-i1*	Filtro IP (*stateless*, *stateful*), *gateway* para servidores da rede local	NSA 3600
e) *firewall-i2*	Filtro IP (*stateless*, *stateful*), *gateway* para *proxy* na DMZ, filtros para acesso direto à Internet	NSA 3600
f) *proxy-r1, proxy-r2*	Função de *proxy* reverso e *gateway* para os servidores WWW na rede local, WAF (*Web Application Firewall*)	VM na DMZ
g) MTA1, MTA2	*Gateway* de correio eletrônico, antispam, antivirus	NSA 3600
h) *proxy1*, *proxy2*	*Proxy* direto e *cache* Web para acesso à Internet, filtro de URL para bloqueio de páginas e sítios indesejados	VM na DMZ
i) RDG	*Gateway* para acesso remoto (usando o protocolo RDP)	VM na DMZ
j) DNS1, DNS2	Servidores de nomes primário e secundário	VM na DMZ

A topologia mostrada na figura 2.2.4 (múltiplos *firewalls*) atende melhor aos princípios de segurança em sistemas computacionais do que

16 Disponível em <https://openvpn.net/index.php/open-source.html> ou no próprio Ubuntu Linux.

aquela mostrada na figura 2.2.3 (*firewall* único por sítio). O NIST, no seu "*Guide to General Server Security*" [17], lista onze princípios de segurança, inicialmente descritos por Saltzer e Schroeder[18]. Os princípios são os seguintes:

a) **simplicidade**: qualquer mecanismo de segurança deve ser o mais simples possível;

b) **segurança em caso de falhas**: se algum mecanismo de segurança falhar, a segurança não pode ser comprometida – é melhor perder funcionalidade do que segurança;

c) **defesa em profundidade**: um único mecanismo de segurança geralmente é insuficiente;

d) **mediação completa**: evitar que o usuário tenha acesso direto à informação;

e) **menor privilégio**: para cada usuário ou processo deve ser fornecido o menor privilégio necessário para a execução de determinada tarefa;

f) **separação de privilégios**: funções devem ser separadas para que se obtenha a máxima granularidade de permissões, e as funções devem ser atribuídas a pessoas, processos ou mecanismos diferentes;

g) **implementação aberta**: um sistema de segurança não deve depender do segredo da implementação ou dos componentes usados;

h) **mecanismos comuns reduzidos**: a implementação de um recurso em um sistema deve evitar que outras partes do sistema tenham acesso aos mesmos dados – por exemplo, se um servidor Web tem acesso a um banco de dados, outras aplicações não devem ter acesso ao mesmo banco;

i) **registro de ocorrências**: devem ser mantidos registros (*logs*) em papel ou outro sistema de armazenamento permanente para que seja possível identificar evidências de invasão e possibilitar a recuperação do sistema invadido ou reduzir o impacto da sua ocorrência;

j) **fator de trabalho** (relação de custo/benefício para o atacante): a quantidade de trabalho realizada pelo atacante deve ser maior que o benefício adquirido com o sucesso na tentativa de invasão;

k) **aceitação psicológica**: os usuários devem entender a necessidade da implementação de mecanismos de segurança.

Os princípios `a, b, c, d, f, g` e `i` são melhor aplicados na topologia da figura 2.2.4, conforme pode-se ver na tabela 2.2.3.

Tabela 2.2.3: comparação de topologias.

Princípio	Figura 2.2.4	Figura 2.2.3
a) Simplicidade	Sim – cada *firewall* executa poucas funções.	Não – um *firewall* único é mais complexo.

17 Obra citada.
18 "*The Protection of Information in Computer Systems*"; Saltzer, Jerome H. e Schoeder, Michael D. ; publicado em "*Proceedings of the IEEE 63*" (pp. 1278-1308) em setembro de 1975.

Princípio	Figura 2.2.4	Figura 2.2.3
b) Segurança em caso de falha	Sim – cada *firewall* é individualmente configurado para bloquear o tráfego em caso de falha.	Talvez – dependendo do tipo de falha pode ocorrer uma violação de segurança – o *firewall* é proprietário e nem todos os detalhes de funcionamento são divulgados.
c) Defesa em profundidade	Sim – o acesso à rede local passa por três dispositivos de segurança.	Não – um *firewall* único é tudo em um.
d) Mediação completa	Sim – v. letra c.	Não – os principais serviços são executados no *firewall*.
f) Separação de privilégios	Sim – o sistema é modular, e funções específicas são executadas em módulos diferentes.	Não – é um sistema tudo em um.
g) Implementação aberta	Sim – os computadores usados são comuns e executam *software* livre.	Não – equipamentos proprietários restringem o acesso aos componentes e o seu completo entendimento.
i) Registro de ocorrências	Sim – cada *firewall* é um sistema Linux com armazenamento de *logs*.	Talvez.

Em relação aos outros princípios, é fácil ver que o “menor privilégio” (letra e) pode ser obtido em qualquer topologia, dependendo apenas de configuração. Os “mecanismos comuns reduzidos” (letra h) são melhor aplicados aos servidores da rede local. O “fator de trabalho” (letra j) é difícil de ser avaliado, pois depende do interesse de um possível atacante. A “aceitação psicológica” (letra k) depende da política de segurança do TCDF.

2.3. Sistema de armazenamento

O TCDF possui dois sistemas independentes de armazenamento: (i) um *storage HP 3Par StoreServ 7400* com capacidade nominal de 74 TiB (81,4 terabytes) e capacidade líquida de ~63,7 TiB [19] (~70 terabytes); (ii) um sistema baseado em computadores servidores de rede usando o protocolo iSCSI (por meio da ferramenta *Open iSCSI* executando em plataforma Linux) com capacidade nominal de 144 TiB (158,3 terabytes) e capacidade líquida de ~86,4 TiB[20] (~95 terabytes).

O sistema de monitoramento por câmeras de vídeo ocupa 12 TiB (~13,2 terabytes) de armazenamento para gravação das imagens, que devem ser sobrescritas depois de 20 a 24 dias. Para que seja possível armazenar as imagens por um período aproximado de seis meses é necessário alocar ~108 TiB (~118,7 terabytes), o que hoje é inviável.

19 A capacidade líquida do HP 3Par Storeserv foi estimada considerando-se que todos os volumes virtuais usam RAID-6, com capacidade líquida de ~86% da capacidade nominal. Esta é a proporção atual.

20 A capacidade líquida foi estimada considerando-se que o *storage* foi construído com duas camadas RAID-5.

O atual sistema *HP 3Par StoreServ* possui 28 unidades de disco de 2,645 TiB (2,9 terabytes) cada instaladas em dois gabinetes de disco. Cada gabinete suporta 24 unidades de disco, o que permite a instalação de mais 20 unidades de disco do tipo SAS (totalizando 48 unidades). Usando-se um modelo de quatro terabytes (~3,5 TiB), a capacidade seria aumentada em ~60,2 TiB (= 3,5 TiB x 20 x 0,86). Para aumentar mais do que isso, seria necessário adicionar mais um gaveteiro. Atualmente, o sistema conecta-se à rede local por duas portas de 10 Gbit/s – os dois canais usados permitem redundância em caso de falha.

Há dois problemas com o sistema da HP: (i) a arquitetura é proprietária, acarretando dependência do fabricante, tanto para aumento da capacidade, como para troca de componentes e manutenção; (ii) a expansibilidade é limitada – a cada 28 unidades de disco deve-se adquirir um gaveteiro, e para aumentar o desempenho da conexão (atualmente em 10 Gbit/s, com redundância) devem ser adquiridos componentes de rede também proprietários.

A figura 2.3.1 mostra a estrutura simplificada do sistema de armazenamento do TCDF, considerando-se a implementação de um terceiro *storage* (o *storage OpeniSCSI 2* na figura), usando computadores e o protocolo iSCSI.

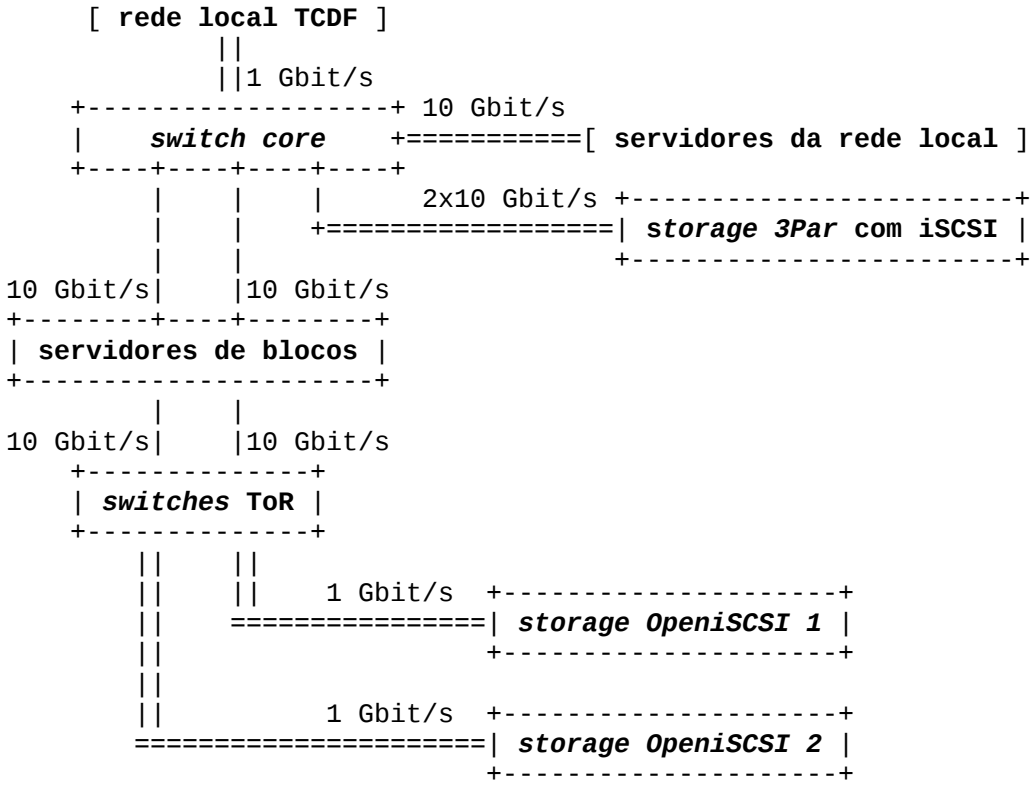


Figura 2.3.1: estrutura proposta para o sistema de armazenamento de dados.

Na figura, as linhas “ | |” e “ ===” indicam múltiplas conexões de rede. Os servidores de blocos são dois computadores (já existentes) que conectam os dispositivos de blocos do *storage* aos servidores da rede local. Cada *storage OpeniSCSI* constitui-se de um conjunto de dispositivos de blocos (denominados *iSCSI targets*).

O *storage OpeniSCSI 1* mostrado na figura constitui-se de dez computadores (dispositivos de blocos – *iSCSI targets*), divididos em dois conjuntos de cinco, onde cada conjunto forma um arranjo RAID-5. Cada computador possui quatro unidades de disco que também formam um arranjo RAID-5. Assim a capacidade de cada conjunto é de 43,2 TiB (= 3,6 TiB x (3/4) x (4/5)), e portanto a capacidade líquida total é de 86,4 TiB (2 x 43,2 TiB). Os dois conjuntos conectam-se aos dois servidores de blocos por meio de um *switch* de distribuição, mas planeja-se trocar esse *switch* por dois outros, cada um conectado a um servidor de blocos. Desse modo será obtida a mesma redundância (dois canais de 10 Gbit/s) que existe no sistema *HP 3PAR StoreServ*.

A solução baseada em computador com *Open iSCSI* é mais complexa para implementar e manter, mas possui as seguintes vantagens: (i) baseia-se em arquitetura aberta (protocolo iSCSI); (ii) utiliza *software* livre (sistema operacional Linux com a ferramenta de aplicação *Open iSCSI*); (iii) é mais flexível, pois é modular, permitindo aumento de capacidade (trocando-se os discos por discos de maior capacidade ou acrescentando-se mais conjuntos ao sistema) e aumento de desempenho (adicionando-se interfaces de rede aos dispositivos de blocos, aumentando-se o número ou a capacidade de processamento dos servidores de blocos).

A implementação de um sistema *Open iSCSI* com capacidade de ~108 TiB (suficiente para armazenamento de imagens por aproximadamente seis meses) necessita da aquisição de 12 computadores, cada um com quatro unidades de disco de 3,6 TiB cada – serão usados dois conjuntos com seis dispositivos de blocos cada um, e cada conjunto será um arranjo em RAID-5, e cada dispositivo de blocos usará as quatro unidades de disco também em um arranjo RAID-5.

Para montar a estrutura da figura 2.3.1 serão usados dois *switches*, cada um conectado a um servidor de blocos. Cada dispositivo de blocos do *storage OpeniSCSI 2* será conectado a cada *switch* usando duas portas de 1000 Mbit/s em *trunking* formando conexões de 2000 Mbit/s – cada computador com a função de dispositivo de blocos deverá possui quatro interfaces de 1000 Mbit/s. Esses *switches* também serão usados pelo *storage OpeniSCSI 1*.

3. Custo total e estimativas de preços

Para manter a coesão e simplicidade do texto, esse tópico foi dividido como o anterior. O tópico anterior tratou da análise de critérios técnicos sobre as soluções disponíveis. Neste, serão tratados aspectos financeiros.

3.1. Computadores para funcionarem como hospedeiros de VMs

Os valores da tabela 3.1.1 foram obtidos no “Banco de Preços” (vide <http://bancodeprecos.com.br/PrecosPublicos/Pesquisa>) e referem-se a equipamentos equivalentes aos que serão adquiridos.

Tabela 3.1.1: Preços de computadores para funcionarem como servidores.

Órgão e Pregão	Data	Marca e modelo	Tipo	R$ (unidade)
RR-UERR 24/2013	12/12/2013	HP Proliant DL360p	modular	20.948,00
TCDF 29/2014	26/09/2014	Dell PowerEdge R420	modular	22.412,37
MD-CE 2/2014	14/10/2014	Dell PowerEdge R620	modular	25.389,99

Órgão e Pregão	Data	Marca e modelo	Tipo	R$ (unidade)
FASI 584424	25/05/2015	Lenovo x3550 M5	modular	19.000,00
SSP-PA 18/2015	25/05/2015	Lenovo x3550 M5	modular	28.950,25
ME-CMS 11/2015	03/08/2015	Dell PowerEdge R630	modular	25.000,00

Os computadores mostrados na tabela 3.1.1 são importados (ou integrados com componentes importados) e as licitações cobrem um período aproximado de 20 meses. Assim, foi montada a tabela 3.1.2, que mostra os valores corrigidos pelo dólar dos EUA.

Tabela 3.1.2: valores estimados corrigidos pela variação do dólar (EUA) até 16/09/2015 [21].

Órgão e Pregão	Data	Marca e modelo	Tipo	R$ (unidade)
RR-UERR 24/2013	12/12/2013	HP Proliant DL360p	modular	34.523,74
TCDF 29/2014	26/09/2014	Dell PowerEdge R420	modular	35.417,08
MD-CE 2/2014	14/10/2014	Dell PowerEdge R620	modular	40.623,98
FASI 584424	25/05/2015	Lenovo x3550 M5	modular	23.384,62
SSP-PA 18/2015	25/05/2015	Lenovo x3550 M5	modular	35.631,08
ME-CMS 11/2015	03/08/2015	Dell PowerEdge R630	modular	27.906,98
Preço unitário médio (R$)				**32.914,58**

3.2. Sistema de *firewall*

3.2.1. Comparação de custos de equipamentos Dell[22]

A tabela 3.2.1 detalha o custo (em dólar dos EUA), obtido no sítio da Dell, do equipamento SonicWall NSA 3600 com os recursos necessários ao seu funcionamento como mostrado na figura 2.2.3.

Tabela 3.2.1: custo do Dell SonicWall NSA 3600 (em dólar dos EUA) [23].

Recurso	US$ para 3 anos	US$ para 6 anos
NSA 3600 com VPN SSL para 25 clientes	4.445,00	4.445,00
Anti-Spam (licença para 3 anos)	3.835,00	7.670,00
DPI-SSL (sem prazo de validade)	1.250,00	1.250,00
Anti-Virus, Anti-Spyware, IPS (licença para 3 anos)	2.109,00	4.218,00
Filtro de conteúdo (licença para 3 anos)	2.301,00	4.602,00
Valor total	**13.940,00**	**22.185,00**

21 Taxas usadas para o dólar dos EUA (<http://www4.bcb.gov.br/pec/conversao/conversao.asp>): 12/12/2013, R$ 2,33; 26/09/2014, R$ 2,43; 14/10/2014, R$ 2,40; 25/05/2015, R$ 3,12; 03/08/2015, R$ 3,44; 16/09/2015, 3,84.

22 Assim como no item 2.2 deste estudo, neste subitem serão analisados e comparados apenas equipamentos da Dell – vide nota de rodapé 8 na página 6.

23 V. <http://www.dell.com/us/business/p/sonicwall-nsa-series/fs>.

A estrutura mostrada na figura 2.2.3 necessita de dois equipamentos do modelo NSA 3600 e um equipamento mais simples – o NSA 2600, cujo valor básico é de US$ 3.960,00.

A tabela 3.2.2 lista o valor, em dólar dos EUA, obtido no sítio da Dell, dos computadores necessários à construção da estrutura mostrada na figura 2.2.4. O item 2 da tabela refere-se aos hospedeiros (um para cada *datacenter*) das máquinas virtuais na DMZ. O item 3 refere-se a um hospedeiro de menor capacidade, que seria usado na configuração da figura 2.2.3.

Tabela 3.2.2: custo de computadores Dell (em dólar dos EUA) [24].

Equipamento	US$/unid.
1) Dell PowerEdge R430 com 1 processador, 16 GiB de RAM, 2 un. disco SATA 2 Tbytes cada, 4 interfaces Gigabit, 2 interfaces de 10 Gbit/s SFP+.	3.284,95
2) Dell PowerEdge R430 com 2 processadores, 24 GiB de RAM, 2 un. disco SATA 2 Tbytes cada, 4 interfaces Gigabit, 2 interfaces de 10 Gbit/s SFP+.	4.001,51
3) Dell PowerEdge R430 com 2 processadores, 16 GiB de RAM, 2 un. disco SATA 2 Tbytes cada, 4 interfaces Gigabit, 2 interfaces de 10 Gbit/s SFP+.	3.513,67

Com os valores das tabelas 3.2.1 e 3.2.2 é possível calcular o custo total para a aquisição de equipamentos para as duas configurações. Primeiro para a estrutura da figura 2.2.3, cujos valores são mostrados na tabela 3.2.3.

Tabela 3.2.3: custo total da estrutura da figura 2.2.3.

Equipamento	US$/unid.	Quant.	US$ total
1a) Dell SonicWall NSA 3600 (6 anos)	22.185,00	2	44.370,00
1b) Dell SonicWall NSA 3600 (3 anos)	13.940,00	2	27.880,00
2) Dell SonicWall NSA 2600	3.960,00	1	3.960,00
3) Dell PowerEdge R430 (item 3, tabela 3.2.2), para VMs da DMZ.	3.513,67	2	7.027,34
Custo total para 6 anos (1a + 2 + 3)			**55.357,34**
Custo total para 3 anos (1b + 2 + 3)			**38.867,34**

A vida útil dos computadores listados na tabela 3.2.2 é de cinco a seis anos. Os valores dos equipamentos necessários à estrutura da figura 2.2.4 são mostrados na tabela 3.2.4.

Tabela 3.2.4: custo total da estrutura da figura 2.2.4.

Equipamento	US$/unid.	Quant.	US$ total
1) Dell PowerEdge R430 (item 1, tabela 3.2.2), para *firewall.*	3.284,95	5	16.424,75
2) Dell PowerEdge R430 (item 2, tabela 3.2.2), para VMs da DMZ.	4.001,51	2	8.003,02
Custo total para 5 a 6 anos			**24.427,77**

24 V. <http://www.dell.com/us/business/p/poweredge-r430/pd?~ck=anav>.

3.2.1. Comparação de valores obtidos em licitações

A tabela 3.2.5 a seguir mostra os valores propostos em licitações para computadores com configurações um pouco superiores àquelas necessárias para dispositivos de *firewall* mostrados na figura 2.2.4.

Tabela 3.2.5: valores propostos em licitações para computadores servidores de rede [25].

Órgão – nº pregão	Data	Produto	R$ (unidade)
TCDF – 29/2014	26/09/2014	Dell PowerEdge R420	13.999,95
MEC-UFV – 595/2014	07/11/2014	HP Proliant DL360e	16.740,00
MEC-UFV – 595/2014	07/11/2014	Lenovo ThinkServer RD540	17.040,00
MEC-UFV – 595/2014	07/11/2014	Dell PowerEdge R620	17.050,00
FASI – 58424	25/05/2015	Lenovo x3550 M5	19.000,00
FASI – 58424	25/05/2015	Dell PowerEdge R630	19.749,50

Corrigindo-se os valores da tabela 3.2.5 levando-se em conta a variação do dólar do EUA, o resultado é mostrado na tabela 3.2.6.

Tabela 3.2.6: valores estimados corrigidos pela variação do dólar (EUA) até 16/09/2015 [26].

Órgão e Pregão	Data	Marca e modelo	Valor corrigido (R$)
TCDF – 29/2014	26/09/2014	Dell PowerEdge R420	22.123,38
MEC-UFV – 595/2014	07/11/2014	HP Proliant DL360e	25.012,30
MEC-UFV – 595/2014	07/11/2014	Lenovo ThinkServer RD540	25.460,54
MEC-UFV – 595/2014	07/11/2014	Dell PowerEdge R620	25.475,49
FASI – 58424	25/05/2015	Lenovo x3550 M5	23.384,62
FASI – 58424	25/05/2015	Dell PowerEdge R630	24.307,08
Valor médio (R$)			**24.293,90**

As principais aquisições de *firewall* (do tipo *Next-Generation*, como o *Dell SonicWall NSA 3600*) incluem o recurso de alta disponibilidade (HA – *High Availability*). A tabela 3.2.7 mostra os valores de dois modelos de fabricantes diferentes, com alta disponibilidade e características semelhantes, que tiveram a licitação realizada em dezembro de 2014. Também foi incluído na tabela o valor obtido no PE 52/2013, realizado em outubro de 2013, cuja melhor proposta foi feita para um *firewall Dell SonicWall NSA 5600*, completo e com alta disponibilidade (HA).

Tabela 3.2.7: valores de aquisição de equipamentos para *firewall* [27].

Órgão – nº pregão	Data	Produto	Valor un. (R$)
TCDF – 52/2013	30/10/2013	Dell SonicWall NSA 5600	138.000,00
TRE-MT – 44/2014	19/12/2014	Check Point 4600	155.000,00
TCE-RO – 44/2014	22/12/2014	Palo Alto PA-3020	142.300,00

25 Pesquisa feita no Banco de Preços (<http://bancodeprecos.com.br/PrecosPublicos/Pesquisa>).
26 Taxas usadas para o dólar dos EUA (<http://www4.bcb.gov.br/pec/conversao/conversao.asp>): 26/09/2014, R$ 2,43; 07/11/2014, R$ 2,57; 25/05/2015, R$ 3,12; 16/09/2015, 3,84.
27 Pesquisa feita no Banco de Preços (<http://bancodeprecos.com.br/PrecosPublicos/Pesquisa>), com exceção da primeira linha – licitação do próprio TCDF (Processo nº 11127/2013).

Para o fabricante Dell SonicWall é possível determinar o custo relativo do recurso de alta disponibilidade, como pode-se ver na tabela 3.2.8.

Tabela 3.2.8: valores para a família Dell SonicWall com e sem HA [28].

Produto	Valor sem HA (US$)	Valor com HA (US$)	Vlr. relat.
Dell SonicWall NSA 2600	6.135,00	7.934,00	0,773
Dell SonicWall NSA 3600	13.940,00	16.737,00	0,833
Dell SonicWall NSA 5600	36.138,00	43.835,00	0,824
Média			**0,810**

Ajustando os preços contidos na tabela 3.2.7 para excluir a alta disponibilidade (por estimativa de 0,810 a partir dos valores da tabela 3.2.8) e considerando-se a variação do dólar do EUA, obtém-se os valores mostrados na tabela 3.2.9.

Tabela 3.2.9: valores estimados corrigidos – *firewall* sem HA [29].

Produto	Data da licitação	Valor original sem HA (R$)	Valor estimado 16/09/2015 (R$)
Dell SonicWall NSA 5600	30/10/2013	111.780,00	195.997,81
Check Point 4600	19/12/2014	125.550,00	181.929,06
Palo Alto PA-3020	22/12/2014	115.263,00	167.022,61
Valor médio (R$)			**181.649,83**

O modelo *NSA 5600* possui maior capacidade que o modelo NSA 3600. Na tabela 3.2.10 podem ser avaliados os valores relativos do *NSA 3600* quando comparado com o *NSA 5600*.

Tabela 3.2.10: valores para a família Dell SonicWall com e sem HA [30].

Produto	NSA 3600 (US$)	NSA 5600 (US$)	Vlr. relat.
Dell SonicWall NSA sem HA	13.940,00	36.138,00	0,386
Dell SonicWall NSA com HA	16.737,00	43.835,00	0,382
Média			**0,384**

O modelo *4600* da Checkpoint também possui uma capacidade muito superior (por exemplo, desempenho de 9 Gbit/s) às necessidades do TCDF. O modelo *4200* é mais adequado (desempenho de 3 Gbit/s). Foram obtidos os valores em dólar do EUA para os dois modelos em duas configurações, como mostrado na figura 3.2.9, para analisar o valor relativo do modelo *4200*.

Tabela 3.2.11: valores para dois modelos de *firewall* da Checkpoint [31].

Produto	4200 (US$)	4600 (US$)	Vlr. relat.
Checkpoint com pacote x	4.902,00	12.236,00	0,401

28 Disponível em <http://www.dell.com/us/business/p/sonicwall-nsa-series/fs>.
29 Taxas usadas para o dólar dos EUA (<http://www4.bcb.gov.br/pec/conversao/conversao.asp>): 30/10/2013, R$ 2,19; 19/12/2014 e 22/12/2014, R$ 2,65; 16/09/2015, R$ 3,84.
30 Disponível em <http://www.dell.com/us/business/p/sonicwall-nsa-series/fs>.
31 Valores obtidos em <http://www.checkfirewalls.com/4200.asp> e <http://www.checkfirewalls.com/4600.asp>.

Produto	4200 (US$)	4600 (US$)	Vlr. relat.
Checkpoint c/pacote x + antimalware	6.440,00	14.893,00	0,432
Média			**0,417**

Podemos agora alterar a tabela 3.2.7 para substituir, por estimativa, respectivamente, o modelo *NSA 5600* da Dell pelo modelo *NSA 3600* e o modelo *4600* da Checkpoint pelo modelo *4200*. O modelo *PA 3020* da Palo Alto, embora mais caro, foi mantido pois seu desempenho é próximo dos outros dois modelos. As estimativas são mostradas na tabela 3.2.12.

Tabela 3.2.12: valores estimados – *firewall* .

Produto	Desempenho bruto (Mbit/s)	Valor estimado 16/09/2015 (R$)
Dell SonicWall NSA 3600	3400	75.263,16
Check Point 4200	3000	75.864,41
Palo Alto PA-3020	2000	167.022,61
Valor médio (R$)		106.050,06

Agora é possível comparar as soluções com valores estimados em reais. A tabela 3.2.13 mostra três configurações: (a) cinco computadores como dispositivos de *firewall* (dois para cada *datacenter* mais um para a garagem); (b) dois dispositivos de *firewall* proprietários (um para cada *datacenter*), usando a média dos dois menores valores da tabela 3.2.12; (c) dois dispositivos de *firewall* proprietários (um para cada *datacenter*), com o valor médio da tabela 3.2.12. Estas duas últimas não incluem a garagem, para simplificar a análise.

Tabela 3.2.13: valores estimados de aquisição para configurações diferentes.

Estrutura	Valor total (R$)
a) referente à figura 2.2.4: 5 computadores como dispositivos de *firewall* (dois por *datacenter* mais um para a garagem) com o valor médio da tabela 3.2.6: R$ 24.293,90 por unidade.	121.469,50
b) referente à figura 2.2.3 sem a garagem: 2 dispositivos de *firewall* proprietário (um por *datacenter*) com o valor médio dos dois menores da tabela 3.2.12: R$ 75.563,79.	151.127,58
c) referente à figura 2.2.3 sem a garagem: 2 dispositivos de *firewall* proprietário (um por *datacenter*) com o valor médio da tabela 3.2.12: R$ 106.050,06.	212.100,12

3.3. Sistema de armazenamento

3.3.1. Comparação de custos de aquisição

A tabela 3.3.1 a seguir mostra os valores de aquisição, pelo TCDF, do *storage HP 3PAR StoreServ 7400* e de componentes que foram utilizados na implementação do *storage OpeniSCSI 1*.

Tabela 3.3.1: valores de aquisição de equipamento e componentes de *storage*. [32].

Órgão – nº pregão	Data	Produto	Valor un. (R$)
TCDF – 23/2013	21/05/2013	HP 3Par StoreServ 7400	152.000,00
TCDF – 29/2014	29/06/2014	Dell PowerEdge R420	13.999,95
TCDF – 29/2014	29/06/2014	HP Proliant DL360e	18.500,00
TCDF – 31/2014	23/10/2014	Dell Networking N3048[33]	12.000,00

Corrigindo-se os valores da tabela 3.3.1, levando-se em conta a variação do dólar do EUA, o resultado é mostra na tabela 3.3.2.

Tabela 3.3.2: valores estimados corrigidos pela variação do dólar (EUA) até 16/09/2015 [34].

Órgão e Pregão	Data	Marca e modelo	Valor corrigido (R$)
TCDF – 23/2013	21/05/2013	HP 3Par StoreServ 7400	286.117,65
TCDF – 29/2014	29/06/2014	Dell PowerEdge R420	22.123,38
TCDF – 29/2014	29/06/2014	HP Proliant DL360e	29.234,57
TCDF – 31/2014	23/10/2014	Dell Networking N3048	18.432,00

A tabela 3.3.3 mostra o custo total de aquisição dos componentes do *storage OpeniSCSI 1*, e compara com o valor do *storage HP 3Par StoreServ*. Os valores foram atualizados para 16/09/2015. Note-se que o custo por TiB da solução *Open iSCSI* é **~18,4% menor** que o do *storage HP 3Par*.

Tabela 3.3.3: valores de aquisição de equipamento e componentes de *storage*.

Produto	Valor un. (R$)	Quantidade	Valor total (R$)
Dell PowerEdge R420	22.123,38	10	221.233,80
HP Proliant DL360e	29.234,57	2	58.469,14
Dell Networking N3048	18.432,00	2	36.864,00
Valor do *storage Open iSCSI 1* (86,4 TiB => R$ 3.663,97 por TiB)			**316.566,94**
Valor do *HP 3Par StoreServ 7400* (63,7 TiB => R$ 4.491,64 por TiB)			**286.117,65**

A tabela 3.3.4 a seguir mostra os valores propostos em licitações para *switches* com a configuração adequada à implementação do sistema de armazenamento *Open iSCSI*: 48 portas de 1000 Mbit/s (1000Base-T) e pelo menos duas interfaces de 10 Gbit/s para conexão com os servidores de blocos.

32 Referentes aos seguintes processos: nº 20059/2013 (PE 23/2013); nº 16352/2014 (PE 29/2014); nº 28569/2013 (PE 31/2014).

33 Na licitação (PE 31/2014), o item correspondia a um conjunto que, no caso da proposta vencedora, constituiu-se de um *switch core* Dell Networking 4064F e um Dell Networking 3048, acompanhados de diversos componentes. O valor do modelo 3048 foi estimado em ~10% do valor de aquisição, que foi de R$ 116,999,00.

34 Taxas usadas para o dólar dos EUA (<http://www4.bcb.gov.br/pec/conversao/conversao.asp>): 21/05/2013, R$ 2,04; 26/09/2014, R$ 2,43; 23/10/2014, R$ 2,50; 16/09/2015, R$ 3,84.

Tabela 3.3.4: valores propostos para *switches* em licitações [35].

Órgão – nº pregão	Data	Produto	R$ unit.
MEC-UFMS – 96/2015	10/07/2015	HP 3800-48G-4SFP+	14.800,00
MS-F. Oswaldo Cruz – 166/2015	30/07/2015	HP 5130-48G-4SFP+	14.750,00

Corrindo-se os valores da tabela 3.3.4 levando-se em conta a variação do dólar do EUA, o resultado é mostrado na tabela 3.3.5.

Tabela 3.3.5: valores estimados corrigidos pela variação do dólar (EUA) até 16/09/2015 [36].

Órgão e Pregão	Data	Marca e modelo	R$ corrigido
MEC-UFMS – 96/2015	10/07/2015	HP 3800-48G-4SFP+	17.928,08
MS-F. Oswaldo Cruz – 166/2015	30/07/2015	HP 5130-48G-4SFP+	16.807,12
TCDF – 31/2014	23/10/2014	Dell Networking N3048	18.432,00
Valor médio (R$)			**17.722,40**

Foi incluído, na última linha da tabela, o valor estimado para o *switch Dell Networking N3048* (v. tabela 3.3.2), que é semelhante aos valores corrigidos para os dois *switches* da tabela 3.3.4.

A tabela 3.3.6 a seguir mostra os valores propostos em licitações para computadores com configurações semelhantes àquelas necessárias para dispositivos de blocos. Essa semelhança significa uma configuração parecida com a do computador Dell PowerEdge R420 adquirido pelo TCDF por meio do pregão 29/2014 por R$ 13.999,95 – v. tabela 3.3.1.

Tabela 3.3.6: valores de aquisição de computadores servidores de rede [37].

Órgão – nº pregão	Data	Produto	Valor un. (R$)
MEC-UFV – 595/2014	07/11/2014	HP Proliant DL360e	16.740,00
FASI – 58424	25/05/2015	Lenovo x3550 M5	19.000,00

Corrigindo-se os valores da tabela 3.3.6 levando-se em conta a variação do dólar do EUA, o resultado é mostrado na tabela 3.3.7. Foi também incluído o valor do computador Dell PowerEdge R420 adquirido pelo TCDF.

Tabela 3.3.7: valores estimados corrigidos pela variação do dólar (EUA) até 16/09/2015 [38].

Órgão e Pregão	Data	Marca e modelo	Valor corrigido (R$)
TCDF – 29/2014	26/09/2014	Dell PowerEdge R420	22.123,38
MEC-UFV – 595/2014	07/11/2014	HP Proliant DL360e	25.012,30
FASI – 58424	25/05/2015	Lenovo x3550 M5	23.384,62
Valor médio (R$)			**23.506,77**

35 Pesquisa feita no Banco de Preços (<http://bancodeprecos.com.br/PrecosPublicos/Pesquisa>).
36 Taxas usadas para o dólar dos EUA (<http://www4.bcb.gov.br/pec/conversao/conversao.asp>): 10/07/2015, R$ 3,17; 30/07/2015, R$ 3,37; 16/09/2015, R$ 3,84.
37 Pesquisa feita no Banco de Preços (<http://bancodeprecos.com.br/PrecosPublicos/Pesquisa>).
38 Taxas usadas para o dólar dos EUA (<http://www4.bcb.gov.br/pec/conversao/conversao.asp>): 26/09/2014, R$ 2,43; 06/11/2014, R$ 2,53; 07/11/2014, R$ 2,57; 25/05/2015, R$ 3,12; 16/09/2015, R$ 3,84.

Finalizando, a tabela 3.3.8 mostra o valor estimado para a aquisição dos componentes necessários para montar um *storage Open iSCSI* com capacidade líquida de ~108 TiB.

Tabela 3.3.8: valores estimados dos componentes de um *storage Open iSCSI*.

Equipamento	Valor un. (R$)	Quant.	Valor total (R$)
1) computador servidor de rede	23.506,77	12	282.081,24
2) *switch* ToR (2 x 10 Gbit/s + 48 x 1000 Mbit/s)	17.722,40	2	35.444,80
Valor total (R$)			**317.526,04**

4. Soluções escolhidas

4.1. Computadores hospedeiros

No processo 16352/2014 foi demonstrado que, para este perfil de computadores, a melhor escolha é pelo tipo modular. Portanto, serão adquiridos cinco computadores do mesmo tipo e configuração (um pouco melhorada) daqueles obtidos por meio daquele processo.

Cada computador terá a seguinte configuração básica:

a) gabinete horizontal com altura 1U para *rack* de 19 polegadas;

b) dois processadores, cada um com oito núcleos (não serão computados núcleos derivados do *hyperthreading*);

c) 64 GiB de memória, em quatro módulos de 16 GiB (dois módulos por processador) ou oito módulos de 8 GiB (quatro módulos por processador);

d) duas unidades de disco rígido SATA de de 3,5” (LFF – *Large Form Factor*), cada uma com capacidade nominal de quatro terabytes;

e) duas interfaces de rede de 10 Gbit/s, com conector SFP+;

f) duas interfaces de rede de 1000 Mbit/s padrão 1000Base-T;

g) um par de fontes redundantes.

4.2. Computadores para dispositivos de *firewall*

Observando-se os itens 2.2 e 3.2, conclui-se que um sistema de segurança para a rede local usando computadores como dispositivos de *firewall* em camadas é mais vantajoso, tanto no aspecto técnico como financeiro. Portanto, serão adquiridos cinco computadores, que serão configurados como dispositivos de *firewall*, cada um com a seguinte configuração básica:

a) gabinete horizontal com altura 1U para *rack* de 19 polegadas;

b) um processador com seis núcleos (não serão computados núcleos derivados do *hyperthreading*);

c) 16 GiB de memória, em dois módulos de 8 GiB ou quatro módulos de 4 GiB – não será aceito um único módulo de 16 GiB;

d) duas unidades de disco rígido SATA de de 3,5” (LFF – *Large Form Factor*), cada uma com capacidade nominal de dois terabytes;

e) duas interfaces de rede de 10 Gbit/s, com conector SFP+;

f) quatro interfaces de rede de 1000 Mbit/s no padrão 1000Base-T;

g) um par de fontes redundantes.

4.3. Sistema de armazenamento

4.3.1. Computadores para dispositivos de blocos

Como foi demonstrado nos itens 2.3 e 3.3 deste documento, um *storage Open iSCSI* montado possui vantagens técnicas e econômicas sobre o *storage HP 3Par StoreServ 7400* que o TCDF possui. Portanto, serão adquiridos os componentes para sua implementação, consistindo de 12 computadores com perfil de servidores de rede, cada um com a seguinte configuração básica:

a) gabinete horizontal com altura 1U para *rack* de 19 polegadas;

b) um processador com quatro núcleos (não serão computados núcleos derivados do *hyperthreading*);

c) oito GiB de memória, em um módulo de 8 GiB ou dois módulos de 4 GiB;

d) quatro unidades de disco rígido SATA de de 3,5” (LFF – *Large Form Factor*), cada uma com capacidade nominal de quatro terabytes;

e) quatro interfaces de rede de 1000 Mbit/s no padrão 1000Base-T;

f) um par de fontes redundantes.

4.3.2. Switches de distribuição

Serão adquiridos também dois *switches*, cada um com a seguinte configuração básica:

a) gabinete horizontal com altura 1U para *rack* de 19 polegadas;

b) 48 portas de 1000 Mbit/s, padrão 1000Base-T;

c) duas interfaces de 10 Gbit/s, tipo SFP+;

d) um par de fontes redundantes.

5. Benefícios esperados

Com a compra dos computadores para os dois sítios será possível montar um ambiente duplicado de forma que se possa realizar a redundância de todos os serviços de rede, incluindo os sistemas da intranet (como e-TCDF, SINJ, SIRAC), de suporte ao usuário (como servidor de impressão, serviço de autenticação, antivírus) e para os serviços básicos de infraestrutura (como serviço de nomes, e-mail, *proxy*).

A compra dos *firewalls* substituirá as antigas máquinas de mesa e deverá ter uma durabilidade e confiabilidade superior, diminuindo a indisponibilidade da Internet e serviço da DMZ (zona desmilitarizada).

Um novo sistema de armazenamento de dados permitirá a gravação e recuperação de imagens do sistema de monitoramento por câmeras de vídeo por um período de até seis meses.

6. Necessidade de adequação do ambiente

No que for necessário, a própria solução já fará a adequação necessária no ambiente. Os equipamentos adquiridos serão instalados em *racks* já existentes com toda a infraestrutura já disponível (ar-condicionado, quadros de energia, canaletas, cabos elétricos na bitola adequada, etc).

7. Demais requisitos

7.1. Capacitação: a(s) empresa(s) contratada(s) deverá(ão) transmitir o conhecimento necessário para que a equipe do Serviço de Infraestrutura da DTI possa operar e, se necessário, reconfigurar os equipamentos.

7.2. Legais: não se aplica.

7.3. Manutenção: os equipamentos deverão possuir uma garantia mínima de 36 meses, com suporte *on site* e cobrindo todos os componentes, mão de obra e transporte.

7.4. Temporal: após a entrega dos equipamentos, o(s) fornecedor(es) deverá(ão) colocá-los em operação em até 15 dias, contados da solicitação do TCDF.

7.5. Segurança: o acesso dos técnicos da Contratada às dependências do TCDF deverá ser sempre com acompanhamento de pessoal do TCDF.

7.6. Sociais, ambientais, culturais: Não se aplica.

8. Análise de Riscos

8.1. Identificação dos principais riscos[39] e danos potenciais

Cumprindo com o disposto no artigo 13 da IN 04 de 2014, serão analisados os riscos inerentes a três situações distintas relacionadas a este processo de contratação:

- durante a fase de licitação (até a assinatura do contrato);
- durante a execução do contrato;
- decorrentes do não atendimento às necessidades e demandas de informática que originaram este processo.

8.1.1. Na fase de licitação:

8.1.1.1. morosidade no processo licitatório;

8.1.1.2. irregularidades no processo licitatório;

8.1.1.3. fracasso do processo licitatório ou não assinatura do contrato.

8.1.2. Na gestão contratual:

8.1.2.1. atraso no fornecimento do objeto;

39 Risco: (1) “possibilidade de perigo, incerto mas previsível, com ameaça de dano a pessoa ou a coisa” - Michaelis, disponível em <http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=risco>; (2) “a probabilidade de acontecer uma situação adversa ou dano e as consequências deste mesmo” - EUFIC, disponível em <http://www.eufic.org/article/pt/seguranca-e-qualidade-alimentar/comunicacao-de-riscos/artid/O-que-e-a-analise-de-risco/>.

8.1.2.2. os equipamentos fornecidos não possuem todas as funcionalidades exigidas no edital;

8.1.2.3. inexecução total ou parcial do contrato;

8.1.3. Não atendimento às necessidades da contratação:

8.1.3.1. os equipamentos adquiridos não suportam a demanda ou não possuem todas a funcionalidades necessárias ao atendimento da demanda;

8.1.3.2. ausência de suporte técnico e manutenção durante a vida útil dos equipamentos (após o encerramento de contrato de suporte e manutenção).

8.2. Tabelas

Tabela 8.2.1 - risco de ocorrência de eventos[40].

Probabilidade (Risco referencial)	Observações
Alta	A probabilidade de ocorrer é grande.
Média	As chances de ocorrer ou não são equivalentes.
Baixa	A probabilidade de ocorrer é pequena.

Tabela 8.2.2 - avaliação do impacto.

Impacto	Observações
Muito grande	Perda do recurso orçamentário; má aplicação de recursos públicos; indisponibilidade de todos os serviços ou perda de dados.
Grande	Perda do processo licitatório; degradação crítica do desempenho, indisponibilidade ou falhas graves em vários serviços, em algum(ns) serviço(s) essencial(is) ou equipamentos.
Moderado	Degradação moderada do desempenho ou falhas contornáveis de alguns serviços, em um serviço essencial ou equipamentos.
Pequeno	Degradação leve do desempenho ou falhas contornáveis em serviços não essenciais.
Muito pequeno	Degradação leve do desempenho em um serviço não essencial.

8.3. Análise qualitativa dos riscos

Tabela 8.3.1 – análise qualitativa dos riscos.

Id. risco	Descrição do risco	Probabilidade de ocorrência	Impacto
8.1.1.1	Morosidade no processo licitatório	Média	Moderado
8.1.1.2	Irregularidades no processo licitatório	Média	Grande
8.1.1.3	Fracasso do processo licitatório ou não assinatura do contrato	Baixa	Grande

40 Adaptado de “Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação” v. 1.0, 2012; Tribunal de Contas da União. Disponível em <http://www.tcu.gov.br>.

Id. risco	Descrição do risco	Probabilidade de ocorrência	Impacto
8.1.2.1	Atraso no fornecimento do objeto	Média	Moderado
8.1.2.2	Os equipamentos fornecidos não possuem todas as funcionalidades exigidas no edital	Baixa	Grande
8.1.2.3	Inexecução total ou parcial do contrato	Média	Grande
8.1.3.1	Os equipamentos adquiridos não suportam a demanda ou não possuem todas a funcionalidades necessárias ao atendimento da demanda	Baixa	Muito grande
8.1.3.2	Ausência de suporte técnico e manutenção durante a vida útil dos equipamentos (após o encerramento de contrato de suporte e manutenção)	Baixa	Muito grande

8.4. Ações de mitigação

Tabela 8.4.1 – ações para mitigação dos riscos.

Id. risco	Ações de mitigação	Responsáveis pelas ações de mitigação	Período de execução das ações (de acordo com as fases previstas na IN 04/2014 – SLTI)
8.1.1.1	• Estabelecer prazos para a entrega de determinados documentos; • Acionar as áreas envolvidas na contratação quando se verificar demora demasiada em determinada fase; • Atender com presteza as demandas relacionadas ao processo licitatório; • Solicitar reuniões com os envolvidos para alinhar pontos da contatação.	Integrante requisitante Integrante técnico Integrante administrativo Ocupantes de cargos com poder de decisão	Planejamento da contratação Seleção do fornecedor
8.1.1.2	• Seguir a legislação relacionada às contratações em geral e contratações de bens e serviços de tecnologia da informação; • Manter relação estritamente profissional com representantes comerciais, com a finalidade de obter estimativas de preços, conhecer produtos e suas funcionalidades; • Atender as recomendações do controle interno; • Agir com transparência e velar pela aplicação dos princípios norteadores da Administração Pública.	Integrante requisitante Integrante técnico Integrante administrativo Ocupantes de cargos com poder de decisão	Planejamento da contratação Seleção do fornecedor Gestão do contrato

Id. risco	Ações de mitigação	Responsáveis pelas ações de mitigação	Período de execução das ações (de acordo com as fases previstas na IN 04/2014 – SLTI)
8.1.1.3	• Seguir a legislação relacionada às contratações em geral e contratações de bens e serviços de tecnologia da informação; • Proceder à especificação dos itens de forma que a maior quantidade possível de licitantes possa participar do certame; • Seguir o trâmite administrativo para aprovação de documentos referentes à contratação. • Convocar, dentro do prazo e condições estabelecidas, o interessado para assinar o termo de contrato.	Integrante requisitante Integrante técnico Integrante administrativo Ocupantes de cargos com poder de decisão	Planejamento da contratação Seleção do fornecedor
8.1.2.1	• Estabelecer um prazo razoável para entrega dos objetos licitados; • Estabelecer penalizações por atrasos, como, por exemplo, multa de mora, na forma prevista no instrumento convocatório ou no contrato.	Integrante requisitante Gestor	Planejamento da contratação Gestão do contrato
8.1.2.2	• Apenas proceder ao recebimento definitivo após realizar os testes necessários com os equipamentos recebidos e atestar que todas as funcionalidades exigidas no edital estão presentes.	Integrante técnico	Gestão do contrato
8.1.2.3	• Acompanhar e fiscalizar a execução do contrato; • Proceder aos pagamentos devidos pela Administração; • Liberar os locais para a execução dos serviços, nos prazos contratuais; • Em casos específicos, rescindir o contrato e aplicar as penalidades previstas em lei ou regulamento.	Integrante requisitante Integrante administrativo Integrante técnico Ocupantes de cargos com poder de decisão	Gestão do contrato
8.1.3.1	• Realizar os estudos técnicos preliminares para obter e atender às necessidades do órgão; • Realizar reuniões com as áreas interessadas a fim de obter suas necessidades.	Integrante técnico Integrante requisitante	Planejamento da contratação
8.1.3.2	• Estabelecer, no edital, que haja suporte técnico e	Integrante requisitante	Planejamento da contratação

Id. risco	Ações de mitigação	Responsáveis pelas ações de mitigação	Período de execução das ações (de acordo com as fases previstas na IN 04/2014 – SLTI)
	manutenção para os equipamentos adquiridos.	Integrante técnico	

Brasília, 18 de setembro de 2015.

Equipe de planejamento

Área	Nome	Matrícula
Requisitante	Angelo Shimabuko	1208-4
Informática	Luiz Antônio Moreira Serrado Ribeiro	1512-3
Administrativa	Oswaldo Junqueira Vaz Júnior	8117-9