MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA
INSTITUTO MILITAR DE ENGENHARIA
CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

Cap DIOGO PACHECO SALAZAR ARAUJO
1º Ten LEONARDO SILVA DE MELO
1º Ten RAFAEL HIPÓLITO DE FARIAS

PROJETO DE REDE E DATA CENTER COM SEGURANÇA PARA INSTITUIÇÕES DE ENSINO DO EXÉRCITO BRASILEIRO

Rio de Janeiro
2019

INSTITUTO MILITAR DE ENGENHARIA

Cap DIOGO PACHECO SALAZAR ARAUJO
1º Ten LEONARDO SILVA DE MELO
1º Ten RAFAEL HIPÓLITO DE FARIAS

PROJETO DE REDE E DATA CENTER COM SEGURANÇA PARA INSTITUIÇÕES DE ENSINO DO EXÉRCITO BRASILEIRO

Projeto de Fim de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Engenheiro de Computação.

Orientador: Prof. Marcelo Figueira de Vasconcelos - D.Sc.
Co-Orientador: Prof. Humberto Henriques de Arruda - M.Sc.

Rio de Janeiro
2019

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80 - Praia Vermelha
Rio de Janeiro - RJ CEP 22290-270

ARAUJO, DIOGO PACHECO SALAzAR
Projeto de Rede e Data Center com Segurança para Instituições de Ensino do Exército Brasileiro / DIOGO PACHECO SALAzAR ARAUJO, LEONARDO SILVA DE MELO, RAFAEL HIPÓLITO DE FARIAS, orientado por Marcelo Figueira de Vasconcelos e Humberto Henriques de Arruda - Rio de Janeiro: Instituto Militar de Engenharia, 2019.

78p.: il.

Projeto de Fim de Curso (graduação) - Instituto Militar de Engenharia, Rio de Janeiro, 2019.

1. Curso de Graduação em Engenharia de Computação - projeto de fim de curso. 1. Data Center. 2. Virtualização. 3. Escolas Militares. I. de Vasconcelos, Marcelo Figueira . II. de Arruda, Humberto Henriques . III. Título. IV. Instituto Militar de Engenharia.

INSTITUTO MILITAR DE ENGENHARIA

Cap DIOGO PACHECO SALAZAR ARAUJO
1° Ten LEONARDO SILVA DE MELO
1° Ten RAFAEL HIPÓLITO DE FARIAS

PROJETO DE REDE E DATA CENTER COM SEGURANÇA PARA INSTITUIÇÕES DE ENSINO DO EXÉRCITO BRASILEIRO

Projeto de Fim de Curso apresentado ao Curso de Graduação em Engenharia de Computação do Instituto Militar de Engenharia, como requisito parcial para a obtenção do título de Engenheiro de Computação.

Orientador: Prof. Marcelo Figueira de Vasconcelos - D.Sc.

Co-Orientador: Prof. Humberto Henriques de Arruda - M.Sc.

Aprovado em 10 de Outubro de 2019 pela seguinte Banca Examinadora:

Prof. Marcelo Figueira de Vasconcelos - D.Sc. do IME - Presidente

Prof. Humberto Henriques de Arruda - M.Sc. do IME

Prof. Leandro de Mattos Ferreira - M.Sc. do IME

Profª. Gabriela Moutinho de Souza Dias - D.Sc. do IME

Rio de Janeiro
2019

Ao Instituto Militar de Engenharia, alicerce da nossa formação e aperfeiçoamento.

AGRADECIMENTOS

Agradecemos à todas as pessoas que nos incentivaram, apoiaram e possibilitaram esta oportunidade de ampliar nossos horizontes.

Aos familiares, cônjuge e mestres.

Em especial ao nosso Professor Orientador Major Marcelo Figueira de Vasconcelos e ao Professor Co-orientador Major Humberto Henriques de Arruda, por suas disponibilidades e atenções.

“A persistência é o caminho do êxito. ”

CHARLES CHAPLIN

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

AHJ	Authority Having Jurisdiction
AMAN	Academia Militar das Agulhas Negras
CBPF	Centro Brasileiro de Pesquisas Físicas
DCT	Departamento de Ciência e Tecnologia
DMZ	Demilitarized Zone
EB	Exército Brasileiro
EsAO	Escola de Aperfeiçoamento de Oficiais
EsACosAAe	Escola de Artilharia de Costa e Antiáerea
ECEME	Escola de Comando e Estado-Maior do Exército
EsFCEx	Escola de Formação Complementar do Exército
EsPCEx	Escola Preparatória de Cadetes do Exército
EsSEx	Escola de Saúde do Exército
EsSLog	Escola de Sargentos de Logística do Exército
ESA	Escola de Sargentos das Armas
HVAC	Heating, Ventilation and Air Conditioning
IDC	Internet Data Center
IME	Instituto Militar de Engenharia
IPS	Intrusion Prevention System
LACP	Link Aggregation Control Protocol
MZ	Militarized Zone
PDC	Private Data Center
ToR	Top Of the Rack

RESUMO

O uso de dados e sistemas computacionais vem crescendo cada vez mais e conquistando mais importância para empresas e instituições. É muito importante que instituições de ensino do Exército Brasileiro tenham a capacidade de manter e operar internamente seus próprios sistemas e base de dados. Outro processo relevante é a virtualização dos servidores ganhando assim maior eficiência de desempenho e espaço físico. Assim, este projeto propõe uma solução de interconexão de redes e Data Center voltado para instituições de ensino do Exército Brasileiro, que atenda às necessidades relacionadas a segurança, alta disponibilidade, redundância, escalabilidade, número de usuários variável, sistemas *web*, alto número de dispositivos móveis, utilização de videoconferência e ligações entre grandes distâncias.

ABSTRACT

The use of data and computer systems has been growing more and more important for companies and institutions. It is very important that Brazilian Army educational institutions have the capacity to maintain and operate their own systems and database internally. Another relevant process is the virtualization of the servers thus gaining greater performance efficiency and physical space. Thus, this project proposes a network and Data Center interconnection solution aimed at Brazilian Army education institutions, which meets the needs related to security, high availability, redundancy, scalability, number of users variable, web systems, high number of mobile devices, use of videoconferencing and connections between large distances.

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO

O Operador Nacional do Sistema Elétrico (ONS), controle de tráfego aéreo, tráfego urbano, sistema bancário, serviços de segurança, programas e sistemas de empresas são apenas alguns exemplos de aplicações de sistemas de tecnologia da informação presentes na sociedade. Todos esses serviços encontram-se em centros de processamento de dados, os Data Centers, que tornam o processamento e armazenamento de dados mais eficiente em termos de controle, segurança, personalização e responsividade.

Pela sua importância para o funcionamento dos serviços, os centros de processamento de dados requerem aspectos fundamentais para o atendimento das necessidades dos usuários. O modelo de nuvem e *cloud computing* permite a utilização de diversos tipos de aplicações. *Cloud computing* é um conjunto de recursos virtuais usáveis e acessíveis. Esses recursos podem ser dinamicamente reconfigurados para se ajustarem a uma carga variável, otimizando recursos. Assim, são exigidas arquiteturas específicas e diferentes para essas aplicações, evidenciando a necessidade de criar mecanismos flexíveis e escaláveis (VERDI et al., 2010).

Outras vertentes também se mostram extremamente relevantes para um projeto de Data Center. A garantia de disponibilidade para sistemas críticos, confiabilidade dos dados, desempenho e custo são fatores que devem ser considerados nesse processo (VERDI et al., 2010). Além de aspectos técnicos, um Data Center conta com diversas especificidades físicas como por exemplo sistema de geração de energia elétrica, arquitetura e planejamento da sala, sistema de refrigeração, sistema de detecção de incêndio, gerenciamento e monitoramento de entrada e saída de pessoal, índices adequados de temperatura e umidade para o funcionamento ótimo dos componentes, cabeamento específico (ZUCCHI; AMÂNCIO, 2013).

Com o aumento contínuo do volume e tráfego de dados, o número de pesquisas para desenvolver arquiteturas de Data Centers mais eficientes também vem crescendo. Há um desafio especial na questão de desenvolvimento sustentável e economia de energia, pois o centro de processamento de dados deve funcionar ininterruptamente para prover disponibilidade ao usuário (FRIGO, 2015). Ainda nessa área, há propostas de utiliza-

ção de energia renovável com uma integração de desempenho do Data Center com redes inteligentes (WIERMAN et al., 2014).

Os Data Centers podem basicamente ser de dois tipos: Data Center Privado (PDC) ou Internet Data Center (IDC). No primeiro caso, pertencem e são operados por instituições ou agências governamentais para aplicações na internet e armazenam dados de processamento internos. Já o IDC é responsável pelo serviço de hospedagem de sites, serviço de conexão de internet e armazenamento de conteúdo. São gerenciados por um provedor de serviço de telecomunicações (COMSTOR, 2013).

1.2 MOTIVAÇÃO

O Exército Brasileiro é uma instituição com características ímpares e peça fundamental da nossa nação. Carrega um enorme número e fluxo de dados diariamente dos mais variados tipos, demandando robustez e eficiência de seus sistemas de tecnologia de informação. Existem sistemas internos, externos, sigilosos, sistemas altamente críticos para o cumprimento das missões, sistemas estratégicos social e politicamente, dentre outros. Assim, devem oferecer o máximo dos princípios de segurança da informação. Aliado a isso, existem diversos regulamentos, normas, portarias com requisitos que devem ser atendidos.

Essa realidade não é diferente em suas escolas de formação e é inevitável a necessidade de Data Centers que ofereçam desempenho e modernidade desejados para a realização das tarefas dessas organizações militares. Assim, o desenvolvimento de um projeto unificado de Data Center que tenha como base as especificidades das normas do Exército Brasileiro aliadas aos requisitos técnicos necessários para o cumprimento das necessidades das instituições de ensino do Exército, promovendo disponibilidade, confiabilidade, flexibilidade, escalabilidade, desempenho, custo controlado e melhores práticas de implementação é de extrema importância para o futuro tecnológico brasileiro.

1.3 OBJETIVO

O objetivo do presente projeto consiste em fornecer materiais de dimensionamento, infraestrutura, arquitetura e monitoramento necessários para um projeto de Data Center aplicável a todas as instituições de ensino do Exército Brasileiro, levando em consideração suas especificidades. O projeto de um centro de processamento de dados trata toda a parte de *hardware* e *software*, seguindo normas mundiais de Data Centers e do Exército Brasileiro.

1.4 METODOLOGIA

A primeira etapa do desenvolvimento do projeto consistiu em analisar toda a infraestrutura física de um Data Center através de normas e padrões militares e civis e toda a parte de software dos componentes do sistema. Definida toda a arquitetura do projeto, os componentes foram instalados fisicamente. Os equipamentos utilizados foram dois *switches*, um *storage*, um *firewall* e dois servidores. Ademais, conceitos de virtualização, sistemas distribuídos, projeto de rede e configuração de servidor também foram apresentados. Após isso, as atividades foram destinadas a realização de monitoramento, autenticação e *backup* do Data Center.

Assim, temos um modelo reduzido de Data Center seguindo a metodologia construída no projeto com as configurações de hardware e software implementadas além de um documento com esse modelo para ser replicado e ampliado nas instituições de ensino do Exército Brasileiro.

1.5 ESTRUTURA

O documento está estruturado da seguinte forma: o capítulo 2 aborda as referências teóricas de normas, *hardware* e *software* necessários no projeto. O capítulo 3 trata do processo de virtualização utilizado e componentes do Data Center. No capítulo 4 temos o projeto físico, lógico, serviços de Tecnologia da Informação e os clientes. O capítulo 5 aborda o dimensionamento do Data Center de acordo com características dos componentes, serviços e das organizações militares. No capítulo 6, temos toda a parte de monitoramento do Data Center. No capítulo 7, apresentamos as considerações finais, conclusão do trabalho e sugestão para continuidade do projeto. E por fim, no capítulo 8, estão as referências utilizadas para a realização deste projeto.

2 REFERÊNCIA TEÓRICA

Para a compreensão do processo de planejamento e levantamento de um Data Center no âmbito militar é necessário introduzir alguns conceitos relativos às tecnologias e as normas gerais e específicas que definem o comportamento de um Data Center no Exército Brasileiro.

2.1 INFRAESTRUTURA DE TELECOMUNICAÇÕES DE DATA CENTERS E SALAS DE COMPUTADORES

Na presente seção, serão abordadas especificações técnicas de infraestrutura de Data Center e salas de computadores.

2.1.1 GERAL

O TIA-942 é a norma que especifica os requisitos mínimos para infraestrutura de telecomunicações de Data Centers e salas de computadores, incluindo Data Centers corporativos com um único inquilino e Data Centers de hospedagem de internet com vários inquilinos. A topologia proposta neste documento destina-se a ser aplicável a qualquer tamanho de Data Center (ASSOCIATION et al., 2006).
Existem outras normas como por exemplo a ANSI/BICSI-002 (*Data Center Design and Implementation Best Practices*) Projeto de Data Center e Melhores Práticas de Implementação, de março de 2011, que classifica o Data Center em cinco níveis de acordo com sua disponibilidade, de F0 a F4, a classe com menos e mais tolerância a falhas, respectivamente.
Porém, a norma mais utilizada atualmente é a TIA-942, que é a única que trabalha com o conceito de Tiers para classificar um Data Center.

2.1.2 FATORES QUE DEVEM SER CONSIDERADOS AO PLANEJAR O DESIGN DE UM DATA CENTER

As etapas do processo de *design* descritas abaixo se aplicam ao *design* de um novo Data Center ou à expansão de um Data Center existente. É essencial para ambos os casos que o projeto do sistema de cabeamento de telecomunicações, a planta baixa do equipamento, os

planos elétricos, o plano arquitetônico, o HVAC, a segurança e os sistemas de iluminação sejam coordenados (ASSOCIATION et al., 2006). Idealmente, o processo deve ser:

a) Estimar os requisitos de telecomunicações, espaço, energia e resfriamento de equipamentos do Data Center com capacidade total. Antecipar as tendências futuras de telecomunicações, energia e resfriamento durante a vida útil do Data Center.

b) Fornecer espaço, energia, resfriamento, segurança, carregamento de piso, aterramento, proteção elétrica e outros requisitos das instalações para arquitetos e engenheiros. Fornecer requisitos para o centro de operações, doca de carregamento, sala de armazenamento, áreas de preparação e outras áreas de suporte.

c) Coordenar os planos preliminares dos centros de dados do arquiteto e engenheiros. Sugerir alterações conforme necessário.

d) Criar uma planta baixa de equipamentos, incluindo a colocação de grandes salas e espaços para salas de entrada, principais áreas de distribuição, áreas de distribuição horizontal, áreas de distribuição de zonas e áreas de distribuição de equipamentos. Fornecer aos engenheiros os requisitos esperados de energia, refrigeração e carregamento do piso para o equipamento. Fornecer requisitos para vias de telecomunicações.

e) Obter um plano atualizado de engenheiros com vias de telecomunicações, equipamentos elétricos e equipamentos mecânicos adicionados à planta baixa do Data Center em capacidade total.

f) Projetar o sistema de cabeamento de telecomunicações com base nas necessidades do equipamento a ser localizado no Data Center.

A Figura 2.1 ilustra os principais espaços de um Data Center típico e como eles se relacionam entre si e com os espaços fora do Data Center.

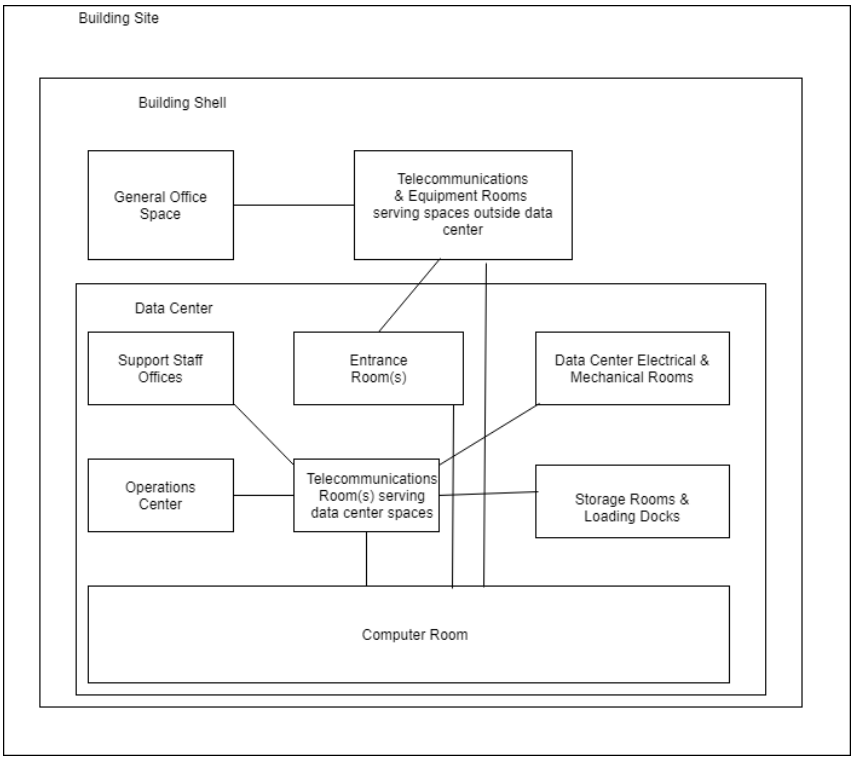

FIG. 2.1: Relacionamento de espaços em um Data Center.
Fonte: Association et al. (2006)

2.2 TIERING

A norma TIA-942 inclui quatro níveis relacionados a vários níveis de disponibilidade da infraestrutura da instalação do Data Center. Níveis mais altos não só correspondem a maior disponibilidade, mas também levam a maiores custos de construção. Em todos os casos, os níveis classificados mais altos incluem os requisitos de níveis inferiores, a menos que especificado de outra forma.

Um Data Center pode ter classificações de nível diferentes para diferentes partes de sua infraestrutura. Por exemplo, um Data Center pode ser classificado como nível 3 para elétrico, mas nível 2 para mecânico. No entanto, a classificação geral de nível do Data Center é igual à classificação mais baixa em todas as partes de sua infraestrutura. Assim, um Data Center classificado como nível 4 para todas as partes de sua infraestrutura, exceto elétrica, onde é classificado como nível 2, é classificado como nível 2 geral. A classificação geral para o Data Center é baseada em sua mais fraca componente.

Deve-se tomar cuidado para manter a capacidade do sistema mecânico e elétrico no nível correto à medida que a carga do Data Center aumenta com o tempo. Um Data Center pode ser degradado do nível 3 ou nível 4 para o nível 1 ou nível 2, pois a

capacidade redundante é utilizada para suportar novos computadores e equipamentos de telecomunicações.

Um Data Center deve atender aos requisitos especificados na norma para ser classificado em qualquer nível de camada. Embora o conceito de camadas seja útil para estratificar os níveis de redundância em vários sistemas de Data Center, é bem possível que as circunstâncias possam exigir que alguns sistemas sejam de níveis mais altos do que outros. Por exemplo, um centro de dados localizado onde a energia elétrica da concessionária é menos confiável do que a média pode ser projetado com um sistema elétrico de nível 3, mas apenas sistemas mecânicos de nível 2. Os sistemas mecânicos podem ser aprimorados com peças de reposição para ajudar a garantir um MTTR baixo (tempo médio de reparo).

Também deve ser notado que fatores humanos e procedimentos operacionais também podem ser muito importantes. Portanto, a confiabilidade real de dois Data Centers de nível 3 pode ser bem diferente. Mais informações sobre Tier são encontradas no Anexo B.

2.2.1 VISÃO GERAL DA REDUNDÂNCIA

Pontos únicos de falha devem ser eliminados para melhorar a redundância e a confiabilidade, tanto no Data Center quanto na infraestrutura de suporte, bem como nos serviços externos e nos suprimentos de utilitários. A redundância aumenta a tolerância a falhas e a facilidade de manutenção. A redundância deve ser abordada separadamente em cada nível de cada sistema.

- Redundância de base N
  O sistema atende aos requisitos básicos e não possui redundância.

- Redundância N + 1
  A redundância N + 1 fornece uma unidade adicional, módulo, caminho ou sistema, além do mínimo necessário para satisfazer o requisito base. A falha ou manutenção de qualquer unidade, módulo ou caminho único não interromperá as operações.

- Redundância N + 2
  A redundância N + 2 fornece duas unidades, módulos, caminhos ou sistemas adicionais, além do mínimo necessário para satisfazer o requisito base. A falha ou manutenção de duas unidades, módulos ou caminhos únicos não interromperá as operações.

- Redundância 2N

  A redundância 2N fornece duas unidades, módulos, caminhos ou sistemas completos para cada um dos requisitos necessários para um sistema básico. A falha ou manutenção de uma unidade, módulo, caminho ou sistema inteiro não interromperá as operações.

- Redundância 2(N + 1)

  A redundância 2 (N + 1) fornece duas unidades completas (N + 1), módulos, caminhos ou sistemas. Mesmo em caso de falha ou manutenção de uma unidade, módulo, caminho ou sistema, alguma redundância será fornecida e as operações não serão interrompidas.

- Capacidade de manutenção e teste simultâneos

  As instalações devem ser capazes de serem mantidas, atualizadas e testadas sem interrupção das operações.

- Capacidade e escalabilidade

  Data Centers e infraestrutura de suporte devem ser projetados para acomodar o crescimento futuro com pouca ou nenhuma interrupção nos serviços.

- Isolamento

  Os Data Centers devem (onde for prático) ser utilizados apenas para os fins a que se destinam e devem ser isolados de operações não essenciais.

2.3 NORMAS E LEIS ADICIONAIS

Esta subseção apresenta normas e legislações, que contêm informações relevantes sobre características técnicas, segurança da informação e comunicações. Destacam-se por seu conteúdo relevante, a Instrução Geral 01.014, do Exército Brasileiro, que trata da segurança da informação no âmbito do EB, e a Instrução Normativa, nº 2, de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. Outras informações relevantes podem ser encontradas nos seguintes trabalhos:

- Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro (EB10-IG-01.014);

- Lei nº 8.159, de 8 de janeiro de 1991 - Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;
- Medida Provisória nº 2.200-2, de 24 de agosto de 2001 - Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências;
- Decreto nº 3.505, de 13 de junho de 2000 - Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- Decreto nº 3.865, de 13 de julho de 2001 - Estabelece requisito para contratação de serviços de certificação digital pelos Órgãos Públicos Federais e dá outras providências;
- Decreto nº 3.996, de 31 de outubro de 2001 - Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;
- Decreto nº 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- Instrução Normativa GSI/PR nº 1, de 18 de junho de 2008 - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
- Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013 - Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal, e suas Normas Complementares;
- Instrução Normativa GSI/PR nº 3, de 6 de março de 2013 - Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal, e suas Normas Complementares;
- Instruções Reguladoras de Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro - IRASEG (IR 13 - 09)
- Portaria Normativa nº 0215-MD, de 27 de março de 2001 - Dispõe sobre a Política para o Sistema Militar de Comando e Controle;

- Portaria Normativa nº 3.389-MD, de 21 de dezembro de 2012 - Dispõe sobre a Política Cibernética de Defesa;
- Portaria do Comandante do Exército nº 11, de 10 de janeiro de 2001 - Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos no Exército Brasileiro;
- Portaria do Comandante do Exército nº 445, de 14 de junho de 2010 - Aprova a Diretriz Estratégica Organizadora do Sistema de Informação do Exército e dá outras providências;
- Portaria do Comandante do Exército nº 508, de 25 de junho de 2013 - Aprova as Instruções Gerais do Ciclo de Vida de Software (EB10-IG-01.006), 1ª Edição, 2013, e dá outras providências;
- Manual de Campanha MC 30-3 - Ramo Contrainteligência;
- ABNT NBR ISO/IEC 27001:2013 - Sistemas de gestão de segurança da informação - Requisitos; e
- ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação.

2.4 DISPOSITIVOS E COMPONENTES DO SISTEMA

No presente tópico, serão apresentados dispositivos e sistemas presentes no projeto de um data center com suas respectivas funcionalidades e aplicações.

2.4.1 *DEMILITARIZED ZONE* (DMZ) E *MILITARIZED ZONE* (MZ)

A *Demilitarized Zone* (DMZ) consiste em uma sub-rede situada entre uma rede confiável e uma rede não confiável. Tipicamente, a divisão entre uma LAN e a Internet. É um meio de segurança que atua física e logicamente. Dessa maneira, há um controle de acesso eficaz fazendo com que o tráfego entre servidores corporativos e *web* estejam isolados por um *firewall* e pela DMZ.

A arquitetura pode ser feita com um *firewall* (*Single Firewall*) ou mais de um (*Multiple Firewall*). No segundo caso, um *firewall* é utilizado para direcionar somente o tráfego da rede não confiável para a DMZ (*front-end*) e os demais direcionam o tráfego entre a DMZ e a rede confiável (ANDRÉA CRISTINA DE SOUZA DORESTE, 2015).

Na *Militarized Zone* (MZ) não há essa proteção. Assim, a rede confiável pode ser acessada diretamente.

2.4.2 *FIREWALL*

Um *firewall* é um dispositivo no qual realiza a segurança da rede através do monitoramento dos dados de entrada e saída e que baseado em regras predefinidas permite ou bloqueia os acessos. Os *firewall*s podem ser um hardware, um software ou ambos e são utilizados para prevenir acessos internos ou externos a uma rede privada e garantir a segurança dos computadores conectados a uma determinada rede, tanto LAN quanto Internet.

Os *firewall*s permitem colaborar com a segurança pois possibilitam a realização de um controle pontual sobre os processos que se comunicam com a rede. Para isso, podem ser utilizados diversos tipos de assinaturas e informações do hospedeiro para realizar o controle do acesso.

As tarefas básicas de um *firewall* são:

- Proteger os recursos
- Validar o acesso
- Gerenciar e controlar o acesso a rede
- Armazenar e reportar os eventos
- Agir como um intermediário

2.4.2.1 *FIREWALL* DE CAMADA 3

São *firewall*s focados em realizar a filtragem dos pacotes baseado nas informações de IP de origem, IP de destino, porta utilizada e protocolos. Basicamente, são baseados em autorizar o tráfego de um determinado IP através de uma lista de permissões, enquanto bloqueia todos os outros (*whitelisting strategy*). Da mesma forma, pode-se bloquear endereços IP específicos.

Para tornar a configuração mais granular e mais restritiva, pode-se adicionar regras específicas para definir portas e protocolos permitidos para a comunicação de determinados endereços IP. (MORELLO, 2018)

2.4.2.2 *FIREWALL* DE CAMADA 7

Dado o crescimento das aplicações *Web*, tivemos um grande aumento da utilização do protocolo HTTP e de sua porta padrão. Os serviços prestados pela Internet tendem a aumentar ainda mais, sendo assim foi necessário desenvolver uma forma de minimizar a

limitação do modelo anterior. Dessa forma surgiu o *firewall* de camada 7, ou *firewall* de aplicação, no qual permite identificar comportamentos padrões, além dos cabeçalhos, mas agora inspecionando o conteúdo de dados dos pacotes e determinar o tipo de aplicação.

Esse recurso é de extrema relevância, pois antes era necessário mapear todas as redes e portas para os serviços utilizados, o que era muito custoso. Agora, independe-se da rede e porta e passamos a analisar o comportamento da aplicação. Dessa forma, garantindo mais segurança e facilidade para o gerenciamento das redes.

2.4.3 SISTEMA DE PREVENÇÃO DE INTRUSÃO (IPS)

As principais funções de um Sistema de Prevenção de Invasões (IPS) são monitorar o tráfego de rede, identificar atividades maliciosas, gerar informações de monitoramento sobre estas atividades e tentar bloquear ou interrompê-las.

O IPS é um sistema de controle, que tem no *firewall* seu contraponto. Diferente do *firewall*, o IPS trabalha com uma série de regras de análise de tráfego que rejeitem determinados pacotes. Ao chegar uma requisição, o IPS verifica todas as regras, caso o pacote se encaixe em algumas das regras ele é rejeitado, caso contrário o IPS permite o tráfego.

O *firewall* trabalha de forma contrária: suas regras são definidas para avaliar permissões para o tráfego. Então o produto avalia todas as razões para permitir que um pacote trafegue na sua rede. Na falta de uma regra que permita, então o *Firewall* bloqueia aquele pacote.

Para um bom funcionamento de um IPS, é importante ter um grande cuidado na fase de configuração, unido de uma base de inteligência ampla, contendo registros de ameaças conhecidas. Com isso, o IPS será capaz de bloquear qualquer ataque já observado e estudado por instituições de segurança.

Apesar dessa ser a principal aplicação de um IPS, existem outras formas de aproveitar o IPS para proteger sua rede. É possível configurar o IPS para reforçar as políticas de segurança da empresa, analisar comportamentos suspeitos e maliciosos e evitar vazamento de dados. Em geral, os IPS possuem uma ferramenta de controle customizada, na qual é possível criar regras personalizadas que se adaptam à necessidade da aplicação.(BLOCKBIT, 2017)

3 VIRTUALIZAÇÃO APLICADA A UM DATA CENTER

Tradicionalmente, utilizavam-se servidores físicos distintos e independentes para cada aplicação, de forma que, geralmente, os servidores eram subutilizados, pois as aplicações não utilizavam toda a capacidade de hardware disponível, assim ocorrendo desperdício de recurso e de dinheiro. Porém, com a virtualização é possível que um único servidor possa ser dividido em múltiplos servidores únicos capazes de processar tarefas independentes.

A tecnologia de virtualização possibilita a criação de representações em *software* de recursos que normalmente estão vinculados ao *hardware*, como servidores, armazenamento e redes. No processo de virtualização os *hardwares* são substituídos por *softwares* virtuais que são capazes de simular o seu funcionamento, criando as Máquinas Virtuais (VMs).

Um exemplo simples seria a utilização de três servidores, cada um utilizando 20% de sua capacidade total, como na Figura 3.1.

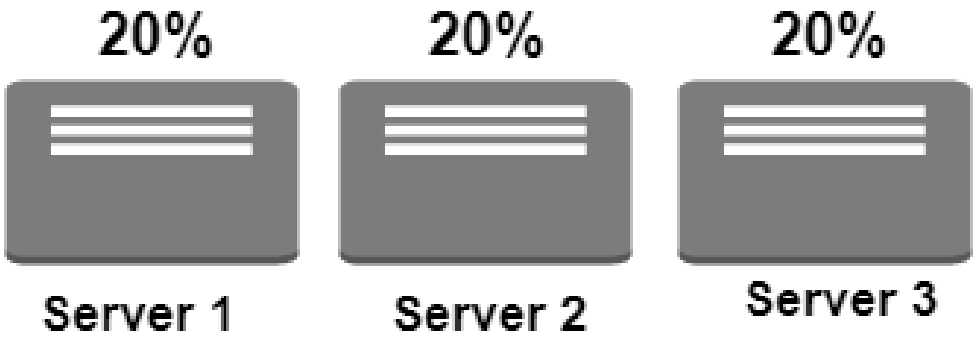

FIG. 3.1: Três servidores físicos separados

Após o processo de virtualização dos três servidores, todos podem ser executados em um único servidor como na Figura 3.2, obtendo uma maior aproveitamento de recurso e descartando a necessidade de outros dois servidores.

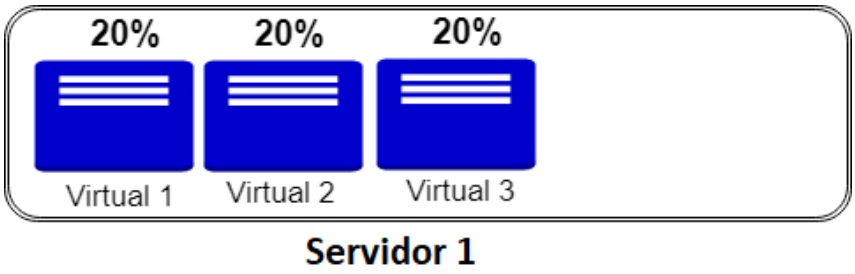

FIG. 3.2: Servidores virtualizados

Dentre as vantagens de utilizar virtualização estão:

- Diminuição de compra e manutenção de *hardware*
- Diminuição de gastos com refrigeração e energia
- Melhor aproveitamento do espaço físico
- Aumento da escalabilidade

Inicialmente, utilizaremos um servidor, contendo duas máquinas virtuais, uma com o sistema operacional Windows 10 e a outra com sistema operacional Ubuntu. Para realizar a execução de múltiplas máquinas virtuais em uma única máquina é necessário que a máquina hospedeira (*host*) contenha um hipervisor.

3.1 HIPERVISOR

Hipervisor, também conhecido como Monitor de Máquinas Virtuais, é um processo que cria e executa máquinas virtuais. Ele possibilita que uma única máquina hospedeira seja capaz de executar múltiplas máquinas virtuais convidadas.

Existem dois tipos de hipervisor, a Figura 3.1 ilustra a diferença de arquitetura:

- Tipo 1 (*bare metal*): É um *software* executado diretamente sobre o *hardware*.
- Tipo 2 (*hosted*): É um *software* executado sobre um sistema operacional.

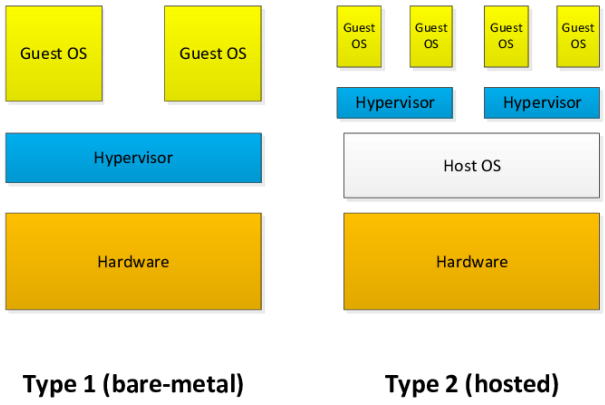

FIG. 3.3: Diferença entre tipos de hipervisor.
Fonte: Pham (2014)

Para o projeto foi utilizado o vSphere Hypervisor da empresa VMware, um hipervisor tipo 1. Essa ferramenta disponibiliza uma interface que pode ser acessada via *browser* como na Figura 3.4.

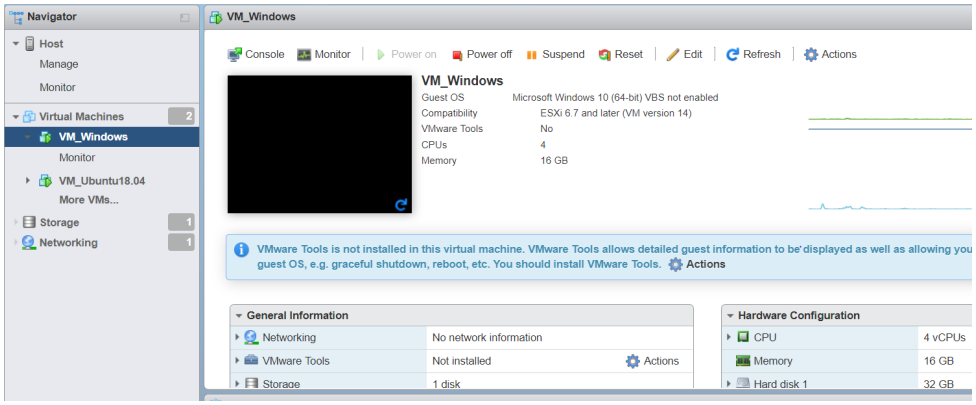

FIG. 3.4: Imagem do vSphere acessado via *browser*

3.2 BALANCEAMENTO DE CARGA

Uma característica importante de um centro de processamento de dados bem gerenciado é a capacidade de evitar pontos de acesso. Nós de acesso sobrecarregados geram problemas de desempenho para a rede e são possíveis pontos de falha. Uma forma de aliviar esse problema é migrar o fluxo de acesso de um nó sobrecarregado para outro pouco utilizado. Dessa forma, possuir um ambiente virtualizado que integra a conexão entre os servidores e o *storage* facilita o processo de migração de máquinas virtuais ou aplicações sem causar falha nas atividades.

4 PROJETO DE DATA CENTER PARA ESCOLAS MILITARES

Com o objetivo de dimensionar a infraestrutura, arquitetura e monitoramento necessários para um projeto de Data Center, está seção aborda o modelo hierárquico que melhor se adéqua a esse projeto, os possíveis clientes, exemplos de serviços de TI comumente utilizados, equipamentos básicos para um Data Center, bem como a configuração física e lógica da rede. Todas essas informações serão úteis para definir a quantidade de equipamentos necessários, como servidores e *storages*.

4.1 MODELO HIERÁRQUICO DE REDE

Conforme descrito por Odom (2013), o design de rede hierárquico é basicamente constituído por três camadas: núcleo, distribuição e acesso. As camadas possuem suas especificidades para dividir as diversas funções que uma rede possui. Por apresentar um design de rede modular, o modelo hierárquico facilita a escalabilidade e melhora o desempenho da rede. Temos na figura 4.1 um exemplo de rede hierárquico com três camadas.

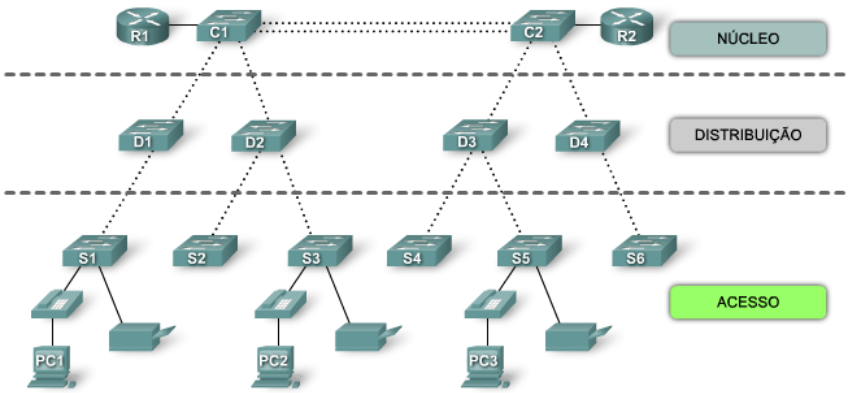

FIG. 4.1: Camadas do Modelo Hierárquico de Rede

- Camada de acesso

  Dispositivos finais, como PCs, telefones IP e impressoras tem sua interface e acesso ao resto da rede feita através da camada de acesso. Podemos ter nessa camada pontos de acesso *wireless, hubs, bridges, switches* e roteadores. A camada de acesso tem como função primordial propiciar um meio de conexão para os dispositivos à rede, bem como controlar essa comunicação e verificar permissões.

- Camada de distribuição

  Os dados recebidos dos *switches* da camada de acesso são agregados na camada de distribuição antes de seguirem seu curso para a camada de núcleo, onde ocorre o roteamento até o destino final. O fluxo do tráfego da rede é controlado por essa camada de distribuição, que determina domínios e políticas de *broadcast* , para realizar as funções de roteamento entre as redes locais virtuais (VLANs), que foram definidas na camada de acesso. Segmentar o tráfego de um *switch* em sub-redes separadas é papel das VLANs. E para assegurar a confiabilidade, são utilizados *switches* de alto desempenho na camada de distribuição, que tem alta disponibilidade e redundância.

- Camada de núcleo

  O *backbone* de alta velocidade das redes interconectadas é a camada de núcleo no design hierárquico. Uma camada de núcleo altamente disponível e redundante é importante, pois essa camada é vital para à interconectividade entre os diversos dispositivos presentes na camada de distribuição. É possível que a área do núcleo se conecte aos recursos da Internet. O núcleo dever ser capaz de encaminhar uma enorme quantidade de dados de forma rápida e eficaz, pois ele concentra o tráfego de todos os dispositivos vindos da camada de distribuição.

4.1.1 BENEFÍCIOS DE UMA REDE HIERÁRQUICA

Designs de rede hierárquica oferecem muitos benefícios.

- Escalabilidade

  Redes hierárquicas possuem a característica de poderem ser expandidas com facilidade, pois à medida que a rede cresce, a modularidade do design propicia replicar os elementos do design. Assim fica simples planejar e implementar a expansão, já que cada instância do módulo é consistente.

- Redundância

  Diante do crescimento de uma rede, é importante manter a disponibilidade. Com as redes hierárquicas podemos aumentar a disponibilidade através de implementações redundantes simples. Para segurar a redundância de caminho, os *switches* da camada de acesso são conectados a dois *switches* distintos na camada de distribuição. Então, o *switch* da camada de acesso tem opção de para comutar caso um *switch* da camada de distribuição venha a falhar. O mesmo ocorre em relação as camadas

de distribuição e núcleo, onde um *switch* de distribuição se conecta a dois ou mais na camada superior.boa noite diogo

- Desempenho

  Por possuírem alto desempenho, os *switches* das camadas de distribuição e núcleo conseguem realizar operações em velocidades altíssimas, com taxas de transmissão perto do limite suportado. Utilizando-se de suas funções de comutação de alto desempenho, a camada de distribuição recebe os dados agregados da camada de acesso e encaminha esse tráfego para a camada de núcleo, para os dados serem roteados até o destino.

- Segurança

  O aprimoramento e o gerenciamento da segurança são facilitados em redes hierárquicas, pois com configurações nos *switches* da camada de acesso, pode-se controlar as permissões para acesso à rede. Políticas de segurança mais avançadas podem ser aplicas com mais flexibilidade, permitindo a implantação de protocolos de comunicação na rede.

- Gerenciabilidade

  Como cada camada em uma rede hierárquica tem funções específicas, gerenciá-la é uma tarefa mais simples. Assim como é mais fácil implementar novas funcionalidades e equipamentos a rede. Os *switches* precisam executar as mesmas funcionalidades em sua camada e deve existir poucas modificações entre eles, logo, a opção de copiar as configurações de um para o outro facilita o gerenciamento.

- Sustentabilidade

  Como somente as camadas de núcleo e de distribuição utilizam *switches* de alto desempenho, o design hierárquico é mais econômico devido a sua modularidade. *switches* mais baratos podem ser implementados na camada de acesso, conforme a rede for sendo expandida.

4.2 CLIENTES

O projeto visa a atender as necessidades dos clientes de acordo com a disponibilidade de recursos e que seja adequado a demanda de serviços. Logo, serão usados conceitos de vários tiers, de forma que ele seja escalável e possa corresponder às expectativas de cada cliente.

- Instituto Militar de Engenharia (IME)

  O IME é um estabelecimento de ensino do Departamento de Ciência e Tecnologia (DCT) responsável, no âmbito do Exército Brasileiro, pelo ensino superior de Engenharia e pela pesquisa básica. Ministra cursos de graduação, pós-graduação e extensão universitária para militares e civis. Insere-se no Sistema de Ciência e Tecnologia do Exército, cooperando com os demais órgãos, por meio da prestação de serviços e pela execução de atividades de natureza técnico-científicas. O Instituto coopera, pelo ensino e pela pesquisa, também para o desenvolvimento científico-tecnológico do País.

- Academia Militar das Agulhas Negras (AMAN)

  A Academia Militar das Agulhas Negras (AMAN), localizada em Resende (RJ), é o único estabelecimento de ensino superior que forma os oficiais combatentes de carreira das armas de Infantaria, Cavalaria, Artilharia, Engenharia e Comunicações, do Quadro de Material Bélico e Serviço de Intendência do Exército Brasileiro.
  Ao longo dos quatro anos de formação na Academia, são realizadas atividades que se fundamentam no desenvolvimento de atributos das áreas afetiva, cognitiva e psicomotora necessários à profissão militar.
  Sua grade curricular inclui disciplinas ligadas às ciências militares, exatas e humanas. Ao final do curso, o concludente é declarado Aspirante a Oficial e recebe o diploma de Bacharel em Ciências Militares.

- Escola de Formação Complementar do Exército (EsFCEx)

  Localizada na cidade de Salvador (BA), é o estabelecimento de ensino militar do Exército responsável pela seleção e preparação de recursos humanos para atuar nas áreas de Administração, Ciências Contábeis, Direito, Magistério, Informática, Economia, Psicologia, Estatística, Pedagogia, Veterinária, Enfermagem e Comunicação Social. O Capelão Militar também tem seu ingresso pela EsFCEx mediante concurso público específico.

- Escola de Aperfeiçoamento de Oficiais (EsAO)

  Fundada em 1920, no Rio de Janeiro, a Escola de Aperfeiçoamento de Oficiais (EsAO) é um estabelecimento pertencente à linha de ensino militar bélico que atua no aperfeiçoamento de capitães do Exército Brasileiro.Seus cursos visam capacitar esses oficiais para o exercício do comando e chefia das unidades de suas Armas,

Quadro e Serviços, habilitando-os para o exercício das funções de Estado-Maior de unidade e demais funções de oficial superior não privativas do Quadro de Estado-Maior da Ativa do Exército.

- Escola de Sargentos das Armas (E S A)

  É o Estabelecimento de Ensino de Nível Superior (Tecnólogo) do Exército Brasileiro, responsável pela formação de Sargentos Combatentes de Carreira das Armas de: Infantaria, Cavalaria, Artilharia, Engenharia e Comunicações.
  A estrutura é composta de alojamentos, refeitórios, salas de aula, laboratório, espaço cultural, biblioteca, auditório, posto médico, capelania, parque de pontes e uma extensa área desportiva constituída por ginásios, campo de futebol, pista de atletismo, piscina, campo de polo, pista hípica e pista de corda. Possui dois campos de instrução: Campo de Instrução do Atalaia com área de 4,6 km^2 e o Campo de Instrução Moacyr Araújo Lopes com área de 20 km^2, sendo este último distante cerca de 40 km de Três Corações/MG.

- Escola de Artilharia de Costa e Antiáerea (EsACosAAe)

  A EsACosAAe é um estabelecimento de ensino de graus superior e médio, de especialização, da Linha de Ensino Militar Bélico destinado a especializar oficiais e sargentos em Artilharia Antiaérea, Defesa da Costa e Defesa do Litoral. Ministrar estágios sobre assuntos peculiares à Artilharia Antiaérea e ao Apoio de Fogo na Defesa do Litoral e Defesa da Costa. Contribuir, por meio de cursos e estágios, com a capacitação de recursos humanos das Forças Singulares e das Nações Amigas. Contribuir para o aperfeiçoamento e o desenvolvimento da doutrina do emprego da Artilharia Antiaérea e do Apoio de Fogo na Defesa do Litoral e Defesa da Costa. E formar reservistas de primeira categoria.

- Escola de Comando e Estado-Maior do Exército (ECEME)

  Criada em 1905 e situada no Rio de Janeiro, a Escola de Comando e Estado-Maior do Exército (ECEME) prepara oficiais superiores para o exercício de funções de Estado-Maior, comando, chefia, direção e assessoramento aos mais elevados escalões do Exército Brasileiro.
  A ECEME ministra cursos de pós-graduação, como o Curso de Altos Estudos Militares (CAEM). Também atua na elaboração e atualização dos manuais sob coordenação do Estado-Maior do Exército (EME), assim como na condução de estudos e

pesquisas com o objetivo de modernizar a doutrina do EME.

Além disso, a ECEME troca experiências com escolas similares da Marinha e da Força Aérea Brasileira, além de universidades. Todo ano, a instituição recebe militares de nações amigas para seus cursos, principalmente da América do Sul e da África.

- Escola de Sargentos de Logística do Exército (EsSLog)

  Localizada na cidade do Rio de Janeiro, RJ, é o Estabelecimento de Ensino do Exército Brasileiro responsável pela formação e o aperfeiçoamento dos sargentos de Material Bélico (Manutenção de Viatura Auto, Manutenção de Armamento e Mecânico Operador), Intendência, Topografia, Manutenção de Comunicações, Saúde e Música. Além do curso de especialização em Mestre de Música e aperfeiçoamento dos sargentos da qualificação militar aviação.

  O ingresso na EsSLog ocorre exclusivamente por meio de concurso de âmbito nacional, realizado pela EsSA.

- Escola Preparatória de Cadetes do Exército (EsPCEx)

  Localizada na cidade de Campinas, SP, é o estabelecimento de ensino militar do Exército responsável por selecionar e preparar os jovens para o ingresso na Academia Militar das Agulhas Negras (AMAN), iniciando a formação do oficial combatente do Exército Brasileiro.

- Escola de Saúde do Exército (EsSEx)

  Localizada na cidade do Rio de Janeiro, é o estabelecimento de ensino militar do Exército responsável pela formação dos oficiais médicos, farmacêuticos e dentistas do Quadro do Serviço de Saúde do Exército Brasileiro.

4.2.1 SERVIÇOS DE TI

Serviços de TI são atividades de desenvolvimento, produção e execução no campo da Tecnologia da Informação visando atender necessidades de indivíduos ou organizações (DA SILVA et al., 2006). Há diversas definições para os serviços de TI e um dos agrupamentos conhecidos é o seguinte:

- Serviços de telecomunicações: têm a função de fornecer conectividade de dados, voz e vídeo aos usuários

- Serviços educacionais de TI: oferecem programas de treinamento e capacitação para os usuários na utilização dos mais variados sistemas e aplicativos
- Serviços de manutenção das plataformas computacionais: são responsáveis por garantir pleno funcionamento dos dispositivos computacionais pertencentes ao usuário, em todas os níveis de grandeza
- Desenvolvimento de padrões de TI: trata da definição das políticas que determinam o emprego da Tecnologia da Informação por parte do usuário
- Serviços de desenvolvimento e suporte de aplicações: responsáveis pela construção e manutenção de aplicações de negócio, como sistemas gerenciais, sistemas CRM, sistemas ERP
- Serviços de gestão das instalações físicas: desenvolvem e administram toda a parte de instalações físicas necessárias para acomodar corretamente serviços de tecnologia, telecomunicações, informática e administração de dados
- Serviços de pesquisa e desenvolvimento em TI: buscam a inovação na área de TI do usuário através de pesquisas em sistemas e tecnologias
- Serviços de gestão de TI: compreende todo o planejamento, execução, monitoramento e controle de um projeto de TI

4.3 GERENCIAMENTO DE SERVIÇOS DE TI: ITIL

O gerenciamento de serviços de TI tem por objetivo gerar valor para o usuário ou organização, evidenciando uma postura proativa para cumprir as necessidades desejadas. Está presente em todo o ciclo de vida do projeto utilizando recursos de forma integrada para tomara de decisão em nível estratégico. O *Information Technology Infrastructure Library* (ITIL) é um conjunto de livros que reúne uma coleção de boas práticas necessária para a integração, implementação e gerenciamento dos processos realizados como serviços de TI. O modelo ITIL é dividido em cinco etapas utilizando a estratégia de serviço como núcleo do ciclo de vida do serviço (FILHO, 2012). As cinco etapas são as seguintes:

- Estratégia de Serviço: decisões estratégicas a respeito de quais serviços serão utilizados são tomadas nessa etapa. Todo o planejamento é realizado para definir quais serviços agregam valor de acordo com as necessidades do cliente

- Projeto de Serviço: tem a responsabilidade de projetar ou desenhar os serviços que foram decididos estrategicamente
- Transição de Serviço: ocorre a transição dos serviços para o ambiente de produção com desenvolvimento, testes e entregas controladas
- Operação de Serviço: realiza o gerenciamento dos serviços que estão em produção para que fiquem alinhados com suas metas. São processos do dia-a-dia que asseguram o funcionamento dos serviços
- Melhoria Contínua de Serviço: é feita a avaliação dos serviços e identificação de oportunidades de melhorias através de *feedbacks* garantindo o atendimento das necessidades do cliente

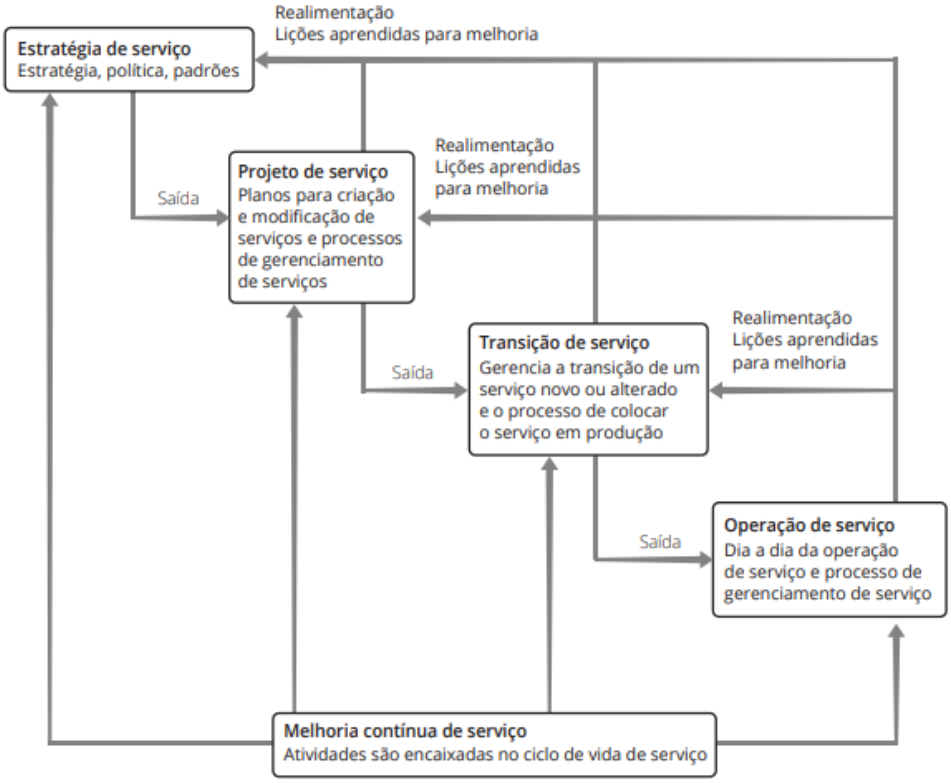

FIG. 4.2: Diagrama ITIL
Fonte: Filho (2012)

4.4 SERVIÇOS NO PROJETO

Neste projeto, serão considerados alguns serviços de TI para o atendimento das necessidades das organizações militares. Existem serviços gerais, que estarão presentes em todas as unidades de ensino, e outros mais específicos, adequados para situações especiais.

4.4.1 CONTROLE DE ACESSO

Quando um acesso é requisitado, o serviço checa a identidade digital desse usuário e verifica se o acesso é permitido. Para esse controle são utilizadas ferramentas de autenticação que podem ser senhas, *tokens*, cartões e impressões digitais, entre outros. É dividido, basicamente, em três etapas sendo elas: Identificação e Autenticação, Autorização e Auditoria. Na primeira, o usuário informa ao sistemas quem ele é (login) e o sistema faz a verificação através de um dos métodos de autenticação confirmando ou não a identidade do usuário. Depois disso, o processo de autorização mostra o que é permitido que o usuário faça no sistema e até qual nível ele possui acesso. Por fim, a informação dessa utilização do usuário é coletada para gerenciamento, planejamento, responsabilização, entre outros (FILHO, 2009). O Controle de Acesso pode ser operado de várias maneiras:

- Centralizado: um sistema central controla todas as decisões sobre acesso ao sistema. Assim, há uma padronização no acesso às informações, mas uma falha nessa entidade compromete todo o serviço
- Descentralizado: a tomada de decisão é feita por entidades mais próximas dos recursos, sendo mais tolerante à falhas, porém podendo contar com diferentes padrões de acesso
- Mandatório: os administradores definem os níveis de privilégios para os usuários e os gestores das informações rotulam as informações de acordo com os níveis, havendo uma separação de tarefas
- Discricionário: nesse caso, o proprietário define a política de controle de acesso e o nível de privilégio obtido
- Baseado em Regras: o controle de acesso é baseado em regras pré-definidas criadas pelo administrador
- Baseado em Perfis: o acesso é baseado no cargo ou função que o funcionário exerce

4.4.2 E-MAIL

Nesse caso, pode ser operado um serviço e-mail corporativo para a instituição que possuir o Data Center, facilitando a comunicação interna profissional. Fornece maior controle do fluxo de mensagens que corre na rede e pode ser baseado em uma nuvem. Permite que o serviço de e-mail seja utilizado externamente ou internamente utilizando os protocolos SMTP, POP3, IMAP

4.4.3 *DOMAIN NAME SYSTEM*

O *Domain Name System* funciona como um sistema de banco de dados distribuídos em uma rede para fazer a conversão dos nomes *user friendly* dos domínios em endereços IP, podendo ser configurado internamente através do Data Center.

4.4.4 ARMAZENAMENTO DE ARQUIVOS

Podemos analisar o armazenamento de arquivos por dois caminhos: armazenamento no *storage* ou *backup*. O armazenamento no *storage* permite maior facilidade no gerenciamento dos dados na estrutura interna e permite compartilhamento de informações com outros usuários. Temos também o *backup* na nuvem, adequado para preservar dados muito importantes e prevenir contra possíveis riscos ou desastres naturais (VERDI et al., 2010). Para o serviço de compartilhamento de arquivos, podem ser utilizados programas, como o Samba, no projeto do Data Center.

4.5 EQUIPAMENTOS BÁSICOS PARA UM DATA CENTER

Considerando o cenário das organizações militares do Exército Brasileiro, serão descritos alguns dos equipamentos essenciais para a construção de um Data Center eficiente. Esses equipamentos fornecerão uma infraestrutura básica, porém eficiente para manter uma alta disponibilidade e garantir a segurança das informações.

- Servidores: Onde serão instaladas as máquinas virtuais responsáveis pelos serviços de TI
- *Storage*: Responsável pelo armazenamento e compartilhamento de arquivos.
- *Firewall*: Equipamento essencial para manter uma política de rede.
- IPS/IDS: Equipamento mais robusto de segurança da informação
- Roteadores: Responsável pela comunicação com os computadores fora da rede local.

A seguir, serão detalhadas as informações gerais, recomendações de aquisição e instruções para configuração para cada um dos equipamentos.

4.5.1 SERVIDORES

Nos servidores, recomenda-se a instalação de um hipervisor *bare metal* que, de preferência, ofereça uma interface com o administrador simples de operar, facilitando sua configuração e manutenção. Alguns exemplos de hipervisores presentes no mercado são: VMware VSphere/VCenter Server, Microsoft Hyper-V e Linux KVM.

Como citado anteriormente, a utilização do hipervisor VSphere, da empresa VMWare, em conjunto com o VCenter oferece um conjunto de funcionalidades, como: *High Availability, VMotion, Dynamic Resource Scheduler, Dynamic Power Management, Storage IO Control, Virtual Volumes, Fault Tolarance*, entre outras. O *VMotion*, por exemplo, permite a migração em tempo real de uma máquina virtual de um servidor físico para outro. A funcionalidade de DRS (*Dynamic Resource Scheduler*) aloca e equilibra dinamicamente a capacidade computacional entre um conjunto de recursos de *hardware* agregados em *pools* lógicos de recursos. (INFRASTRUCTURE, 2006)

4.5.2 STORAGE

O *storage* é o dispositivo físico que atua como uma central de armazenamento do Data Center. Normalmente composto por um conjunto de discos rígidos (HDs) ou discos de estado sólido (SSDs), permite que múltiplos servidores possam compartilhar arquivos, aplicações e outros recursos. O *storage* é responsável por realizar o armazenamento dos arquivos, incluindo as imagens das máquinas virtuais de cada serviço, que serão utilizados pelos servidores. Essa comunicação é controlada através do hipervisor, como mostra a figura 4.3.

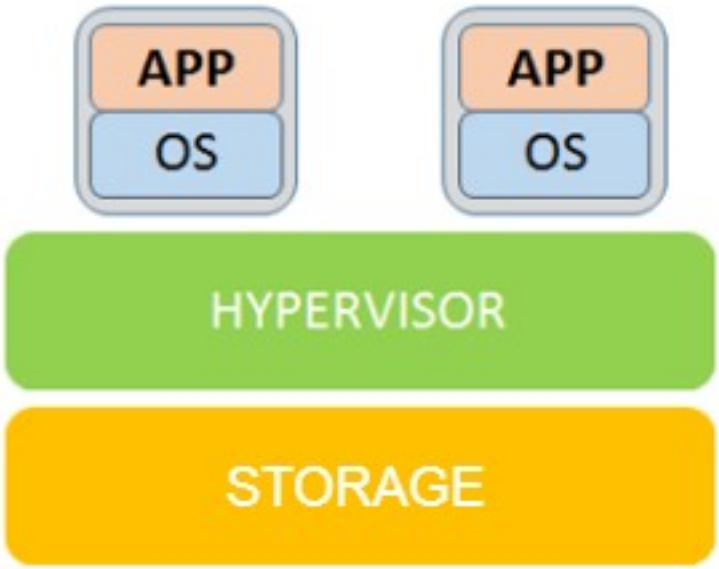

FIG. 4.3: Comunicação entre *hosts* e o *storage* através do hipervisor

Existem algumas formas de configurar este equipamento com a finalidade de garantir a melhor disponibilidade para o Data Center. Essas configurações, conhecidas como *RAID Level* definem como o sistema dividirá o espaço disponível, utilizará as redundâncias, entre outras configurações de armazenamento. É necessário realizar o mapeamento entre os servidores e os respectivos *storages*, dessa forma definindo quais servidores têm acesso a quais *storages*.

É recomendada a utilização do *RAID Level* 5, pois ele permite criar uma camada de redundância, dedicando apenas uma fração do espaço total. Para isso utiliza um sistema de paridade para manter a integridade dos dados, de forma que dedica um segmento de cada HD para armazenar as informações de paridade. Geralmente, utiliza-se a configuração de *RAID* 5 quando o servidor possui um grande número de HDs, o que condiz com a realidade de um Data Center. (CHEN; LEE, 1995)

4.5.3 SWITCH TOP OF THE RACK (TOR)

O *switch ToR* é o equipamento que permite a comunicação dos servidores com o *storage* e dos servidores entre si, como o seu nome diz, localiza-se geralmente no topo do rack e atendem às necessidades dos servidores.

Os servidores devem ter no mínimo duas interfaces, uma interface de dados e uma interface de gerência. A interface de dados é onde trafega especificamente os serviços de TI que são fornecidos, por exemplo, o acesso a internet e o acesso de rede interna. Enquanto isso, a interface de gerência é responsável pela comunicação do *host* com os equipamentos

de *hardware*, como os *storage*. Dessa forma, a comunicação interna e externa trafegam por interfaces diferentes.

Além disso, a conexão entre os servidores e os *switches* recomenda-se a utilização de uma técnica de empilhamento de *switches*, esta técnica utililiza portas dedicadas, exclusivamente para realizar a conexão entre os *switches*. Ou seja, para cada *switch* emparelhado funcional será necessário um par de equipamentos, que estarão fisicamente conectados e logicamente representados como um só, como mostra a figura 4.4. Para os *switches* da Cisco essa técnica é conhecida como VSS (*Virtual Switching System*).

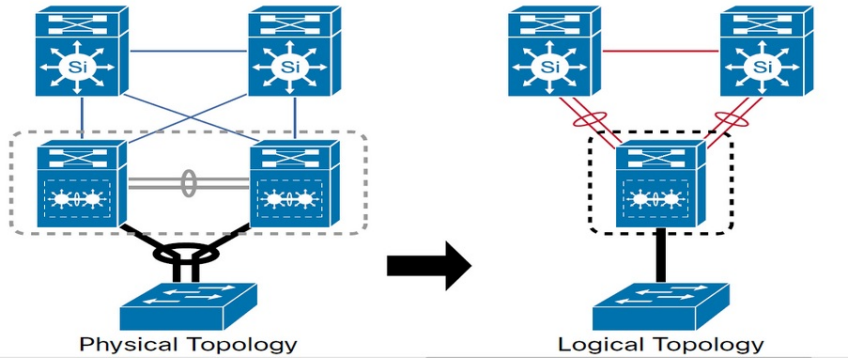

FIG. 4.4: Representação físico x lógico utilizando VSS

Dessa forma, é necessário conectar ambas as interfaces, dados e gerência, a cada um dos *switches* físicos, pois caso um dos equipamentos pare de funcionar o outro aparelho ainda manterá o sistema em atividade mantendo uma alta disponibilidade, apesar da redução de capacidade total. Nesse cenário é necessário que o servidor possua quatro interfaces de conexão, porém é possível agrupar as duas portas do servidor em um único canal lógico utilizando o protocolo LACP (*Link Agreggation Control Protocol*). Esse agrupamento lógico também pode ser realizado nas interfaces do *switch* utilizando o *etherchannel*, no caso de um *switch* Cisco.

Dada essa configuração, recomenda-se, para um Data Center básico, a utilização de dois *switches* empilhados de 48 portas 1G + 2 portas 1/10 G cada, que devem ser o suficiente para atender a necessidade de um rack 44U (unidades de rack).

Tendo o projeto de rede para os *switches* que atendem aos servidores, deve-se configurar o restante da rede física.

4.5.4 CONFIGURAÇÃO FÍSICA DA REDE

A conexão do *switch* ToR com o restante dos equipamentos será mediado através de um outro *switch*, chamado de *core*. Para isso, conectam-se as portas de 10G do *switch* ToR a

cada um dos *switches core*, conforme mostra a figura 4.5. Conforme citado anteriormente, o objetivo é sempre manter uma alta disponibilidade fornecendo alguma redundância nas conexões, pois caso haja algum problema em um dos equipamentos o seu par redundante conseguirá manter a disponibilidade.

Além disso, os *switches core* devem se conectar com o *firewall*, que determinará as políticas de conexão com a Internet. Essa conexão pode ser intermediada por um IPS ou IDS, dependendo das necessidades de segurança e disponibilidade do equipamento. Os *storages* e a rede *WiFi* também são fisicamente conectados aos *switch cores*, conforme exemplificado na figura 4.5

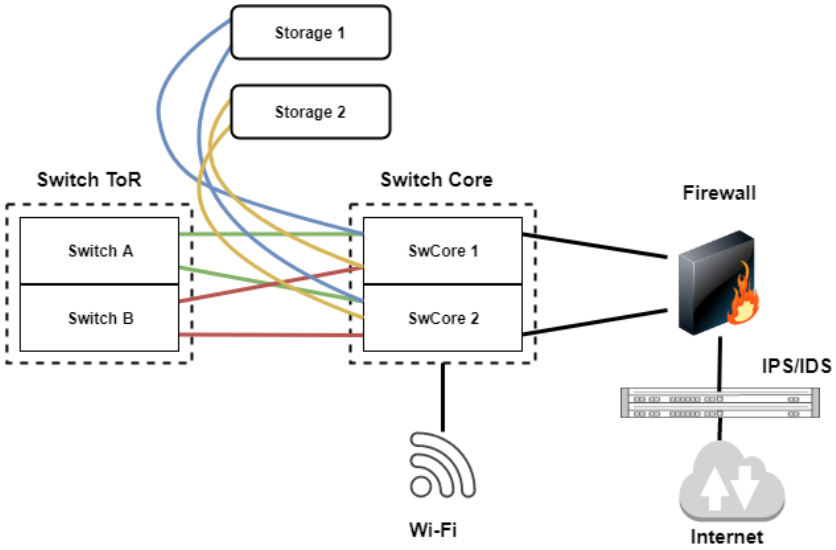

FIG. 4.5: Conexões físicas entre os equipamentos

Uma vez que temos a configuração física dos equipamentos, é necessário montar a estrutura lógica da rede.

4.5.5 CONFIGURAÇÃO LÓGICA DA REDE

Uma configuração lógica básica para a rede consiste em ter a entrada da conexão com a Internet através de um IPS ou IDS, passando em seguida por um *firewall* e seguindo para o seu destino final, como mostra a figura 4.6.

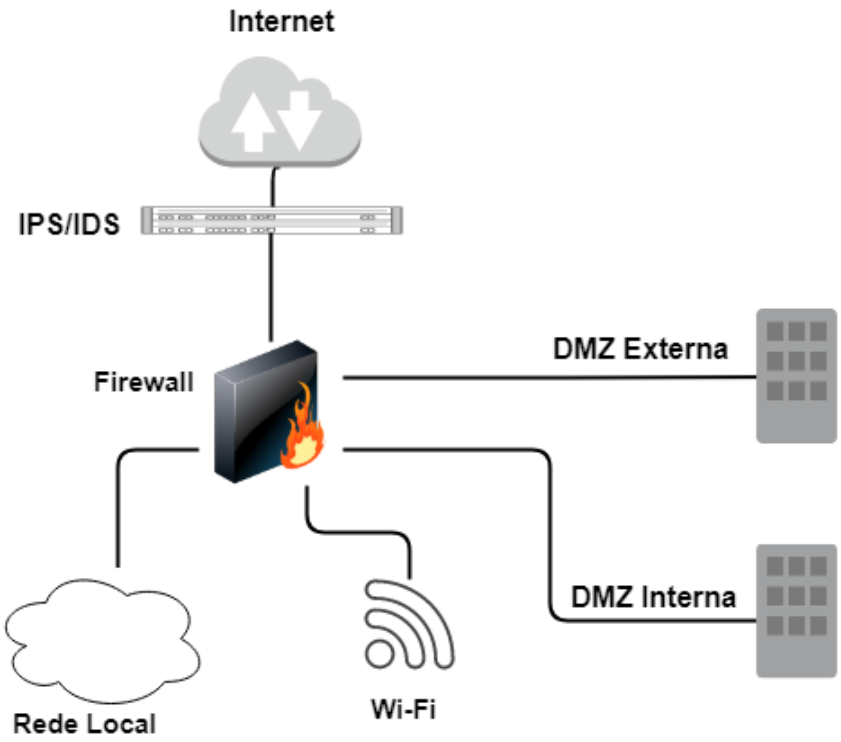

FIG. 4.6: Diagrama lógico da rede

Também podemos observar pela figura 4.6 que cada DMZ, a rede local e a rede wi-fi são redes separadas e o *firewall* é o equipamento que efetivamente faz o controle.

Nessa representação, é importante compreender a diferença entre a DMZ interna e a DMZ externa. No qual a DMZ externa é aquela que possui conexão com a Internet, ou seja, existe uma regra de *firewall* que direciona as requisições da Internet para esta DMZ. Já a DMZ interna, a rede local e a rede wi-fi são apenas para conexões internas, a figura 4.7. Essa segregação ocorre para reduzir a exposição dos serviços para o ambiente externo e aumentar a segurança da rede.

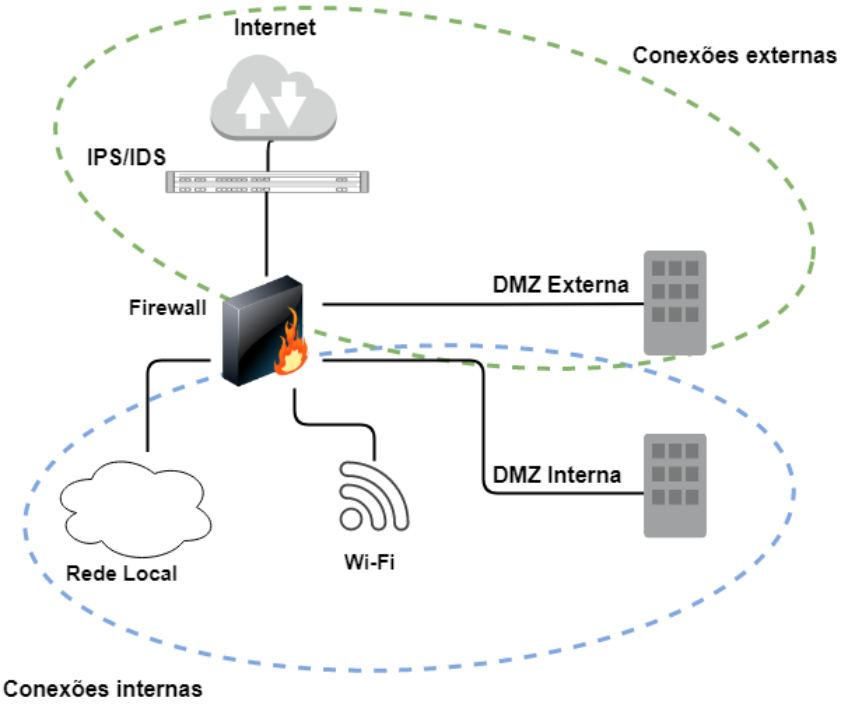

FIG. 4.7: Agrupamento lógico para conexões externas e internas

Na tabela 4.1 temos alguns exemplos de onde alocar determinados serviços com segurança.

DMZ interna	**DMZ externa**
Compartilhamento de arquivos	E-mail.
Páginas Internas	DNS
DHCP	Páginas externas

TAB. 4.1: Onde alocar os serviços

Finalizando a configuração lógica, é necessário adicionar a comunicação com os *storages*. Esses acessos deverão ser feitos somente por alguma DMZ, pois nelas se encontram os serviços de TI que necessitam diretamente do acesso aos arquivos e imagens das máquinas virtuais. Dessa forma, a comunicação é feita através de uma rede intermediária, chamada rede de gerenciamento, como pode ser observado na figura 4.8.

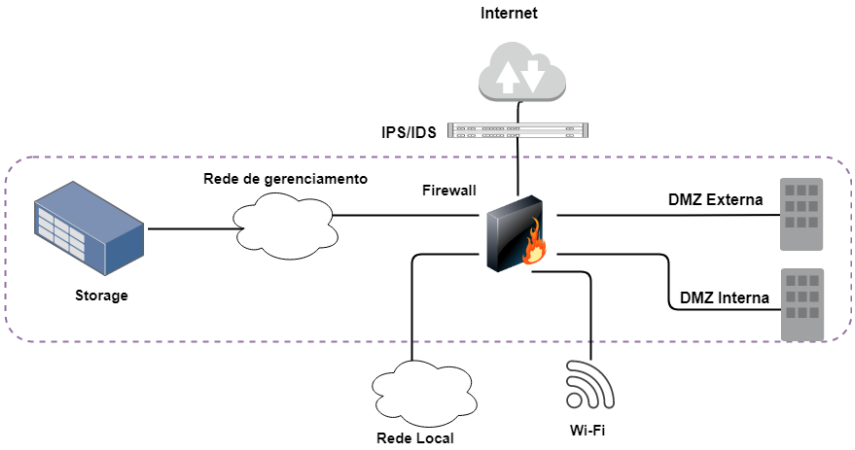

FIG. 4.8: Diagrama lógico da rede

5 DIMENSIONAMENTO DO DATA CENTER

Para a realização do dimensionamento de um Data Center, isto é, estimar a quantidade de mínima de equipamentos para o seu funcionamento, é necessário saber quantos usuários consumirão os serviços, quais os serviços que serão hospedados e quanto de recurso computacional cada serviço utiliza. Pois, esses fatores determinam quanto de recurso total os servidores devem possuir para garantir alta disponibilidade.

Para a realização de um dimensionamento genérico o conjunto das escolas militares foi dividido em dois tipos baseado seu efetivo estimado, conforme apresentado na tabela 5.1 a seguir.

Escola	**Usuários (estimativa)**	**Classificação**
IME	2000	Tipo 1
EsAO	3000	
EsFCEx	1000	
EsLog	3000	
ECEME	2000	
EsPCEx	2000	
AMAN	7000	Tipo 2
EsA	5000	

TAB. 5.1: Classificação das escolas militares

Foram levantados os principais serviços utilizados em uma escola militar tendo como modelo o Instituto Militar de Engenharia (IME). Esses serviços, por sua vez, foram separados em cinco grupos de acordo com o quanto necessitam de CPU, memória e espaço de disco como indicado na tabela 5.2.

Grupo	**CPU**	**Memória (GB)**	**Disco (GB)**
Grupo 1	2	4	20
Grupo 2	4	8	40
Grupo 3	8	16	80
Grupo 4	2	8	3000
Grupo 5	4	16	10000

TAB. 5.2: Classificação dos serviços

Esses grupos serão utilizados para classificar cada serviço utilizado pela OM, permitindo assim determinar o total de recurso necessário para o funcionamento do Data Center.

5.1 PRINCIPAIS SERVIÇOS PARA ESCOLAS MILITARES

Analisando a necessidade das escolas militares devemos conjugar características de um quartel genérico com a de uma escola, com isso, obtendo um conjunto de serviços essenciais para o funcionamento de ambas as partes como: SPED, EAD, correio eletrônico, entre outros serviços. Os principais serviços levantados foram:

- Correio Eletrônico: Responsável pelo armazenamento e gerenciamento dos e-mails da OM, para isso necessita de uma grande capacidade de armazenamento, porém não requer muito recursos de CPU e memória.
- *Webmail*: Serviço que fornece uma interface de interação para o usuário do correio eletrônico, isto é, um *front-end* para o serviço de correio eletrônico.
- DNS primário e secundário: Responsável por realizar resolução de nomes, isto é, fazer a tradução dos domínios para os respectivos endereços IP. Para isso não é necessário grande esforço computacional.
- EAD primário e secundário: Serviço de armazenamento e gerência de todo conteúdo de ensino a distância. Dependendo da quantidade de matérias ministradas e material disponível pode necessitar de uma grande capacidade de armazenamento, porém não utiliza muito recurso de CPU e de memória.
- Hospedagem de páginas: Serviço de hospedagem de páginas, geralmente contém conteúdo institucional para divulgação externa, informações de professores. Por ser um serviço de acesso público é necessário que o servidor possua uma maior robustez quanto a CPU e memória para suportar os acessos e ter uma rápida resposta para o usuário.
- Sistema de inscrição: Serviço utilizado nos períodos de inscrição de concursos para a escola. Serviço que será utilizado com pouca frequência e não requer muito utilização de recurso.
- Squid: Serviço de *proxy* muito utilizado para diminuir a utilização da conexão e melhorar a velocidade de respostas de requisições frequentes através de um cache de páginas web. Devido a funcionalidade de cache e de resposta rápida ao usuário requer mais capacidade de armazenamento e utilização de memória/CPU, respectivamente.

- VPN: Serviço básico de VPN, não consome muito recurso, além de não ser muito comumente utilizado pela maioria dos usuários.
- DCNM: O serviço *Data Center Network Manager* é um serviço da empresa Cisco utilizado para realizar o gerenciamento de equipamentos de rede.
- VCenter: Serviço que fornece um *hub* universal para o gerenciamento de todos os *hosts* vSphere e máquinas virtuais no Data Center a partir de um único console.
- ZABBIX: Ferramenta de monitoramento que permite acompanhamento e monitoramento de rede e serviços hospedados no Data Center. Dependendo da quantidade de usuários pode necessitar de uma maior capacidade de processamento para monitoramento de todo o tráfego de rede.
- Sistema Acadêmico: Serviço onde é realizado o controle dos graus obtidos pelos alunos nas avaliações, que servem para gerar o histórico escolar. Também realiza o controle de frequência dos alunos. Não requer muitos recursos.
- Banco de dados de produção: Serviço para armazenar e manipular informações de outros sistemas. Requer mais capacidade de armazenamento.
- Banco de dados de backup: Serviço que faz uma ou mais cópias dos arquivos de dados com a finalidade de preservar e recuperar esses dados em caso de perda por qualquer motivo. Requer mais capacidade de armazenamento.
- CFTV: O circuito fechado de televisão é um sistema de TV para fins de vigilância e segurança em que os sinais não são distribuídos de forma pública, mas serão monitorados e possivelmente armazenados. Neste último caso, tem que ser levado em consideração o tamanho físico da área a ser monitorada e o período pelo qual esses dados vão ser armazenados. Um CFTV requer uma grande capacidade de armazenamento e pode exigir mais de uma VM.
- DHCP: O *Dynamic Host Configuration Protocol* é um protocolo utilizado em redes de computadores que permite aos dispositivos finais obterem um endereço IP automaticamente. Não requer muitos recursos.
- FTPServer: Um servidor FTP possibilita um serviço de acesso para usuários, através de uma rede de computadores, a um disco rígido ou servidor de arquivos através do *File Transfer Protocol*. Requer uma grande capacidade de armazenamento e utilização de memória.

- Gitsever: O Git é um sistema utilizado para controlar a versão de arquivos. Diversas pessoas podem contribuir simultaneamente com a criação e edição de um mesmo projeto, sem o risco de suas colaborações serem sobrescritas. Devido as características das escolas militares, não requer uma grande quantidade de recursos para operar.

- Homologação 1 e 2: Serviços que realizam testes em sistemas internos desenvolvidos para cada OM especificamente. Requer uma quantidade mediana de armazenamento e utilização de memoria.

- ISEServer: O *Identity Services Engine* é um serviço de controle de acesso para autenticação de equipamentos. É uma solução da CISCO mais abrangente que o LDAP, pois a maioria dos outros serviços pode utilizar o ISE para autenticação, mas poucos serviços podem fazer uso do LDAP com está finalidade. Requer uma quantidade mediana de armazenamento e utilização de memória/CPU.

- KSCServer: O *Kaspersky Security Center* é um sistema de gerenciamento de antivírus, que facilita a administração da segurança de sistemas de TI. Requer poucos recursos de armazenamento, memória e processamento.

- LDAP: O *Lightweight Directory Access Protocol* é uma base de dados para armazenar usuários e senhas. Outros sistemas podem consultar esses dados para autenticação. O LDAP possui uma interface muito bem definida, onde os usuários podem ser divididos em grupos. Não requer uma grande quantidade de recursos.

- Página Intranet: É um serviço que disponibiliza um canal de comunicação direto entre o comando da OM e os seus servidores civis e militares. Pode conter todas as informações relevantes e de caráter geral da organização. Não requer uma grande quantidade de recursos.

- Samba: É um serviço para sistemas baseados em Unix, onde computadores com sistema Windows podem compartilhar e gerenciar recursos. Requer uma grande capacidade de armazenamento e utilização de memória.

- Sisbol: Sistema do Exército que gera o boletim interno. Não requer grande quantidade de recursos.

- Sistema de Identificação: Sistema de identificação de pessoal nas organizações militares. Varia de acordo com o número de usuários, mas não necessita de grande

quantidade de recursos computacionais.

- Sistemas Internos: Sistemas próprios desenvolvidos internamente por cada OM para necessidades específicas e locais. Pode variar sua capacidade computacional de acordo com o número de sistemas internos.

- Sistema de Biblioteca: Serviço que gerencia toda a atividade da biblioteca de uma OM. Necessita de uma capacidade mediana de memória e processamento que pode ser maior ou menor de acordo com o número de usuários e tamanho do acervo de materiais.

- SPED64: Sistema administrativo que gerencia a documentação no Exército Brasileiro. A quantidade de recursos computacionais depende diretamente da quantidade de documentos gerados.

- Suporte OTRS: Sistema de chamado que gera *tickets* para filas de atendimento. Requer pouca memória e capacidade de processamento.

Classificando os serviços citados nos grupos predeterminados para cada tipo de escola militar obtém-se a Tabela 5.3 que permite ter uma visão geral de quanto de recurso cada serviço consumirá e estimar a quantidade de recurso necessária para hospedar todos os serviços.

Nome do serviço	**Tipo de Rede**	**Grupo para escola tipo 1**	**Grupo para escola tipo 2**
Correio Eletrônico	Externa	4	5
Webmail	Externa	1	2
DNS primário	Externa	1	1
DNS secundário	Externa	1	1
EAD primário	Externa	4	4
EAD secundário	Externa	4	4
Hospedagem Páginas	Externa	2	3
Sistema de Inscrição	Externa	1	1
Squid	Externa	2	3
VPN	Externa	1	1
DCNM	Gerência	1	1
Vcenter	Gerência	1	1
ZABBIX	Gerência	1	2
Academico	Interna	1	1
Banco de Dados Produção	Interna	4	4
Banco de Dados Backup	Interna	4	4
CFTV	Interna	4	4
DHCP	Interna	1	1
FTPServer	Interna	4	5
Gitserver	Interna	1	1
Homologação 1	Interna	2	2
Homologação 2	Interna	2	2
ISEServer	Interna	2	2
KSCServer	Interna	1	2
LDAP	Interna	1	1
Página Intranet	Interna	1	2
Samba	Interna	4	5
Servidor de Licenças de Software	Interna	1	1
Sisbol	Interna	1	1
Sistema de Identificação	Interna	1	1
Sistemas 1	Interna	1	2
Sistemas 2	Interna	1	2
Sistemas 3	Interna	1	2
Sistemas 4	Interna	1	2
Sistema de Biblioteca	Interna	2	2
SPED64	Interna	1	2
Suporte OTRS	Interna	1	1

TAB. 5.3: Serviços classificados de acordo com seu consumo

Na realização do dimensionamento será considerado somente o consumo de memória, pois para efeitos práticos é o recurso que fornece maior limitação de *hardware* para os equipamentos, uma vez que o hipervisor tem capacidade de alocar dinamicamente os

processadores de acordo com a demanda de cada serviço e o armazenamento será realizado majoritariamente no *storage*. Com isso, realizando a soma do consumo de memória de todos os serviços para cada tipo de escola e considerando uma folga de 25% como margem de segurança e para garantia de escalabilidade para próximos cinco anos são obtidos os valores de utilização de memória de 255 GB e 350 GB para escolas do tipo 1 e tipo 2, respectivamente. Considerando um servidor padrão de 48 GB de memória RAM, como o PowerEdge R900 da empresa Dell, serão necessários seis desses servidores para atender uma escola tipo 1 e oito para uma escola do tipo 2, como indicado na tabela 5.4.

Tipo de escola	**Número de processadores**	**Capacidade de Disco (TB)**	**Memória (GB)**	**Nº de Servidores**
Tipo 1	86	24,7	255	6
Tipo 2	118	45,96	350	8

TAB. 5.4: Quantidade total de recursos utilizado e número de servidores PowerEdge R900 necessários.

Analisando a capacidade de disco total ocupada pelos serviços, pode-se estimar a capacidade total do *storage* para suprir esse Data Center. Para escolas do tipo 1, 25 TB de armazenamento são o suficiente para manter todos os serviços ativos em seu máximo consumo, enquanto para escolas do tipo 2 são necessários, aproximadamente, 46TB.

Determinando a quantidade de servidores necessário para cada tipo de escola e assumindo que cada servidor conecta-se através de duas portas com cada um dos *switches* empilhados, conclui-se que um único par de *switches* é o suficiente para suprir o total de conexões do rack.

Com isso, para ambos os tipos de escola, um único rack contendo 44 unidades de rack é capaz de suprir toda a necessidade de espaço para alocar os servidores, os *switches* e o *firewall*.

6 MONITORAMENTO DO DATA CENTER

O monitoramento de um Data Center é uma tarefa fundamental para evitar a paralisação das operações e fornecer uma melhor visualização do consumo de recursos para o administrador responsável. Através da utilização de ferramentas é possível obter informações de disponibilidade e desempenho de aplicações, ativos e serviços de rede. Durante o projeto, configurou-se e testou-se a ferramente Zabbix, e recomenda-se o seu uso para o monitoramento dos Data Center nas instituições de ensino do EB.

Portanto nesse capítulo será explicada a ferramenta, seu uso, e como ela pode facilitar a manutenção para o gestor do Data Center.

6.1 ZABBIX

O Zabbix é uma ferramenta de monitoramento de servidores moderna, *Open Source* e multiplataforma, livre de custos de licenciamento, pois sua licença é a GPLv2. (HORST et al., 2015)

Essa ferramenta possui diversos módulos, mas podem-se destacar algumas principais funcionalidades, como:

- Autodescoberta de dispositivo de rede;
- Autodescoberta de recursos de hospedeiro;
- *Low Level Discovery*, permitindo criação de gatilhos, itens e gráficos para diferentes recursos;
- Monitoramento distribuído com administração centralizada.

Além disso, é fornecida uma interface web aos usuários que permite realizar toda a configuração e gerenciamento remotamente.

6.1.1 *LOW LEVEL DISCOVERY*

Nativamente, o Zabbix fornece os seis tipos de descoberta de baixo nível a seguir.

- Descoberta de sistemas de arquivo;

- Descoberta de interfaces de rede;
- Descoberta de CPUs seus núcleos;
- Descoberta de árvores de OID SNMP;
- Descoberta usando consultas SQL/ODBC;
- Descoberta de serviços Windows.

Porém os usuários podem desenvolver modelos personalizados de descobertas através de *scripts* próprios. Para isso, o usuário deve criar regras de descobertas na aba de *templates*. Em seguida, a configuração é dividida em duas etapas: definição de um item capaz de descobrir os elementos de configuração de interesse (por exemplo, sistemas de arquivo ou interfaces de rede) e definição dos protótipos de itens, *triggers* e gráficos que poderão ser criados dinamicamente usando as informações descobertas.

Por exemplo, para realizar a descoberta de um sistemas de arquivo basta o usuário escolher qual modelo deseja utilizar e selecionar a opção "descoberta". Em seguida, deverá preencher um conjunto de informações que definirão as regras de descoberta e filtros que serão aplicados após a descoberta e antes da criação de entidades, como mostrado na figura 6.1.

Com a criação dessas regras, torna-se possível a criação protótipos de itens, protótipos de *triggers* e protótipos de gráficos, que fornecerão de forma visual e organizada as informações obtidas do agente. Esse conjunto de configurações representam um modelo que pode ser utilizado outros serviços.

Após a configuração dos itens que desejam ser monitorados, é possível realizar o acompanhamento dos principais problemas através do *dashboard* inicial. Como exibido na figura 6.3, essa interface exibe os problemas que ocorreram nos servidores nas últimas horas, destacando a gravidade, o *host* em que ocorreu e a duração. Outras informações, como utilização de CPU e utilização de memória, podem ser obtidas na aba *latest data*, no qual permite o filtro por *hosts* e aplicações.

6.1.2 MONITORAMENTO COM ZABBIX

Utilizando como modelo as informações do Zabbix utilizado no monitoramento do Data Center do Instituto Militar de Engenharia (IME), pode-se observar a diversidade de informações que são fornecidas de forma clara e direta ao administrador do Data Center.

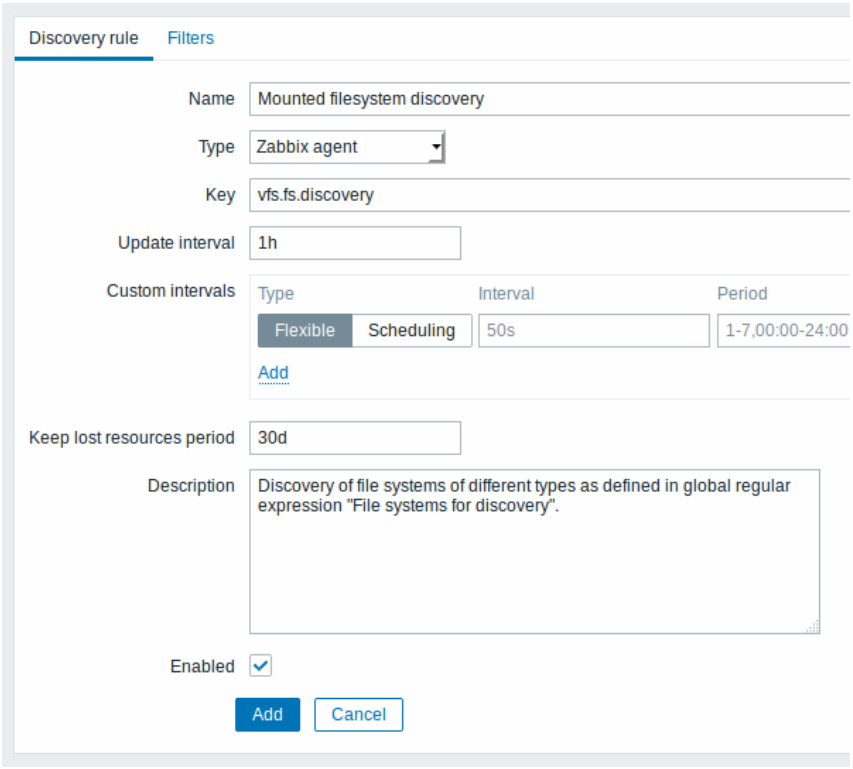

FIG. 6.1: Criação de regra de descoberta na interface Web do Zabbix
Fonte: ZabbixSIA (2019)

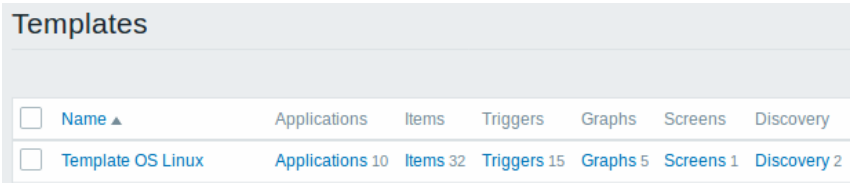

FIG. 6.2: Exemplo de um *template* no Zabbix
Fonte: ZabbixSIA (2019)

Por exemplo, a figura 6.4 exibe os gráficos referentes a Internet fornecida ao IME pelo Centro Brasileiro de Pesquisas Físicas (CBPF) e a utilização rede interna do IME.

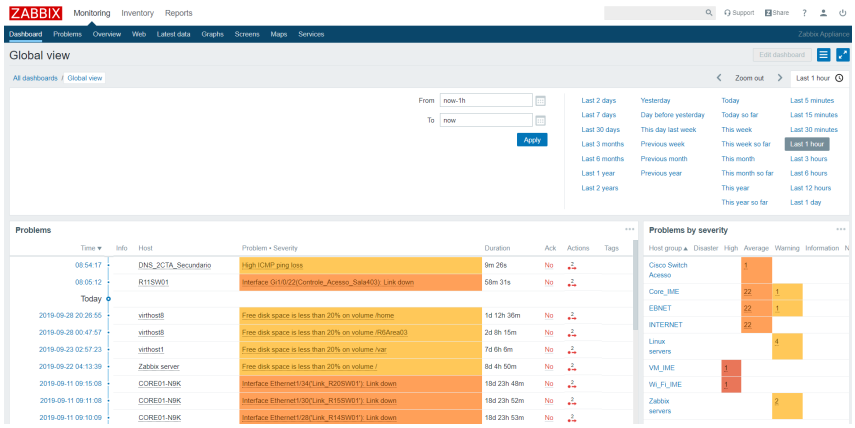

FIG. 6.3: *Dashboard* do Zabbix utilizado no IME

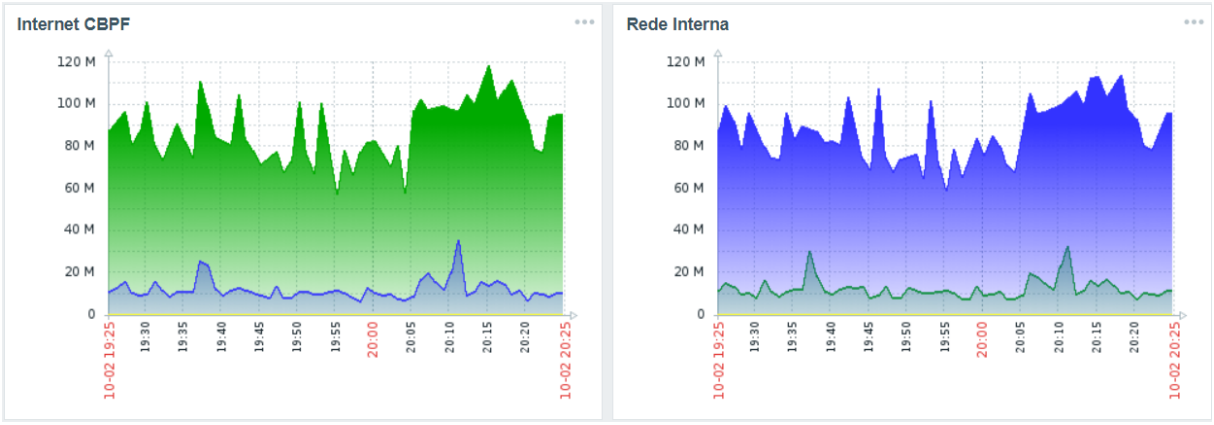

FIG. 6.4: Gráficos exibindo Internet fornecida pelo Centro Brasileiro de Pesquisas Físicas e a utilização da rede interna do IME

Além de informações genéricas de rede, podem ser obtidos dados referentes a *hardwares* específicos, como mostrado na figura 6.5 que exibe o tráfego nos principais *switches* que se atendem os servidores.

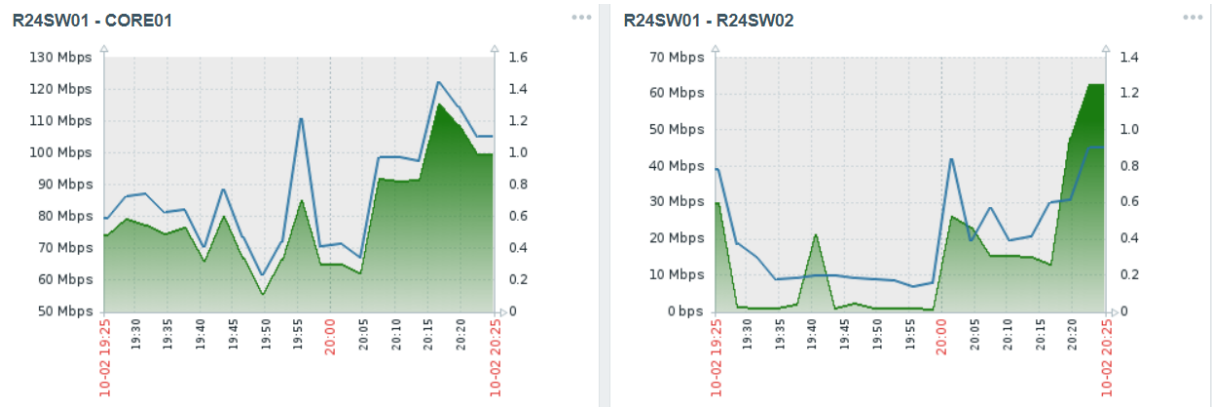

FIG. 6.5: Monitoramento dos principais *switches* do Data Center do IME

O Zabbix também é capaz de auxiliar no controle e gerenciamento de acessos à rede sem fio. A figura 6.6, mostra o número de usuários conectados à rede Wi-Fi, que permite o responsável ter um maior controle dos acessos a rede.

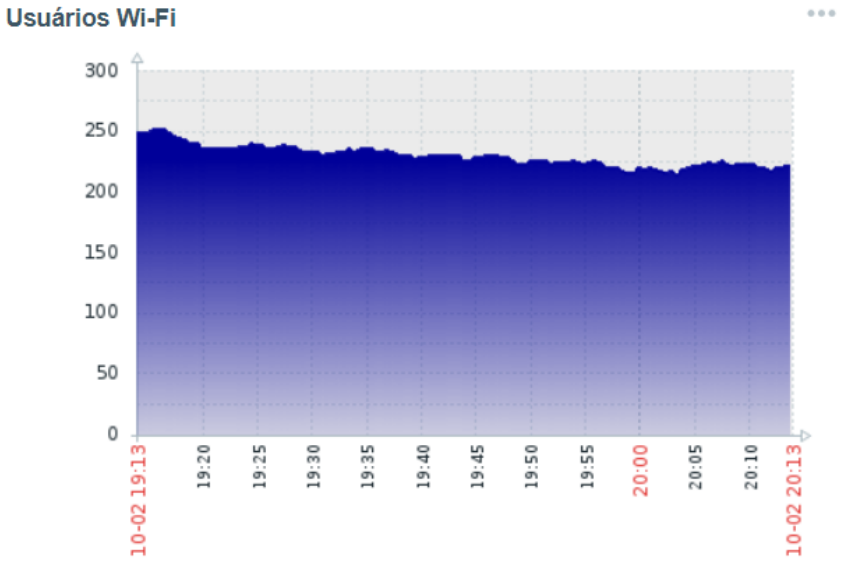

FIG. 6.6: Número de usuários conectados à rede sem fio no tempo

Além das ferramentas para monitoramento de rede, permite a análise de servidores virtualizados e de serviços. Dessa forma, sendo capaz de fornecer informações sobre o uso de CPU, consumo de memória e armazenamento de cada serviço. As figuras 6.7 e 6.8 exibem a utilização da CPU e a quantidade de memória RAM disponível para o um dos *virtual hosts*.

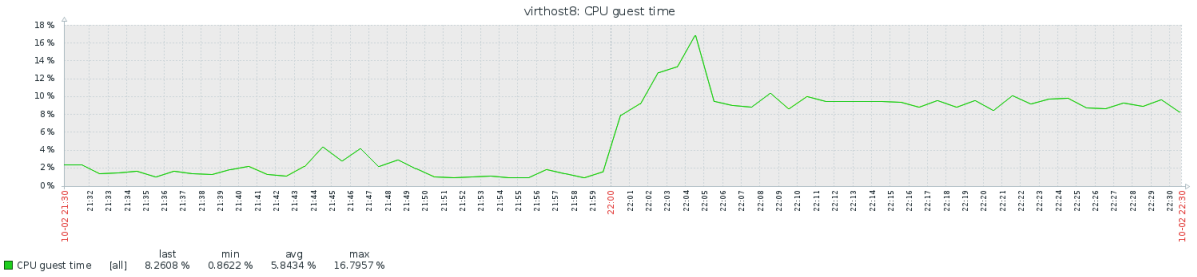

FIG. 6.7: Utilização da CPU do servidor virthost8

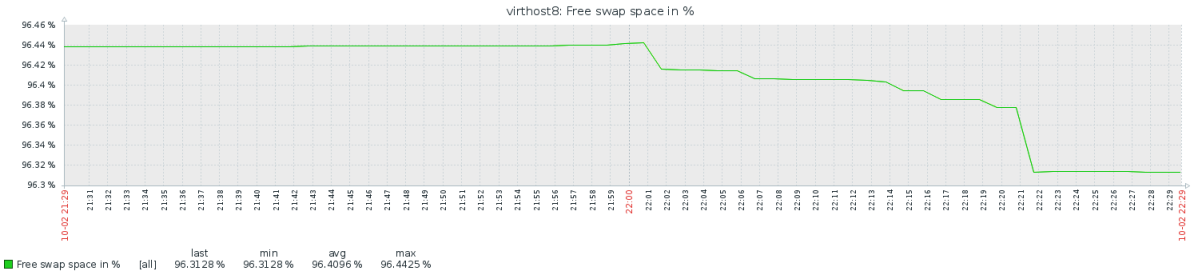

FIG. 6.8: Utilização de memória do servidor virthost8

7 CONSIDERAÇÕES FINAIS

As informações contidas neste trabalho, permitem a qualquer comandante de escola militar do Exército Brasileiro, escolher qual tipo de Data Center construir em sua OM.

Em nossa exaustiva busca por informações, colocamos à disposição do leitor, não só o dimensionamento de um Data Center, mas também sua infraestrutura, arquitetura e sugestão de software para monitoramento. Todo esse arcabouço teórico permite que o agente decisor leve em consideração as especificidades da escola como o número de alunos e instrutores, a área construída e outros fatores técnicos que são inerentes à construção de uma estrutura tão complexa, mas que neste texto, foi abordada de forma simples e prática.

Também tratamos de toda parte de *hardware* e *software* necessários a um centro de processamento de dados, os quais são prescritos em normas mundialmente reconhecidas e nos padrões técnicos do EB. Colocamos à disposição resultados de observação em um Data Center real, o do Instituto Militar de Engenharia, que serve de modelo para outras escolas de formação castrense.

Fica como principal sugestão para trabalhos futuros, a visita de outros Data Centers das Forças Armadas, para obter um *feedback* sobre as lições aprendidas no projeto. Tal documentação pode evitar desperdícios de recursos em projetos futuros.

8 REFERÊNCIAS BIBLIOGRÁFICAS

ANDRÉA CRISTINA DE SOUZA DORESTE, BRIAN ROCHA CONFESSOR E IGOR DOMINICES BAÍA DO AMARAL. Firewalls uma maior segurança. Disponível em: <https://www.gta.ufrj.br/grad/15_1/firewall/dmz.html>. Acesso em: 15 maio de 2019.

ASSOCIATION, T. I.; OTHERS. Tia-942 data center standards overview. **White Paper**, v. 2, p. 148, 2006.

BLOCKBIT. IDS ou IPS: o quê você precisa?. Disponível em: <https://www.blockbit.com/pt-br/2017/10/02/ids-ou-ips-o-que-voce-precisa/>. Acesso em: 16 abr. de 2019.

CHEN, P. M.; LEE, E. K. **Striping in a RAID level 5 disk array**. [S.l.]: ACM, 1995.

CANAL COMSTOR. O QUE É UM DATA CENTER. Disponível em: <https://blogbrasil.comstor.com/bid/334188/o-que-um-data-center>. Acesso em: 15 maio de 2019.

DA SILVA, E. M.; YUE, G. K.; ROTONDARO, R. G. ; LAURINDO, F. J. B. Gestão da qualidade em serviços de ti: em busca de competitividade. **Production**, v. 16, n. 2, p. 329–340, 2006.

FILHO, F. C. **ITIL v3 Fundamentos**. Rio de Janeiro: Escola Superior de Redes, 2012. 1 p.

SÓCRATES FILHO. Segurança da Informação: Autenticação. Disponível em: <http://waltercunha.com/blog/2009/08/19/seguranca-da-informacao-autenticacao/>. Acesso em: 20 jul. de 2019.

FRIGO, A. B. G. **Infraestrutura de data center e suas tendências com foco em eficiência energética**. 2015. Trabalho de Conclusão de Curso (Bacharelado - Engenharia Elétrica) – Universidade Estadual Paulista, São Paulo, 2015.

HORST, A. S.; DOS SANTOS PIRES, A. ; DÉO, A. L. B. **De A a Zabbix: Aprenda a monitorar e gerenciar aplicações e equipamentos de redes com o Zabbix**. [S.l.]: Novatec Editora, 2015.

INFRASTRUCTURE, V. Resource management with vmware drs. **VMware Whitepaper**, v. 13, 2006. Disponível em: <http://golftreeinternational.com/other/VMWare/module%2011/page%20519/vmware_drs_wp.p Acesso em: 17 jul. de 2019.

MORELLO, JOHN. Know Your Firewall: Layer 3 vs. Layer 7. Disponível em: <https://www.twistlock.com/2018/10/23/know-firewall-layer-3-vs-layer-7/>. Acesso em: 15 abr. de 2019.

ODOM, W. **Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic Edition**. 1st. ed. [S.l.]: WebEx Communications, 2013. ISBN 1587144859, 9781587144851.

PHAM, K. **Embedded Virtualization of a Hybrid ARM - FPGA Computing Platform**. 2014. Tese (Mestrado em Engenharia) – Nanyang Technological University, Singapore, 2014.

VERDI, F. L.; ROTHENBERG, C. E.; PASQUINI, R. ; MAGALHÃES, M. Novas arquiteturas de data center para cloud computing. **Minicursos do XXVIII SBRC**, v. 28, p. 103–152, 2010.

WIERMAN, A.; LIU, Z.; LIU, I. ; MOHSENIAN-RAD, H. Opportunities and challenges for data center demand response. In: INTERNATIONAL GREEN COMPUTING CONFERENCE, 8., 2014. **Anais**... [S.l.: s.n.], 2014, p. 1–10.

ZABBIXSIA. Zabbix Documentation 3.4. Disponível em: <https://www.zabbix.com/documentation/3.4/pt/manual/discovery/low_level_discovery>. Acesso em: 29 set. de 2019.

ZUCCHI, W. L.; AMÂNCIO, A. B. Construindo um data center. **Revista USP**, v. 97, 2013. Disponível em: <https://doi.org/10.11606/issn.2316-9036.v0i97p43-58>. Acesso em: 15 mai. de 2019.

9 ANEXOS

9.1 ANEXO A - REFERÊNCIAS NORMATIVAS

As seguintes normas contêm, disposições que, através de referência neste texto, constituem provisões da TIA-942. No momento da publicação, as edições indicadas eram válidas. Todas as normas estão sujeitas a revisão, e as partes em acordos baseados nesta norma são encorajadas a investigar a possibilidade de aplicar as edições mais recentes das normas publicadas por elas.

- ANSI / TIA / EIA-568-B.1-2001, Norma Comercial de Cabeamento de Telecomunicações: Parte 1: Requisitos Gerais;
- ANSI / TIA / EIA-568-B.2-2001, Padrão de Cabeamento de Telecomunicações para Edifícios Comerciais: Parte 2: componentes de cabeamento de par trançado balanceado;
- ANSI / TIA / EIA-568.B.3-2000, Padrão de Componentes de Cabeamento de Fibra Ótica;
- ANSI / TIA-569-B, Padrão de Edifícios Comerciais para Caminhos e Espaços de Telecomunicações;
- ANSI / TIA / EIA-606-A-2002, Norma de Administração para Infraestrutura de Telecomunicações Comerciais;
- ANSI / TIA / EIA-J-STD-607-2001, Aterramento do Edifício Comercial (Aterramento) e Requisitos de Ligação para Telecomunicações;
- ANSI / TIA-758-A, Padrão de cabeamento de telecomunicações de instalações externas de propriedade do cliente;
- ANSI / NFPA 70-2002, Código Elétrico Nacional;
- ANSI / NFPA 75-2003, Norma para a proteção de equipamentos de tecnologia da informação;

- ANSI T1.336, Requisitos de engenharia para um quadro universal de telecomunicações;
- ANSI T1.404, interfaces de instalação de redes e clientes - DS3 e especificação de interface metálica;
- ASHRAE, Diretrizes Térmicas para Ambientes de Processamento de Dados;
- Telcordia GR-63-CORE, NEBS (TM) Requisitos: proteção física;
- Telcordia GR-139-CORE, Requisitos genéricos para cabo coaxial de escritório central.

9.2 ANEXO B - DATA CENTER TIERING

Os quatro níveis de Data Center definidos originalmente pelo *The Uptime Institute* são:

- Data Center Tier I : Básico
  Um Data Center Tier I é suscetível a interrupções de atividades planejadas e não planejadas. Ele tem distribuição e resfriamento de energia do computador, mas pode ou não ter um piso elevado, um *no-break* ou um gerador de motor. Se tiver UPS ou geradores, eles são sistemas de módulo único e possuem muitos pontos de falha únicos. A infraestrutura deve ser completamente desligada anualmente para realizar trabalhos de manutenção e reparo preventivos. Situações urgentes podem exigir desligamentos mais frequentes. Erros de operação ou falhas espontâneas dos componentes da infraestrutura do site causarão uma interrupção no Data Center.
- Data Center Tier II : Componentes Redundantes
  As instalações de Nível II com componentes redundantes são ligeiramente menos suscetíveis a interrupções de atividades planejadas e não planejadas do que um Data Center básico. Eles têm um piso elevado, UPS e geradores de motor, mas seu *design* de capacidade é "*Need plus One*" (N + 1), que tem um caminho de distribuição *singlethreaded* por toda parte. A manutenção do caminho crítico de energia e outras partes da infraestrutura do site exigirão um encerramento de processamento.
- Data Center Tier III : simultaneamente mantido
  A capacidade de nível Nível 3 permite qualquer atividade de infraestrutura de site planejada sem interromper a operação do hardware do computador de forma alguma. As atividades planejadas incluem manutenção preventiva e programável,

reparo e substituição de componentes, adição ou remoção de componentes de capacidade, teste de componentes e sistemas e muito mais. Para grandes locais usando água gelada, isso significa dois conjuntos independentes de tubos. A capacidade e a distribuição suficientes devem estar disponíveis para transportar simultaneamente a carga em um caminho enquanto executa a manutenção ou o teste no outro caminho. Atividades não planejadas, como erros na operação ou falhas espontâneas nos componentes da infraestrutura da instalação, ainda causarão uma interrupção do centro de dados. Os sites de Nível 3 geralmente são projetados para serem atualizados para o Nível IV quando o caso de negócios do cliente justifica o custo da proteção adicional. O site deve ser operado 24 horas por dia.

- Data Center Tier IV : tolerante a falhas
  Um Data Center de Nível 4 possui vários caminhos ativos de distribuição de energia e resfriamento. Como pelo menos dois caminhos estão normalmente ativos em um Data Center de tier IV, a infraestrutura oferece um grau mais alto de tolerância a falhas. Os Data Centers de tier IV fornecem vários alimentadores de energia para todos os computadores e equipamentos de telecomunicações. O Nível 4 requer que todos os equipamentos de computador e de telecomunicações tenham várias entradas de energia. O equipamento deve poder continuar funcionando com uma dessas entradas de energia desligadas. Equipamentos que não são construídos com múltiplas entradas de energia precisarão de chaves de transferência automáticas.
  O Nível 4 fornece capacidade de infraestrutura do site para permitir qualquer atividade planejada sem interromper a carga crítica. A funcionalidade tolerante a falhas também fornece a capacidade da infraestrutura do site de sustentar pelo menos uma falha ou evento não planejado no pior caso, sem impacto na carga crítica. Isso requer caminhos de distribuição ativos simultaneamente, normalmente em uma configuração *System + System*. Eletricamente, isso significa dois sistemas UPS separados nos quais cada sistema tem redundância N + 1. Devido aos códigos de segurança contra incêndio e eletricidade, ainda haverá exposição devido a alarmes de incêndio ou pessoas iniciando um desligamento de emergência (EPO). O Nível IV requer que todo o hardware do computador tenha duas entradas de energia, conforme definido pelo *Institute's Fault-Tolerant Power Compliance Specification.*
  As infraestruturas de Data Center da Nível 4 são as mais compatíveis com conceitos de tecnologia da informação de alta disponibilidade que empregam *clustering* de CPU, *Redundant Array* de disco independente / dispositivo de armazenamento de

acesso direto (RAID / DASD) e comunicações redundantes para obter confiabilidade, disponibilidade e capacidade de manutenção.

9.2.1 REQUISITOS DE SISTEMAS DE TELECOMUNICAÇÕES

a) TIER 1

A infraestrutura de telecomunicações deve atender aos requisitos da norma para ser classificada como, no mínimo, nível 1.

Uma instalação de nível 1 terá uma abertura de manutenção e um caminho de entrada para a instalação de um cliente. Os serviços do provedor de acesso serão encerrados em uma sala de entrada. A infraestrutura de comunicações será distribuída da sala de entrada para as principais áreas de distribuição e distribuição horizontal em todo o Data Center por meio de um único caminho. Embora a redundância lógica possa ser incorporada na topologia da rede, não haveria redundância física ou diversificação fornecida em uma instalação de nível 1.

Etiquete todos os painéis, tomadas e cabos, conforme descrito em ANSI / TIA / EIA-606-A. Etiquete todos os gabinetes e racks com o identificador na parte frontal e traseira.

Alguns possíveis pontos únicos de falha de uma instalação de nível 1 são:

- indisponibilidade do provedor de acesso, interrupção da central telefônica ou interrupção ao longo de um direito de acesso do provedor de acesso;
- falha no equipamento do provedor de acesso;
- falha no roteador ou no switch, se não forem redundantes;
- qualquer evento catastrófico dentro da sala de entrada, área de distribuição principal ou furo de manutenção pode interromper todos os serviços de telecomunicações para o centro de dados;
- danos no *backbone* ou no cabeamento horizontal.

b) TIER 2

A infraestrutura de telecomunicações deve atender aos requisitos do nível 1.

Equipamentos de telecomunicações críticos, equipamentos de provisionamento de provedores de acesso, roteadores de produção, switches LAN de produção e switches SAN de produção devem ter componentes redundantes (fontes de alimentação, processadores).

O cabeamento de *backbone* LAN e SAN do centro de dados de switches nas áreas de distribuição horizontal para switches de *backbone* na área de distribuição principal deve ter pares de fios ou de fibra redundantes dentro da configuração global da estrela. As conexões redundantes podem estar na mesma ou em diferentes bainhas de cabo.

Configurações lógicas são possíveis e podem estar em uma topologia de anel ou malha sobreposta à configuração física da estrela.

Uma instalação de nível 2 aborda a vulnerabilidade dos serviços de telecomunicações que entram no edifício.

Uma instalação de nível 2 deve ter dois furos de manutenção e caminhos de entrada para a instalação do cliente. Os dois caminhos de entrada redundantes serão terminados dentro de uma sala de entrada. Recomenda-se que a separação física dos caminhos dos orifícios de manutenção redundantes até a sala de entrada seja de no mínimo 20 m (66 pés) ao longo de toda a rota da via. Recomenda-se que os caminhos de entrada entrem nas extremidades opostas da sala de entrada. Não é recomendável que as vias de entrada redundantes entrem na instalação na mesma área, pois isso não fornecerá a separação recomendada ao longo de todo o percurso.

Todos os *patch cords* e *jumpers* devem ser rotulados nas duas extremidades do cabo com o nome da conexão nas duas extremidades do cabo para que um Data Center seja classificado como nível 2.

Alguns possíveis pontos únicos de falha de uma instalação de nível 2 são:

- equipamento de provedor de acesso localizado na sala de entrada conectada à mesma distribuição elétrica e suportada por componentes ou sistemas de AVAC únicos;
- hardware redundante de roteamento e comutação central localizado na principal área de distribuição, conectado à mesma distribuição elétrica e suportado por componentes ou sistemas HVAC únicos;
- hardware de comutação de distribuição redundante localizado na área de distribuição horizontal conectada à mesma distribuição elétrica e suportada por componentes ou sistemas HVAC únicos;
- qualquer evento catastrófico na sala de entrada ou na principal área de distribuição pode interromper todos os serviços de telecomunicações para o centro de dados.

c) TIER 3

A infraestrutura de telecomunicações deve atender aos requisitos do nível 2.

O Data Center deve ser atendido por pelo menos dois provedores de acesso. O serviço deve ser prestado a partir de pelo menos dois escritórios centrais de provedores de acesso ou pontos de presença. O cabeamento do provedor de acesso a partir de seus escritórios centrais ou pontos de presença deve ser separado por pelo menos 20 m (66 pés) ao longo de toda a rota, para que as rotas sejam consideradas roteadas de forma diversa.

O Data Center deve ter duas salas de entrada, de preferência em extremidades opostas do Data Center, mas um mínimo de 20 m (66 pés) de separação física entre as duas salas. Não compartilhe equipamentos de fornecimento de provedores de acesso, zonas de proteção contra incêndio, unidades de distribuição de energia e equipamentos de ar condicionado entre as duas salas de entrada. O equipamento de fornecimento de provedores de acesso em cada sala de entrada deve poder continuar operando se o equipamento na outra sala de entrada falhar.

O Data Center deve ter caminhos de *backbone* redundantes entre as salas de entrada, a área de distribuição principal e as áreas de distribuição horizontal.

O cabeamento de *backbone* LAN e SAN do centro de dados de switches nas áreas de distribuição horizontal para switches de I na área de distribuição principal deve ter pares de fios ou de fibra redundantes dentro da configuração global da estrela. As conexões redundantes devem estar em *shells* de cabos diversamente roteados.

Deve haver um *backup* de reserva "quente"para todos os equipamentos de telecomunicações críticos, equipamentos de provisionamento de provedores de acesso, roteadores de produção de Nível central e switches LAN / SAN de produção de Nível central.

Todos os cabos, conexões cruzadas e *patch cords* devem ser documentados usando planilhas, bancos de dados ou programas projetados para realizar a administração de cabos. A documentação do sistema de cabeamento é um requisito para que um Data Center seja classificado como nível 3.

Alguns possíveis pontos únicos de falha de uma instalação de nível 3 são:

- qualquer evento catastrófico na principal área de distribuição pode interromper todos os serviços de telecomunicações para o Data Center;

- qualquer evento catastrófico dentro de uma área de distribuição horizontal pode interromper todos os serviços para a área que ele atende.

d) TIER 4

A infraestrutura de telecomunicações deve atender aos requisitos do nível 3.

O cabeamento de *backbone* do Data Center deve ser redundante. O cabeamento entre dois espaços deve seguir rotas fisicamente separadas, com caminhos comuns apenas dentro dos dois espaços finais. O cabeamento de *backbone* deve ser protegido pelo direcionamento por conduíte ou pelo uso de cabos com blindagem intertravada.

Deve haver *backup* automático para todos os equipamentos de telecomunicações críticos, equipamentos de provisionamento de provedores de acesso, roteadores de produção de camada central e switches LAN / SAN de produção de camada central. Sessões / conexões devem mudar automaticamente para o equipamento de *backup*.

O Data Center deve ter uma área de distribuição principal e uma área de distribuição secundária, preferencialmente em extremidades opostas do Data Center, mas um mínimo de 20 m (66 pés) de separação física entre os dois espaços. Não compartilhe zonas de proteção contra incêndio, unidades de distribuição de energia e equipamentos de ar condicionado entre a área de distribuição principal e a área de distribuição secundária. A área de distribuição secundária é opcional, se a sala de computadores for um único espaço contínuo, provavelmente haverá pouco a ganhar implementando uma área de distribuição secundária.

A área de distribuição principal e a área de distribuição secundária terão, cada uma, um caminho para cada sala de entrada. Também deve haver um caminho entre a área de distribuição principal e a área de distribuição secundária.

Os roteadores e chaves de distribuição redundantes devem ser distribuídos entre a área de distribuição principal e a secundária, de modo que as redes dos centros de dados possam continuar operando se a área principal de distribuição, a área de distribuição secundária ou uma das salas de entrada apresentar uma falha total .

Cada uma das áreas de distribuição horizontal deve ter conectividade com a área de distribuição principal e com a área de distribuição secundária.

Sistemas críticos devem ter cabeamento horizontal para duas áreas de distribuição horizontal. O cabeamento horizontal redundante é opcional mesmo para instalações de nível 4.

Alguns possíveis pontos únicos de falha de uma instalação de nível 4 são:

- a área de distribuição principal (se a área de distribuição secundária não estiver implementada);
- na área de distribuição horizontal e no cabeamento horizontal (se o cabeamento horizontal redundante não estiver instalado).

9.2.2 REQUISITOS ARQUITETÔNICOS E ESTRUTURAIS

a) TIER 1

Arquitetonicamente, um Data Center de nível 1 é um Data Center sem requisitos de proteção contra eventos físicos, intencionais ou acidentais, naturais ou feitos pelo homem, que poderiam causar falha no Data Center.

A carga mínima de piso para áreas de equipamento deve ser de 7,2 kPa (150 lbf/ft^2) de carga viva com 1,2 kPa (25 lbf/ft^2) para cargas penduradas no fundo do piso. Pode-se consultar a especificação Telcordia GR-63-CORE referente à medição da capacidade de carga do piso e aos métodos de teste.

b) TIER 2

As instalações de Nível 2 devem atender a todos os requisitos do nível 1. Um Data Center de Nível 2 inclui proteções mínimas adicionais contra eventos físicos, intencionais ou acidentais, naturais ou feitos pelo homem, que podem causar falha no Data Center.

Barreiras de vapor devem ser fornecidas para as paredes e teto da sala de computadores para garantir que o equipamento mecânico possa manter os limites de umidificação.

Todas as portas de segurança devem ser de madeira maciça com armações de metal. Portas para equipamentos de segurança e salas de monitoramento também devem ser fornecidas com um olho mágico de 180 graus.

Todas as paredes de segurança devem ter altura total (do chão ao teto). Além disso, as paredes dos equipamentos de segurança e as salas de monitoramento devem ser temperadas instalando-se madeira compensada de no mínimo 16 mm (5/8 pol.) No interior da sala com adesivo e parafusos a cada 300 mm (12 pol.).

A carga mínima de piso para as áreas de equipamento deve ser de 8,4 kPa (175 lbf/ft^2) de carga viva com 1,2 kPa (25 lbf/ft^2) para cargas penduradas no fundo do piso.

c) TIER 3

As instalações de Nível 3 devem atender a todos os requisitos do nível 2. Um Data Center de nível 3 estabeleceu proteções específicas contra a maioria dos eventos físicos, intencionais ou acidentais, naturais ou feitos pelo homem, o que poderia causar falha no Data Center.

Devem ser fornecidas entradas redundantes e pontos de verificação de segurança. Estradas de acesso redundantes com pontos de verificação de segurança devem ser fornecidas para garantir o acesso em caso de inundação de estradas ou outros problemas e / ou para permitir a separação do acesso de funcionários e fornecedores.

Não deve haver janelas nas paredes externas do perímetro da sala de computadores. A construção dos edifícios deve fornecer proteção contra a radiação eletromagnética. A construção de aço pode fornecer essa blindagem. Alternadamente, uma gaiola de Faraday para fins especiais pode ser embutida nas paredes, consistindo de folha de alumínio, placa de gesso com revestimento de alumínio ou arame de galinha.

Mantraps em todas as entradas da sala de informática devem fornecer medidas que reduzam o potencial de pegar carona ou permitir que mais de uma pessoa intencionalmente use somente uma credencial. Intertravamentos de segurança para uma única pessoa, catracas, portais ou outros hardwares projetados para impedir o retorno de credenciais devem ser empregados para controlar o acesso da entrada principal da sala de computadores.

A separação física ou outra proteção deve ser fornecida para separar equipamentos e serviços redundantes para eliminar a probabilidade de paralisações simultâneas.

Uma cerca de segurança deve ser considerada, com pontos de acesso seguros e controlados. O perímetro do local deve ser protegido por um sistema de detecção de intrusão de micro-ondas e monitorado por sistemas de Circuito Fechado de Televisão (CFTV) visíveis ou infravermelhos.

O acesso ao site deve ser protegido por sistemas de identificação e autenticação. Controle de acesso adicional deve ser fornecido para áreas cruciais, como a sala de informática, salas de entrada e áreas elétricas e mecânicas. Os centros de dados devem receber uma sala de segurança dedicada para fornecer monitoramento central para todos os sistemas de segurança associados ao Data Center.

A carga mínima do piso para as áreas de equipamento deve ser de 12 kPa (250 lbf/ft^2) carga viva com cargas de 2,4 kPa (50 lbf/ft^2) suspensas do fundo do piso.

d) TIER 4

As instalações de Nível 4 devem atender a todos os requisitos do nível 3.

Um Data Center de nível 4 considera todos os possíveis eventos físicos, intencionais ou acidentais, naturais ou feitos pelo homem, que poderiam causar falha no Data Center. Fornece proteções específicas e, em alguns casos, redundantes contra tais eventos. Os Data Centers de nível 4 consideram os possíveis problemas com desastres naturais, como eventos sísmicos, enchentes, incêndios, furacões e tempestades, bem como problemas potenciais com o terrorismo e funcionários insatisfeitos. E têm controle sobre todos os aspectos de suas instalações.

Deve haver uma área localizada em um prédio separado ou gabinete externo para um bloco seguro de gerador.

Deve haver também uma área designada fora do prédio o mais próximo possível do gerador de tanques de armazenamento de combustível.

As instalações localizadas dentro das zonas sísmicas 0, 1 e 2 devem ser projetadas de acordo com os requisitos da zona sísmica 3. As instalações localizadas dentro das zonas sísmicas 3 e 4 devem ser projetadas de acordo com os requisitos da zona sísmica 4. Todas as instalações devem ser projetadas com um fator de importância I = 1,5. Os equipamentos e racks de dados nas zonas sísmicas 3 e 4 devem ser fixados na base e fixados na parte superior para resistir às cargas sísmicas.

A carga mínima do piso para as áreas de equipamento deve ser de 12 kPa (250 lbf/ft^2) carga viva com cargas de 2,4 kPa (50 lbf/ft^2) suspensas do fundo do piso.

9.2.3 REQUISITOS DE SISTEMAS ELÉTRICOS

a) TIER 1

Uma instalação de nível 1 fornece o nível mínimo de distribuição de energia para atender aos requisitos de carga elétrica, com pouca ou nenhuma redundância. Os sistemas elétricos são de caminho único, em que uma falha ou manutenção em um painel ou alimentador causará uma interrupção parcial ou total das operações. Nenhuma redundância é necessária na entrada do serviço de utilidade.

Os geradores podem ser instalados como unidades únicas ou em paralelo para capacidade, mas não há requisito de redundância. Um ou mais comutadores de transferência automática são normalmente usados para detectar a perda de potência normal, o início da partida do gerador e a transferência de cargas para o sistema gerador. Os disjuntores de transferência automática de *bypass* de isolamento (ATSs) ou os disjuntores de transferência automática são usados para este propósito, mas não são

necessários. Bancos de carga permanentemente instalados para testes de gerador e no-break não são necessários. Provisão para anexar bancos de carga portáteis é necessária.

O sistema de fonte de alimentação ininterrupta pode ser instalado como uma unidade única ou em paralelo para capacidade. As tecnologias de UPS estáticas, rotativas ou híbridas podem ser utilizadas, com projetos de dupla conversão ou interativos de linha. A compatibilidade do sistema UPS com o sistema gerador é necessária. O sistema UPS deve ter um recurso de *bypass* de manutenção para permitir operação contínua durante manutenção do sistema UPS.

Transformadores separados e painéis de painéis são aceitáveis para a distribuição de energia para as cargas eletrônicas críticas em Data Centers de nível 1. Os transformadores devem ser projetados para lidar com a carga não linear que eles devem alimentar. Transformadores de cancelamento harmônico também podem ser usados no lugar de transformadores com classificação K.

Unidades de distribuição de energia (PDU) ou transformadores discretos e painéis de painéis podem ser usados para distribuir energia às cargas eletrônicas críticas. Qualquer método de cabeamento compatível com código pode ser utilizado. Redundância não é necessária no sistema de distribuição. O sistema de aterramento deve estar em conformidade com os requisitos mínimos de código.

Uma infraestrutura de aterramento do Data Center não é necessária, mas pode ser desejável como um método econômico para atender aos requisitos de aterramento dos fabricantes de equipamentos. A decisão de instalar proteção contra raios deve se basear em uma análise de risco de relâmpago conforme a NFPA 780 e requisitos de seguro. Se o Data Center for classificado como uma Sala de Equipamentos de Tecnologia da Informação por NEC 645, um sistema de Desligamento de Emergência (EPO) deve ser fornecido.

O monitoramento de sistemas elétricos e mecânicos é opcional.

b) TIER 2

As instalações de Nível 2 devem atender a todos os requisitos do nível 1.

Uma instalação de nível 2 fornece módulos UPS redundantes N + 1. Um sistema gerador dimensionado para lidar com todas as cargas do Data Center é necessário, embora os grupos geradores redundantes não sejam necessários. Nenhuma redundância é necessária na entrada do serviço público ou no sistema de distribuição de energia.

Provisões para conectar bancos de carga portáteis devem ser fornecidas para testes de gerador e UPS.

As unidades de distribuição de energia (PDUs) devem ser usadas para distribuir energia às cargas eletrônicas críticas. Quadros de painel ou "*sidecars*" da PDU podem ser sub-alimentados a partir de PDUs, onde circuitos adicionais são necessários. Duas PDUs redundantes, cada uma preferencialmente alimentada por um sistema UPS separado, devem ser fornecidas para atender a cada rack de equipamentos de informática; equipamento de computador de cabo único e três cabos deve ser fornecido com um comutador de transferência rápida montado em rack ou um comutador estático alimentado por cada PDU.

Alternativamente, as PDUs de comutação estática de alimentação dupla alimentadas a partir de sistemas UPS separados podem ser fornecidas para equipamentos de cabo único e de três cabos, embora esse arranjo ofereça menos flexibilidade e redundância. A codificação por cores das placas de identificação e dos cabos de alimentação para diferenciar as distribuições A e B deve ser considerada, por exemplo, todo o lado A branco, todo o lado B azul.

Um circuito não deve atender a mais de um rack para evitar que uma falha no circuito afete mais de um rack. Para fornecer redundância, os racks e gabinetes devem ter, cada um, dois circuitos elétricos dedicados de 120 ampères de 120 volts alimentados por duas unidades de distribuição de energia (PDUs) ou painéis elétricos. Para a maioria das instalações, os receptáculos elétricos devem estar travando os receptáculos NEMA L5-20R. Podem ser necessárias altas ampacidades para racks de alta densidade, e alguns servidores de nova tecnologia podem possivelmente requerer um ou mais receptáculos de 208 volts monofásicos ou trifásicos classificados para 50 amperes ou mais. Cada receptáculo deve ser identificado com o PDU e o número do circuito, que serve a ele. Recomenda-se o alimentador redundante para o quadro de distribuição do sistema mecânico, mas não é obrigatório.

O sistema de aterramento do prédio deve ser projetado e testado para fornecer uma impedância ao aterramento de menos de cinco ohms. Uma rede de ligação comum deve ser fornecida. Um sistema de desligamento de emergência (EPO) deve ser fornecido.

c) TIER 3

As instalações de Nível 3 devem atender a todos os requisitos do nível 2.

Todos os sistemas de uma instalação de nível 3 devem ter pelo menos N + 1 redun-

dância no módulo, caminho e nível do sistema, incluindo o gerador e os sistemas UPS, o sistema de distribuição e todos os alimentadores de distribuição. A configuração de sistemas mecânicos deve ser considerada ao projetar o sistema elétrico para garantir que a redundância N + 1 seja fornecida no sistema eletromecânico combinado. Esse nível de redundância pode ser obtido tanto fornecendo duas fontes de energia para cada unidade de ar condicionado, quanto dividindo o equipamento de ar condicionado entre várias fontes de energia. Alimentadores e quadros de distribuição são caminhos duplos, em que uma falha ou manutenção em um cabo ou painel não causará a interrupção das operações. Deve ser fornecida redundância suficiente para permitir o isolamento de qualquer item de equipamento mecânico ou necessária para manutenção essencial sem afetar os serviços que estão sendo fornecidos com resfriamento. Ao empregar uma configuração redundante distribuída, pontos únicos de falha são virtualmente eliminados da entrada do serviço de utilidade até o equipamento mecânico e até a PDU ou equipamento de computador.

Pelo menos dois alimentadores de serviços públicos devem ser fornecidos para atender o Data Center em média ou alta tensão (acima de 600 volts). A configuração do alimentador da rede elétrica deve ser seletiva primária, utilizando disjuntores de transferência automática ou chaves de transferência de derivação de isolamento automático. Como alternativa, uma configuração automática *main-tie-main* pode ser usada. Transformadores de distribuição tipo almofada, subestação ou tipo seco podem ser utilizados. Os transformadores devem ser configurados para redundância N + 1 ou 2N e devem ser dimensionados com base em classificações ao ar livre. Um sistema gerador de reserva é usado para fornecer energia ao sistema de fonte de alimentação ininterrupta e ao sistema mecânico. O armazenamento de combustível no local deve ser dimensionado para fornecer um mínimo de 72 horas de operação do gerador na condição de carregamento do projeto.

Interruptores de transferência automática de *bypass* de isolamento ou disjuntores de transferência automática devem ser fornecidos para detectar a perda de potência normal, iniciar a partida do gerador e transferir cargas para o sistema do gerador. Sistemas de bombeamento duplex devem ser fornecidos com controle automático e manual, com cada bomba alimentada a partir de fontes elétricas separadas. Devem ser fornecidos tanques de combustível e sistemas de tubulação redundantes e isolados para garantir que a contaminação do sistema de combustível ou a falha do sistema de combustível mecânico não afete todo o sistema do gerador. Partidas duplas redundantes e baterias devem ser fornecidas para cada motor do gerador.

Onde sistemas de paralelismo são empregados, eles devem receber sistemas de controle redundantes.

Para aumentar a disponibilidade de energia para a carga crítica, o sistema de distribuição é configurado em uma topologia redundante distribuída isolada (caminho duplo). Essa topologia requer o uso de chaves de transferência estáticas automáticas (ASTS) colocadas no lado primário ou secundário do transformador da PDU. Os requisitos de chaves de transferência estáticas automáticas (ASTS) são para carga de cabo único. Para o projeto de cabo com dois cabos (ou mais), proporcionando operação contínua com apenas um cabo energizado, nenhum interruptor de transferência estática automática (ASTS) é usado, desde que os cabos sejam alimentados por diferentes fontes do UPS. Os interruptores automáticos de transferência estática (ASTS) terão um circuito de *bypass* e um disjuntor de saída única.

Deve ser fornecida uma infraestrutura de aterramento do centro de dados e um sistema de proteção contra raios. A supressão de surto de voltagem transiente (TVSS) deve ser instalada em todos os níveis do sistema de distribuição de energia que atende às cargas eletrônicas críticas.

Um sistema central de monitoramento e controle de energia e ambiente (PEMCS) deve ser fornecido para monitorar todos os principais equipamentos elétricos, como painéis principais, sistemas geradores, sistemas UPS, chaves de transferência estática automática (ASTS), unidades de distribuição de energia, chaves de transferência automáticas, controle de motor centros, sistemas de supressão de surto de tensão transiente e sistemas mecânicos. Um sistema de controle lógico programável separado deve ser fornecido, programado para gerenciar o sistema mecânico, otimizar a eficiência, utilizar o ciclo do equipamento e indicar a condição de alarme.

Servidor redundante é fornecido para garantir monitoramento e controle contínuos em caso de falha do servidor.

d) TIER 4

As instalações de Nível 4 devem atender a todos os requisitos do nível 3.

As instalações de Nível 4 devem ser projetadas em uma configuração "2 (N + 1)"em todos os módulos, sistemas e caminhos. Todos os alimentadores e equipamentos devem ser capazes de *bypass* manual para manutenção ou em caso de falha. Qualquer falha transferirá automaticamente a energia da carga crítica do sistema com falha para um sistema alternativo sem interromper a energia para as cargas eletrônicas críticas.

Um sistema de monitoramento de bateria capaz de monitorar individualmente a impedância ou resistência de cada célula e a temperatura de cada jarro de bateria e alarmar a falha iminente da bateria deve ser fornecido para garantir o funcionamento adequado da bateria.

As entradas do serviço de utilidade pública devem ser dedicadas ao Data Center e isoladas de todas as instalações não críticas.

O edifício deve ter pelo menos dois alimentadores de concessionárias de diferentes subestações para redundância.

9.2.4 REQUISITOS DE SISTEMAS MECÂNICOS

a) TIER 1

O sistema HVAC de uma instalação de nível 1 inclui unidades de condicionamento de ar únicas ou múltiplas com capacidade de resfriamento combinada para manter a temperatura e a umidade relativa do espaço crítico em condições de projeto sem unidades redundantes. Se essas unidades de ar condicionado forem servidas por um sistema de rejeição de calor do lado da água, como um sistema de água gelada ou de condensador, os componentes desses sistemas também são dimensionados para manter as condições do projeto, sem unidades redundantes. O sistema ou sistemas de tubulação são de via única, pelo que uma falha ou manutenção em uma seção do tubo causará uma interrupção parcial ou total do sistema de ar condicionado.

Se um gerador for fornecido, todo o equipamento de ar condicionado deve ser alimentado pelo sistema gerador de reserva.

b) TIER 2

O sistema HVAC de uma instalação de nível 2 inclui várias unidades de ar condicionado com capacidade de resfriamento combinada para manter a temperatura e a umidade relativa do espaço crítico em condições de projeto, com uma unidade redundante (N + 1). Se essas unidades de ar condicionado são servidas por um sistema de água, os componentes desses sistemas são dimensionados do mesmo modo para manter as condições de projeto, com uma unidade redundante (s). O sistema ou sistemas de tubulação são de via única, pelo que uma falha ou manutenção em uma seção do tubo causará uma interrupção parcial ou total do sistema de ar condicionado.

Os sistemas de ar condicionado devem ser projetados para operação contínua 7 dias

/ 24 horas / 365 dias / ano e incorporar um mínimo de redundância N + 1 nas unidades CRAC (*Computer Room Air Conditioning*).

O sistema de condicionadores de ar de sala de computadores (CRAC) deve ser fornecido com redundância N + 1, com um mínimo de uma unidade redundante para cada três ou quatro unidades necessárias.

As salas de informática e outros espaços associados devem ser mantidos sob pressão positiva em salas não relacionadas ao Data Center, bem como ao ar livre.

Todos os equipamentos de ar condicionado devem ser alimentados pelo sistema de gerador de reserva.

Os circuitos de energia do equipamento de ar condicionado devem ser distribuídos entre vários painéis de energia / quadros de distribuição para minimizar os efeitos das falhas do sistema elétrico no sistema de ar condicionado.

Todos os sistemas de controle de temperatura devem ser alimentados através de circuitos dedicados redundantes do no-break.

O suprimento de ar para o Data Center deve ser coordenado com os tipos e *layouts* dos racks de servidores a serem instalados. A planta de tratamento de ar deve ter capacidade suficiente para suportar a carga de calor projetada total do equipamento, iluminação, ambiente, etc., e manter níveis constantes de umidade relativa dentro do Data Center. A capacidade de refrigeração necessária deve ser calculada com base no fornecimento de kW (não kVA) disponível no sistema UPS.

O ar condicionado deve ser distribuído para o equipamento através do espaço de acesso através de painéis de piso perfurados com amortecedores de balanceamento.

Um sistema de gerador de reserva a diesel deve ser instalado para fornecer energia ao sistema de fonte de alimentação ininterrupta e ao equipamento mecânico. Tanques de armazenamento de combustível no local devem ser dimensionados para fornecer um mínimo de 24 horas de operação do gerador na condição de carregamento do projeto. Sistemas de bombeamento duplex devem ser fornecidos com controle automático e manual, com cada bomba alimentada a partir de fontes elétricas separadas.

A redundância e o isolamento devem ser fornecidos no sistema de armazenamento de combustível para garantir que a contaminação do sistema de combustível ou uma falha no sistema de combustível mecânico não afete todo o sistema do gerador.

c) TIER 3

O sistema HVAC de uma instalação de nível 3 inclui várias unidades de ar condicionado com capacidade de resfriamento combinada para manter a temperatura e

umidade relativa do espaço crítico em condições de projeto, com unidades redundantes suficientes para permitir a falha ou manutenção de um quadro elétrico. Se essas unidades de ar condicionado forem servidas por um sistema de rejeição de calor do lado da água, como um sistema de água gelada ou de condensador, os componentes desses sistemas também são dimensionados para manter as condições do projeto, com um quadro elétrico removido de serviço. Esse nível de redundância pode ser obtido tanto fornecendo duas fontes de energia para cada unidade de ar condicionado, quanto dividindo o equipamento de ar condicionado entre várias fontes de energia. O sistema ou sistemas de tubulação são de caminho duplo, pelo que uma falha ou manutenção em uma seção do tubo não causará a interrupção do sistema de ar condicionado.

A alimentação elétrica deve ser fornecida com unidades alternadas de CRAC servidas a partir de painéis separados para fornecer redundância elétrica. Todas as unidades de condicionadores de ar de sala de computadores (CRAC) devem ter *backup* pela energia do gerador.

Equipamentos de refrigeração com redundância N + 1, N + 2, 2N ou 2 (N + 1) devem ser dedicados ao Data Center. Deve ser fornecida redundância suficiente para permitir o isolamento de qualquer item do equipamento, conforme necessário para manutenção essencial, sem afetar os serviços fornecidos com resfriamento.

Sujeito ao número de condicionadores de ar de precisão (PACs) instalados e à consideração dos fatores de manutenção e redundância, os circuitos de resfriamento dos condicionadores de ar de precisão (PACs) devem ser subdivididos. Se sistemas de água gelada ou resfriada a água forem usados, cada sub-circuito dedicado do Data Center deverá ter bombas independentes fornecidas a partir de um circuito central de anel de água. Um *loop* de água deve estar localizado no perímetro do Data Center e estar localizado em um subsolo para conter vazamentos de água para a área da calha. Sensores de detecção de vazamento devem ser instalados na calha. Deve-se considerar as voltas de água gelada totalmente isoladas e redundantes.

d) TIER 4

O sistema HVAC de uma instalação de nível 4 inclui várias unidades de ar condicionado com capacidade de resfriamento combinada para manter a temperatura e umidade relativa do espaço crítico nas condições de projeto, com unidades redundantes suficientes para permitir a falha ou manutenção de um quadro elétrico. Se essas unidades de ar condicionado forem servidas por um sistema de rejeição de

calor do lado da água, como um sistema de água gelada ou de condensador, os componentes desses sistemas também são dimensionados para manter as condições do projeto, com um quadro elétrico removido de serviço. Esse nível de redundância pode ser obtido tanto fornecendo duas fontes de energia para cada unidade de ar condicionado, quanto dividindo o equipamento de ar condicionado entre várias fontes de energia. O sistema ou sistemas de tubulação são de caminho duplo, pelo que uma falha ou manutenção em uma seção do tubo não causará a interrupção do sistema de ar condicionado. Recursos alternativos de armazenamento de água devem ser considerados quando sistemas de evaporação estão em vigor para um sistema de nível 4.