DJALMA RAFAEL TEIXEIRA

MODELO CONCEITUAL DE MONITORAMENTO E GERENCIAMENTO PARA *SMART DATACENTERS*

Três de Maio

2019

DJALMA RAFAEL TEIXEIRA

MODELO CONCEITUAL DE MONITORAMENTO E GERENCIAMENTO PARA *SMART DATACENTERS*

Trabalho de Conclusão de Curso apresentado à Faculdade Três de Maio - SETREM para obtenção do grau de Tecnólogo em Redes de Computadores.

Orientador:

Dr. Dalvan Griebler

Co-orientador:

M. Sc. Adriano Vogel

Três de Maio

2019

TERMO DE APROVAÇÃO

DJALMA RAFAEL TEIXEIRA

MODELO CONCEITUAL DE MONITORAMENTO E GERENCIAMENTO PARA SMART DATACENTERS

Relatório aprovado como requisito parcial para obtenção do título de **Tecnólogo em Redes de Computadores** concedido pela Faculdade de Redes de Computadores da Sociedade Educacional Três de Maio, pela seguinte Banca examinadora:

Orientador: Prof. Dalvan Jair Griebler, Dr.
Faculdade de Tecnologia em Redes de Computadores da SETREM.

Orientador: Prof. Adriano José Vogel, M. Sc.
Faculdade de Tecnologia em Redes de Computadores da SETREM.

Prof. Priscila Guarienti, M. Sc.
Faculdade de Sistemas de Informação da SETREM.

Prof. Fernando Krein Pinheiro, M. Sc.
Faculdade de Sistemas de Informação da SETREM.

Prof. Vera Lúcia Lorenset Benedetti, M.Sc.
Coordenação do Curso Tecnologia em Redes de Computadores
Faculdade de Redes de Computadores da SETREM.

Três de Maio, 17 de Junho de 2019.

RESUMO

A demanda por *datacenters* inteligentes vem aumentando consideravelmente devido a complexidade de gerenciamento das infraestruturas atuais, que ocorre devido à crescente necessidade por recursos computacionais dentro das organizações. O presente trabalho tem como objetivo propor um modelo de gerenciamento e monitoramento inteligente para *datacenters* e testar sua eficácia através da implantação parcial do mesmo. Foi realizado um levantamento completo da infraestrutura física, rede lógica e dos serviços na infraestrutura de TI do LARCC. Por meio dos resultados obtidos, foi feita a classificação do *datacenter* do laboratório de acordo com os requisitos exigidos pelo norma ANSI TIA 942. Através da análise e da pesquisa realizada por trabalhos relacionados, foi elaborado um modelo conceitual para monitoramento e gerenciamento inteligente para infraestruturas computacionais, o qual foi dividido em cinco grande áreas: climatização, energia, computação, rede e segurança. Também foram definidos os eventos que afetam estes elementos, como monitorá-los e como gerenciá-los baseando-se na abordagem de computação autônoma. Com isso, foram implantados os modelos referentes a temperatura e energia, que utiliza ações reativas para abordar e conter consequências de superaquecimento e queda de energia. Para implementação deste fluxo de ações foi utilizada a ferramenta *Zabbix*, e sua função de execução de comandos remotos para aplicação prática do modelo. Conclui-se que o modelo conceitual proposto tem maior eficácia na contenção de eventos críticos que possam vir a afetar a infraestrutura estes resultados foram testados e validados na prática para os elementos de temperatura e energia.

Palavras-chave: Redes de Computadores, Smart Datacenter, Modelo conceitual, Monitoramento, Gerenciamento.

ABSTRACT

The demand for smart datacenters has been increasing considerably due to the complexity of managing the current infrastructures, which is due to the increasing need for computing resources within organizations. The present work aims to propose a model of intelligent management and monitoring for datacenters and to test its effectiveness through the partial implementation of the same. A complete survey of the physical infrastructure, logical network and services in the LARCC IT infrastructure was carried out. By means of the results obtained, the classification of the datacenter of the laboratory was made according to the requirements of ANSI TIA 942. Through the analysis and research carried out by related works, a conceptual model for monitoring and management was elaborated intelligent for computer infrastructures, which was divided into five major areas: air conditioning, energy, computing, network and security. We also defined the events that affect these elements, how to monitor them and how to manage them based on the autonomous computing approach. With this, the models were implemented regarding temperature and energy, which uses reactive actions to address and contain consequences of overheating and energy loss. To implement this flow of actions was used the tool Zabbix, and its function of executing remote commands for practical application of the model. It is concluded that the proposed conceptual model is more effective in the containment of critical events that may affect the infrastructure, these results were tested and validated in practice for the elements of temperature and energy.

Keywords: Network Computing, Smart Datacenter, Conceptual Model, Monitoring, Management.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

AC	Ar Condicionado
API	*Application Programming Interface*
CPU	*Central Process Unit*
CPS	*Cyber-Physical System*
EPO	*Emergency Power Off*
HD	*Hard Drive*
IDC	*Internet Datacenter*
IaaS	*Infrastructure as a Service*
IoT	*Internet Of Things*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
LARCC	Laboratório de pesquisa avançada de computação em nuvem
LDAP	*Lightweight Directory Access Protocol*
MAC	*Mandatory Access Control*
NFPA	*National Fire Protection Association*
PaaS	*Platform as a service*
SETREM	Sociedade Educacional Três de Maio
RAM	*Random Access Memory*
SaaS	*Software as a Service*
SLA	*Service Level Agreement*
SNMP	*Simple Network Management Protocol*
TIA	*Telecommunications Industry Association*
TI	Tecnologia da Informação

VM	*Virtual Machine*
WSN	*Wireless Sensor Networks*

SUMÁRIO

INTRODUÇÃO

A crescente demanda pelo uso da computação em nuvem impulsionou um crescimento nas infraestruturas dos *datacenters* provedores deste serviço. A computação em nuvem revolucionou a forma de oferecer e cobrar por serviço, trazendo vantagens para usuários e provedores. Exemplos de vantagens são alocação de recursos sob demanda, acesso rápido e fácil, alta disponibilidade e baixo investimento inicial.

No entanto, o aumento no uso de Computação em Nuvem demanda que ambientes de *datacenters* ofereçam um aumento contínuo no poder computacional disponível. Isso faz com que *datacenters* necessitem um crescente aumento no espaço físico e na quantidade de equipamentos. Em consequência disso, ocorre uma série de problemas como aumento do consumo de energia, geração de calor e o crescimento da complexidade no gerenciamento da infraestrutura. O monitoramento inteligente é uma alternativa para redução do custo operacional e otimização do gerenciamento dos recursos disponíveis na infraestrutura.

No entanto, ainda existe escassez de pesquisas que sirvam de base para que *datacenters* mais básicos possam seguir e implantar um modelo de gestão mais inteligente. Deste modo, buscou-se propor um modelo de monitoramento e gerenciamento inteligente que seja adaptável a heterogeneidade das infraestruturas atuais.

Este estudo tem como objetivo propor um modelo conceitual de monitoramento e gerenciamento para *smart datacenter*, desenvolvendo o estudo de nor-

mas, métricas e uma pesquisa bibliográfica referente ao tema. Além disso, se objetiva implantar parte deste modelo na infraestrutura do LARCC, a fim de validar a proposta. Consequentemente, a contribuições deste trabalho são as seguintes:

- Organização e convergência das normas (TIA 942) para simplificar o processo de classificação de *datacenter*.
- Classificação do *datacenter* do LARCC para dimensionar os níveis de alta disponibilidade atuais e pretendidos.
- Modelo conceitual de monitoramento e gerenciamento para *Smart Datacenter* que simplifica o processo de implantação.
- Validação do modelo na prática referente a energia e temperatura com base nos princípios da computação autonômica. Os experimentos demonstraram a aplicabilidade do modelo conceitual em um ambiente real.

O trabalho está estruturado em três capítulos: o Capítulo 1 descreve a proposta do trabalho a justificativa para sua realização, o levantamento das hipóteses e sua problematização. O mesmo também descreve a metodologia utilizada, juntamente com o cronograma e orçamentos utilizados. O Capítulo 2 aborda o referencial teórico, onde foi pesquisado os conceitos e temas abordados no trabalho como *datacenters*, computação em nuvem, monitoramento de ambientes computacionais e *datacenters* inteligentes, além dos trabalhos relacionado selecionados neste estudo.

No Capítulo 3, foram descritos e apresentados o levantamento físico e lógico dos serviços executados do ambiente, a classificação atual da infraestrutura do LARCC de acordo com a norma ANSI TIA 942, o desenvolvimento do modelo conceitual, os testes de implantação do mesmo e os resultados obtidos pela implantação parcial da proposta de monitoramento e gerenciamento para *smart datacenters*.

CAPÍTULO 1: ASPECTOS METODOLÓGICOS

Este capítulo apresenta os aspectos metodológicos que auxiliam na pesquisa desenvolvida para realização do trabalho.

1.1 TEMA

O tema deste estudo é uma proposta de um modelo conceitual de monitoramento e gerenciamento para *Smart DataCenters*.

1.2 DELIMITAÇÃO DO TEMA

Este trabalho propõe a criação de um modelo conceitual de monitoramento e gerenciamento para *smart datacenter*. O foco está na redução do consumo energético dos servidores e na prevenção do superaquecimento de componentes através de ações pró-ativas. Também foi realizada a implementação experimental do modelo conceitual respectivo ao foco do trabalho. Isso foi feito na infraestrutura do Laboratório de Pesquisas Avançadas para Computação em Nuvem - LARCC da Faculdade Três de Maio - SETREM, com o intuito de validar a abordagem proposta.

O LARCC é um laboratório que fornece estrutura e computadores de alto desempenho para a realização de pesquisas acadêmicas na SETREM. Sua infraestrutura se encontra em processo de crescimento para se tornar um *datacenter* de computação em nuvem. Embora não seja certificado, o ambiente permite realizar experimentos próximos da realidade.

O modelo conceitual proposto no presente trabalho foi baseado em normas já estabelecidas (por exemplo, ANSI TIA 942 A (TIA-942, 2012) e ISO 27002 (ISO, 2013) utilizadas para classificação e qualificação de *datacenters*. Os experimentos de implantação irão usar ferramentas existentes, tais como Zabbix (DOCUMEN-

TATION, 2008) ou Nagios, (GALSTAD, 2008) bem como customizar os ambientes com Scripts.

O presente trabalho foi desenvolvido como Trabalho de Conclusão do Curso de Redes de Computadores da Faculdade Três de Maio - SETREM, no período de Julho de 2018 à Julho de 2019, tendo como área específica o monitoramento e gerenciamento de elementos fundamentais para o funcionamento de um *datacenter* moderno.

1.3 PROBLEMA

Segundo Viswanathan, Lee e Pompili (2011), o gerenciamento de *datacenters* modernos está excedendo rapidamente a capacidade humana, tornando essenciais as abordagens autonômicas. Para Norouzi e Bauer (2015), a crescente complexidade dos *datacenters* levou pesquisadores a investigar formas de utilizar cada vez mais métodos inteligentes para gerenciamento de infraestruturas. como por exemplo: auto-gerenciamento, monitoramento proativo e reativo, agendamento de tarefas, balanceamento da carga de trabalho dos servidores entre outras.

Utilizar o conceito *smart datacenter* é uma forma de alcançar uma solução para os tradicionais problemas que ocorrem em infraestruturas computacionais, como por exemplo, o aumento do consumo energético dos servidores ou superaquecimento de seus componentes em função de um eventual problema de refrigeração. No entanto, não foram encontradas normas, guias de boas práticas, modelos ou definições de gerenciamento e monitoramento de *smart datacenters* até o presente momento.

Desta forma, este trabalho busca propor um modelo conceitual para auxiliar no monitoramento e gerenciamento de *smart datacenters*. Além disso, o projeto busca responder a seguinte pergunta. A implantação do modelo conceitual referente ao gerenciamento e monitoramento dos recursos computacionais permite reduzir o consumo de energia e evitar o superaquecimento de servidores?

1.4 HIPÓTESES

Nesta seção serão apresentadas as hipóteses levantadas para chegar a um solução para o problema da pesquisa através da corroboração ou não das mesmas.

- A implantação do modelo conceitual permite gerenciar a temperatura dos servidores de forma autonômica e evitar superaquecimento de componentes.
- A implantação do modelo conceitual permite gerenciar os recursos dos servidores de forma autonômica para a redução do consumo energético.

1.5 OBJETIVOS

Nesta seção estão descritos os objetivos que o presente trabalho busca alcançar.

1.5.1 Objetivo Geral

Propor um modelo conceitual de monitoramento e gerenciamento para *smart datacenter* e implantar parte do mesmo na infraestrutura do LARCC para validar a abordagem.

1.5.2 Objetivos Específicos

Nesta seção estão descritos os objetivos específicos, essenciais para definir quais são as tarefas necessárias para alcançar o principal objetivo do trabalho.

- Entender o conceito de smart datacenter.
- Estudar e entender a infraestrutura computacional do LARCC.
- Identificar e interligar os conceitos relativos ao modelo conceitual.
- Implantar a parte do modelo conceitual relativo ao monitoramento e gerenciamento da temperatura dos servidores.
- Implantar a parte do modelo conceitual relativo ao monitoramento e gerenciamento do consumo energético dos servidores.

- Avaliar experimentalmente o modelo conceitual para gerenciamento inteligente de energia.
- Avaliar experimentalmente o modelo conceitual para gerenciamento inteligente de temperatura.

1.6 JUSTIFICATIVA

O crescimento das redes de computadores tem exigido um avanço considerável nas infraestruturas necessárias para o funcionamento dos *datacenters*. De acordo com Yogendra e Pramod (2012), *datacenters* são ambientes projetados para concentrar servidores, equipamentos de rede e armazenamento de informação, bem como prover uma grande variedade de serviços intolerantes a interrupções. Para garantir a disponibilidade destes serviços a estrutura requer um ambiente adequado com segurança, climatização e redundância energética, além de um monitoramento constante de todos os recursos computacionais.

No entanto, os *datacenters* atuais consomem uma grande quantidade de energia, devido ao hardware robusto dos servidores, climatização e a necessidade de disponibilidade em tempo integral, o que gera altos custos para manter sua estrutura. Segundo Koomey (2011), *datacenters* consomem cerca de 1,3% da oferta mundial de eletricidade, e este nível deverá aumentar para 8% até 2020. O gerenciamento autonômico procura usar os recursos do *datacenter* de forma eficiente, tendo em vista o sistema de tarifas e bandeiras da ANEEL executando o maior volume de serviços em horários com menor custo do KVH, visando diminuir o custo operacional energético do data center.

Segundo Norouzi e Bauer (2015), serviços de *cloud computing* são os principais responsáveis pelo grande aumento de proporções nos *datacenters* atuais. E tem sido cada vez mais procurados tanto por usuários domésticos como empresariais, devido a fatores como preço, alta disponibilidade e alocação de recursos computacionais conforme a necessidade dos clientes, exigindo infraestruturas cada vez mais robustas para suportar o crescimento desta demanda. Um *datacenter* de computação em nuvem deve permanecer acessível em tempo integral e garantir praticidade e segurança as aplicações nele hospedadas. Desta forma, o monito-

ramento desta infraestrutura se faz necessário, para disponibilizar uma completa visibilidade além de analisar e gerenciar o funcionamento da infraestrutura.

A complexidade dos *datacenters* atuais levou pesquisadores a investigar formas de usar métodos autonômicos para gerenciamento de data center. Hoje, existem diversas ferramentas para monitoramento e gerenciamento para infraestruturas, cada uma delas com suas singularidades e limitações. Este trabalho visa avaliar e aplicar uma delas na infraestrutura estudada para monitorar de forma inteligente o laboratório de pesquisa de computação em nuvem - LARCC.

O monitoramento e gerenciamento inteligente de *datacenters* busca reduzir esta complexidade em administrar as infraestruturas computacionais, que ocorre devido ao crescimento em proporções (tamanho) e de quantidade de serviços disponibilizados. Além de buscar a redução de custos operacionais dos *datacenters*, e oferecer praticidade na operação e manutenção dos recursos.

Também busca garantir a integridade dos equipamentos através de acões pró ativas, permitindo melhor desempenho e aumento de disponibilidade. Atualmente, existem poucos materiais definindo o que é *smart datacenter*, portanto, este trabalho busca realizar um estudo na literatura e propor um modelo aplicável de gerenciamento de infraestrutura.

Para isso serão consideradas normas já estabelecidas, como por exemplo, ANSI TIA 942 A e ISO 27002, que são referências no controle de infraestruturas de *datacenter* e servirão como base para o desenvolvimento do modelo conceitual de monitoramento e gerenciamento para *smart datacenter* com foco na redução do consumo energético dos servidores e na prevenção do superaquecimento de componentes. Também contribui com a implantação de parte do modelo no LARCC, na qual serão analisadas as mudanças e melhorias consequentes da aplicação.

1.7 METODOLOGIA

Segundo Lovato (2013) Metodologia da pesquisa é o ramo da ciência que pesquisadores utilizam para alcançarem o resultado final de seus estudos. Tem como objetivo conduzir a um ampliação do conhecimento, levando em conta o raciocínio, os procedimentos e as técnicas para validação dos resultados alcançados.

1.7.1 Abordagem

Segundo Lovato (2013) pesquisa dedutiva parte de um conhecimento abstrato podendo ser uma lei geral, uma teoria, ou uma hipótese aceita temporariamente como verdade.

A pesquisa parte da dedução de por meio das ferramentas, dispositivos, métricas e normas atualmente disponíveis será possível desenvolver um modelo funcional e eficiente de monitoramento e gerenciamento inteligente para *smart datacenter*, evitando riscos de avariações de hardware causadas por superaquecimento e monitoramento e controle do consumo energético dos servidores em uma infraestrutura de TI heterogênea.

Para Lovato (2013) existem duas dimensões para os métodos de abordagem, a primeira diz respeito a qual tipo de raciocínio foi utilizado, já a segunda segunda fala se serão ou não utilizados dados estatísticos.

Também foi utilizado o método de abordagem quali-quantitativo, uma vez que o modelo proposto nesta pesquisa trabalha diferentes conceitos para chegar a uma conclusão. E também para o estudo de dados numéricos obtidos por meio do monitoramento da infraestrutura como tráfego de rede, consumo energético e temperatura dos servidores e seus componentes.

1.7.2 Procedimentos

De acordo com Marconi e Lakatos (2017) pesquisa bibliográfica é aquela que abrange toda a bibliografia já publicada com relação ao tema do trabalho, por exemplo, liros, revistas, artigos acadêmicos etc. Tem por objetivo o acesso a tudo que foi escrito, dito ou filmado sobre determinado assunto.

Foi desenvolvido um estudo bibliográfico referente a monitoramento inteligente de data centers, afim de levantar informações necessárias para desenvolver um modelo conceitual que informe quais são os requisitos necessários para definir monitoramento e gerenciamento de infraestruturas computacionais inteligentes.

O presente trabalho busca formas de comparar ferramentas de monitoramento *open source*, métricas de medição de desempenho e abordagens inteligen-

tes de gerenciamento, para determinar quais são as características necessárias para que uma infraestrutura de *Smart datacenter* possa ser controlada de forma inteligente, além de definir quais itens são importantes monitorar?

De acordo com Marconi e Lakatos (2017) pesquisa exploratória busca formular um problema com o objetivo de desenvolver hipóteses, aumentar o conhecimento do pesquisador sobre o tema estudado modificar e aumentar a visibilidade dos conceitos. Também procura obter descrições tanto qualitativas quanto qualitativas do estudo, e as relações entre propriedades do fenômeno fato ou ambiente observado.

1.7.3 Validação

Para realizar a validação da primeira hipótese que tem como pressuposto, que a implantação do modelo conceitual permite gerenciar a temperatura dos servidores de forma autonômica e evitar superaquecimento de componentes serão executados os seguintes procedimentos, levantamento e mapeamento da infraestrutura do LARCC, implementação do monitoramento da temperatura dos servidores, estudo de técnicas de gerenciamento pró ativo para desligar máquinas que excedam o limite de temperatura que será definido no modelo conceitual.

Para a validação da segunda hipótese que tem como pressuposto que a implantação do modelo conceitual permite gerenciar os recursos dos servidores de forma autonômica para redução do consumo energético, serão executados os seguintes procedimentos, testar formas de mensurar o consumo energético dos servidores, testar abordagens inteligentes para reduzir a atividade do *hardware*, evitando o desperdício de energia e analisar os resultados obtidos afim de estudar possíveis melhorias.

1.7.4 Técnicas

Segundo Marconi e Lakatos (2017) técnica corresponde a um conjunto de processos e preceitos que seguem uma ciência ou arte, bem como a habilidade para colocá-los em prática.

Para Marconi e Lakatos (2017) a técnica de testes funciona como um ins-

trumento com objetivo de obter dados para medir o desempenho, rendimento, comportamento e competência de algo de forma quantitativa. Os testes são um excelente forma para coletar informações e analisar comportamentos.

O presente trabalho utilizará a técnica de testes com o objetivo de determinar quais são as melhores formas para coletar e tratar dados obtidos através do monitoramento da infraestrutura do *datacenter* estudado. Além de testar abordagens inteligentes para gerenciar a temperatura dos servidores de modo a evitar avariações de componentes e consumo energético dos servidores do LARCC.

1.8 CRONOGRAMA

O cronograma é uma etapa importante do projeto de pesquisa, pois apresenta de forma detalhada todas as etapas de trabalho, bem como o período de realização de cada etapa.

Quadro 1: Cronograma

Atividade	**2018**				**2019**					
	Set	**Out**	**Nov**	**Dez**	**Jan**	**Fev**	**Mar**	**Abr**	**Mai**	**Jun**
Escrita do projeto de TCC			X							
Estudo Bibliográfico	X	X	X	X	X					
Estudar normas e métricas			X	X						
Revisão de trabalhos relacionados				X						
Levantamento de infraestrutura					X	X				
Classificação Atual do datacenter							X			
Propor Modelo conceitual							X	X		
Avaliação prática do modelo								X	X	
Analisar e documentar os resultados									X	

Previsto	
Realizado	X

1.9 ORÇAMENTO

Para realização deste trabalho foi previsto os itens descritos no Quadro 2 abaixo.

Quadro 2: Orçamento

Itens	Quantidade	Valor Unitário	Valor Total
Impressões	200	R$0,15	R$
Horas Trabalhadas	450	R$45,00	R$20.250,00
Encadernação espiral	4	R$3,00	R$12,00
Encadernação capa dura	2	R$70,00	R$140,00
Valor Total			R$20.432,00

CAPÍTULO 2: FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica tem como objetivo apresentar os estudos realizados por outros autores sobre os temas, apresentando e analisando o pensamento dos estudiosos sobre os assuntos apresentados no mesmo.

2.1 DATACENTERS

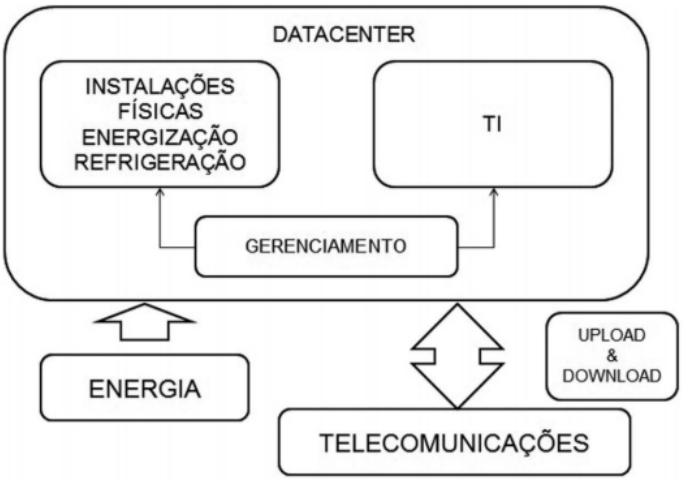
De acordo com Veras (2012) *datacenter* é um conjunto de componentes altamente tecnológicos com objetivo de prover serviços de infraestrutura de TI em grande escala, sendo intolerante a falhas e interrupções. Com o aumento constante das demandas computacionais e o paradigma emergente da computação em nuvem, esses ambientes vem se tornando cada vez maiores e complexos tendendo a ultrapassar a capacidade humana de gerenciamento.

Segundo Veras (2012) atualmente os *datacenters* estão sendo construídos visando o aumento constante da demanda por poder computacional, as normas de fiscalização e a recuperação da infraestrutura em caso de um desastre. A localização física das instalações é determinada levando em conta o seguintes fatores: condições de fornecimento de energia, telecomunicações e clima.

Normalmente os *datacenters* são definidos em três grandes blocos: instalações (instalações físicas, equipamentos de energia e sistema de refrigeração), que tem o objetivo de assegurar o funcionamento correto da infraestrutura por meio da entrega de energia redundante, temperatura ideal para evitar aquecimento de hardware e espaço físico capaz de comportar todos os equipamentos. Gerenciamento que diz respeito ao controle e monitoramento de todos os recursos do *datacenter*, com objetivo de melhorar e centralizar a administração da infraestrutura. E TI que diz respeito a ao poder e recursos computacionais, e serviços sendo

executados e providos como ilustrado na Figura 1.

Figura 1: *Datacenter*.



Fonte: Extraída de Veras (2012)

Segundo a TIA-942 (2012) o planejamento de um *datacenter* é uma etapa altamente vulnerável a erros, portanto deve ser feita visando os aspectos da norma.

Segundo Ebbers e Archibald et al. (2011), ao mesmo tempo, os avanços tecnológicos permitem que mais trabalho seja feito em uma área física menor. À medida que mais servidores lotam o mesmo ambiente físico, a capacidade não é mais ditada simplesmente pela disponibilidade espacial. Energia, resfriamento, rede, armazenamento e outras métricas de capacidade também devem ser gerenciadas. Preocupações ambientais e regulamentações governamentais associadas introduzem um foco nas emissões de carbono. Todas essas tendências convergem em um único local: o data center.

2.1.1 Sistema energético de *datacenters*

Segundo Veras (2012) o *datacenter* é o elemento chave para toda infraestrutura de TI, no entanto seus componentes de alto desempenho resultam em um alto consumo de energia. Deste modo o primeiro passo para obter melhorias e projetá-lo de acordo com aspectos de eficiência energética. Este fator era anteriormente medido, visando apenas poder computacional e disponibilidade. Atualmente são considerados aspectos com sustentabilidade ao montar uma estrutura.

Segundo Jayaswal (2005) o sistema energético de *datacenter* inclui transformadores elétricos, painéis de distribuição de energia, disjuntores, fiação, mecanismo de aterramento, tomadas de energia utilizadas para o equipamento e fontes de energia de backup com alimentação ininterrupta (UPS) além de fontes externas como geradores.

Um sistema elétrico para *datacenters* bem projetado possui as seguintes características: fornecer energia suficiente para alimentar o hardware e redundância adequada sem pontos de falha para evitar interrupção dos serviços devido queda de energia e conformidade com padrões de segurança locais.

Segundo Ebbers e Archibald et al. (2011) o consumo de energia de um *datacenter* pode ser analisado tomando três visões diferentes: a energia é distribuída entre equipamentos de TI (servidores, armazenamento, equipamentos de rede) e instalações de suporte (energia, refrigeração e iluminação), Como a energia é distribuída entre os componentes separados dos equipamento de TI (processador, memória, disco e assim por diante) e como a energia alocada aos recursos de TI é realmente usada para produzir resultados de negócios (os recursos ociosos são ativados usando energia sem resultados produtivos?).

2.1.2 Cabeamento Estruturado

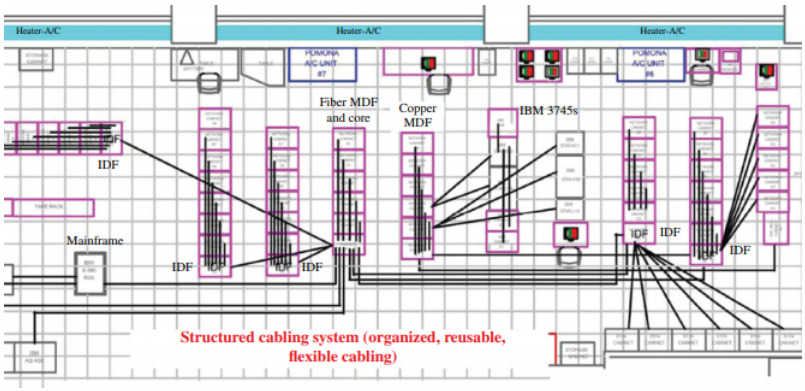
O *datacenter* é o local onde se encontra a centralização dos componentes responsáveis por prover os serviços e telecomunicações em uma infraestrutura de TI. Os dados transmitidos e as inúmeras conexões entre componentes como servidores, *switches* e demais equipamentos de rede são inter-relacionas e conectadas pelo sistema de cabeamento estruturado, o qual é projetado para oferecer uma melhor escalabilidade, flexibilidade de gerenciamento, disponibilidade e menor custo total de propriedade.

Segundo Geng (2014) em *datacenters* sem cabeamento estruturado os cabos são simplesmente instalados diretamente entre dois equipamentos que precisam ser conectados. Porém desta forma sempre que ocorrerem mudanças na infraestrutura, a não padronização descarta a possibilidade de reutilizar o cabeamento, fazendo com que esse material seja descartado, além de dificultar a orga-

nização do ambiente.

De acordo com Geng (2014) o cabeamento estruturado apresenta as seguintes vantagens para uma infraestrutura: Melhora a forma de utilizar e expandir e adicionar redundância e divisão e padronização para melhorar o gerenciamento do *datacenter*. A Figura 2 ilustra uma estrutura de cabeamento estruturado que oferece flexibilidade para expansão e mudanças, além de um layout mais limpo que facilita o gerenciamento. Neste modelo ocorre um aumento na disponibilidade pois a identificação dos cabos agiliza a manutenção.

Figura 2: Cabeamento Estruturado.



Fonte: Extraída de Geng (2014)

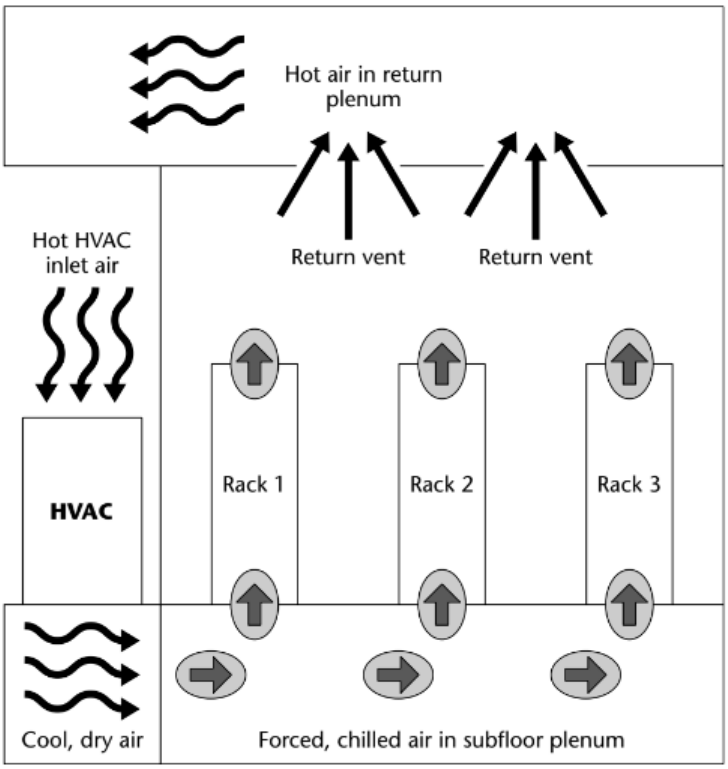
2.1.3 Sistema de refrigeração de *datacenters*

Os principais e mais robustos equipamentos de hardware utilizados nas organizações são agrupados e armazenados nos *datacenters*, consequentemente causando uma grande quantidade de calor no ambiente. Deste modo, para controlar a temperatura ambiente e evitar interrupções causadas por superaquecimento, são utilizados sistemas de refrigeração específicos. No entanto a climatização juntamente com equipamento de TI causa um grande consumo de energia.

Visto que os *datacentes* gastam muita energia é importante otimizar o uso do HVAC, (*Healting, Ventilation and Air Conditioning*), que é composto por três mecanismos: aquecimento, ventilação e ar-condicionado. De acordo com Jayaswal (2005) estas unidades operam em tempo integral porém exigem uma série de manutenções programadas, o que torna necessária uma redundância para estes equipamentos, em caso de falhas ou para intervalos de manutenção.

A Figura 3 ilustra um sistema HVAC, onde ar retira o calor do equipamento que flui ao redor e dentro dele, e depois é ejetado para o outro lado (corredor quente). O equipamento deve estar voltado para ou longe do ar forçado, para obter um resfriamento ideal.

Figura 3: Sistema HVAC.



Fonte: Extraída de Jayaswal (2005)

Segundo Ebbers e Archibald et al. (2011) grande parte dos *datacenters* têm agora 10 a 20 anos e suas instalações de resfriamento não estão adaptadas às necessidades presentes. Os métodos tradicionais de resfriamento permitem 2-3 kW de resfriamento por rack. Os requisitos de hoje podem atingir de 20 a 30 kW por rack, e a densidade de calor pode facilmente gerar "pontos quentes"em racks onde estão concentrados servidores com uma maior carga de trabalho .

2.1.4 Segurança de ambiente datacenter

Os *datacenters* atuais tem a missão de fornecer alta disponibilidade de serviços e recursos de TI , além de complexidade de seu gerenciamento e o grande volume de dados e informações trafegados, tendo isso em vista manter o ambiente

seguro é fundamental. Segundo Oliveira (2018) o objetivo das políticas de segurança físicas é, principalmente prevenir o acesso não autorizado as instalações.

De acordo com a ISO (2013) é necessário que ambiente *datacenter* tenha segurança física contra possíveis roubos de equipamentos que contenham informaçõe e dados referentes a organização.

2.1.5 Norma para classificação de *datacenters* TIA 942 A

Para padronizar e classificar o nível de criticidade dos projetos de instalações dos *datacenters*, é utilizado um conjunto de normas chamado ANSI TIA 942 (*Telecommunications Industry Association*). Segundo Veras (2012) a norma TIA-942 é responsável por definir quais os requisitos mínimos de telecomunicação para infraestruturas computacionais. Esta norma trata de diversos aspectos referentes a *datacenters*, desde o *layout* do espaço físico, infraestrutura de cabeamento, aspectos mecânicos e elétricos, além da principal contribuição da norma que é a classificação das infraestruturas em quatro niveis (Tier I, Tier II, Tier III e Tier IV).

Tier I: Neste nível são fornecidadas as condições básicas de segurança, arquitetura, mecânica, eletricidade e telecomunicações para que uma infraestrutura seja classificada como *datacenter*, são elas:

- não mais que 28,8 horas de tempo de inatividade por ano. Estas instalações são permitidas a maior quantidade de tempo de inatividade de qualquer nível.
- Redundância zero. Este nível de uma instalação não tem redundância em nenhuma parte de suas operações.
- as instalações não possuem nenhuma garantia de redundância dentro de seu processo de certificação de energia e resfriamento.
- 99,671% de uptime por ano. Esta é a menor quantidade de tempo de atividade que uma instalação classificada pelo Uptime Institute pode produzir.

Tier II: neste nível o *datacenter* possui capacidade redundante de energia e resfriamento e fornece oportunidades de manutenção selecionadas além de uma margem maior de segurança contra interrupções no processo de TI.

- Não mais do que 22 horas de inatividade por ano. Há um salto considerável entre os níveis II e III em relação ao tempo de inatividade. A redundância é uma das principais razões para isso.
- 99.741% de *uptime* por ano. Essa é uma quantidade mínima de tempo de atividade que esse provedor pode produzir em um ano.
- Resfriamento parcial e várias redundâncias de energia. Um fornecedor de Nível II não desfruta de redundância em todas as áreas de operação. Os aspectos mais críticos de sua estrutura mecânica recebem prioridade. Esses dois aspectos são distribuição de energia e resfriamento. A redundância nessas áreas é apenas parcial. Nenhuma parte do sistema é tolerante a falhas.

Tier III: Possibilita manutenções e substituições de componentes sem desligamento dos servidores do *datacenter*, se diferencia das camadas anteriores por apresentar um foco muito maior na proteção do sistema para garantir a integridade dos dados e informações trafegadas no *datacenter*.

- 99,982% de tempo de atividade (nível 3 de tempo de atividade).
- Não mais do que 1,6 horas de tempo de inatividade por ano.
- N + 1 tolerante a falhas fornecendo pelo menos 72 horas de proteção contra falta de energia.

Tier IV: Neste nível os *datacenters* possuem dois caminhos de distribuição de energia e resfriamento ativos simultaneamente, além de componentes redundantes em cada caminho os quais devem tolerar qualquer falha de equipamento sem afetar a carga de trabalho da infraestrutura.

- Sem pontos de falha. Os provedores de nível IV têm redundâncias para todo processo e fluxo de proteção de dados. Nenhuma falha ou erro único pode desligar o sistema.
- 99,995% de tempo de atividade por ano. Este é o nível com o maior tempo de atividade garantido. Deve ser mantido por um centro para manter o ranking de Nível IV.

- Não mais do que 26,3 minutos de inatividade por ano como valor máximo. Os provedores devem permitir algum tempo de inatividade para operações mecânicas otimizadas; no entanto, esse tempo de inatividade anual não afeta as operações voltadas ao cliente.

- 96 horas de proteção contra falta de energia. Uma infraestrutura de nível IV deve ter pelo menos 96 horas de energia independente para se qualificar nesse nível. Este poder não deve ser conectado a nenhuma fonte externa e é inteiramente proprietário. Alguns centros podem ter mais.

De acordo com a TIA-942 (2012) é necessário definir um nível de criticidade e padronizar o *datacenter* baseando-se na norma, para determinar uma classificação para a infraestrutura. A TIA 942 é baseada em um conjunto de normas relacionadas a estruturação de ambientes computacionais, são elas:

- TIA/EIA 568: norma utilizada para planejamento do cabeamento estruturado em ambientes computacionais como *datacenters* por exemplo. Também define um padrão para comprimento, conectores e padrões de telecomunicação entre os cabos. Seu objetivo é fornecer melhores práticas para a instalação de projetos de cabeamento de redes.

- TIA/EIA 569: esta norma é utilizada para definir a área ocupada pelos componentes do cabeamento estruturado, isso inclui dimensões e encaminhamento de espaços. É um padrão para construção comercial de espaços de telecomunicações.

- TIA/EIA 606: a norma tem como objetivo administração, etiquetagem e documentação de infraestruturas de cabeamento de telecomunicações, além de contribuir com o prolongamento da vida útil da estrutura, e reduzir custos de gerenciamento de mudanças e contribuir com a rápida recuperação de disponibilidade.

- TIA/EIA 607: esta norma fornece princípios básicos, componentes e design de ligações de telecomunicações e aterramento que devem ser seguidas para

garantir que os sistemas de ligação e aterramento de telecomunicações em um edifício tenham um potencial elétrico.

2.2 COMPUTAÇÃO EM NUVEM

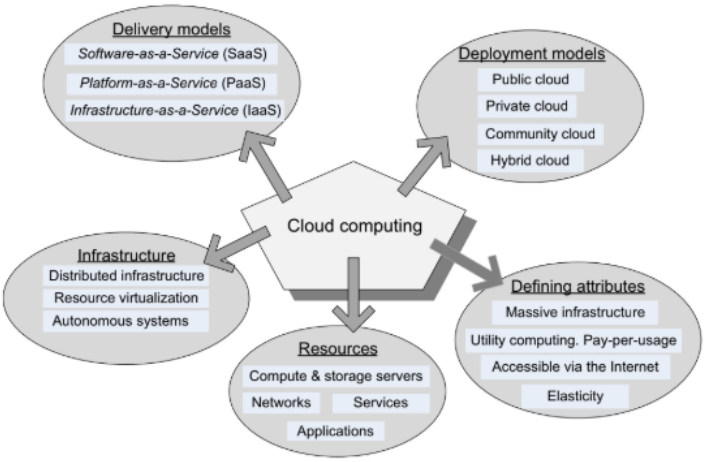
O conceito de computação em nuvem vem sendo aprimorado ao decorrer do tempo, mas a ideia inicialmente abordada foi o armazenamento e processamento de dados fora de ambientes corporativos, isso passou a ser feito em componente central conhecido como *datacenter*. Segundo Veras (2012) o *datacenter* é o componente central de qualquer infraestrutura de computação em nuvem, no entanto, gera demandas de redundância energética, sistema de climatização dedicado e um boa conexão com a internet.

A computação em nuvem é a entrega de serviços de computação sob demanda - de aplicativos a armazenamento e poder de processamento - normalmente pela Internet e em base de pagamento conforme o uso. Pode se dizer que é um tipo de terceirização de software, armazenamento de dados e processamento

A computação em nuvem ganhou enorme popularidade ao fornecer alta disponibilidade e escalabilidade bem como serviços sob demanda. Segundo Buyya, Vecchiola e Selvi (2013), este é um grande avanço tecnológico concentrado na forma como projetamos sistemas de computação, desenvolvemos aplicativos e alavancamos serviços existentes para a criação de softwares. Pode se dizer que é a entrega da computação como um produto e não como um serviço.

Deste modo para Buyya, Vecchiola e Selvi (2013) computação em nuvem não é aplicada apenas aos serviços, mas também à capacidade de computação, armazenamento, rede e infraestrutura de tecnologia da informação (TI) em geral. Esta tecnologia também é frequentemente associada a infraestrutura virtualizada e hardware sobre demanda. A Figura 4 descreve os modelos de distribuição de computação em nuvem, modelos de implantação, atributos de definição, recursos e organização da infraestrutura.

Figura 4: Computação de Nuvem.



Fonte: Extraída de Marinescu (2013)

A computação em nuvem é um modelo que permite acesso de qualquer lugar desde que o usuário possua conexão com a internet, também oferece um conjunto compartilhado de recursos de computação configuráveis e sob demanda por exemplo: redes, servidores, armazenamento, aplicativos e serviços. Estes podem ser rapidamente provisionados e liberados com praticidade no gerenciamento e interação com o provedor de serviços.

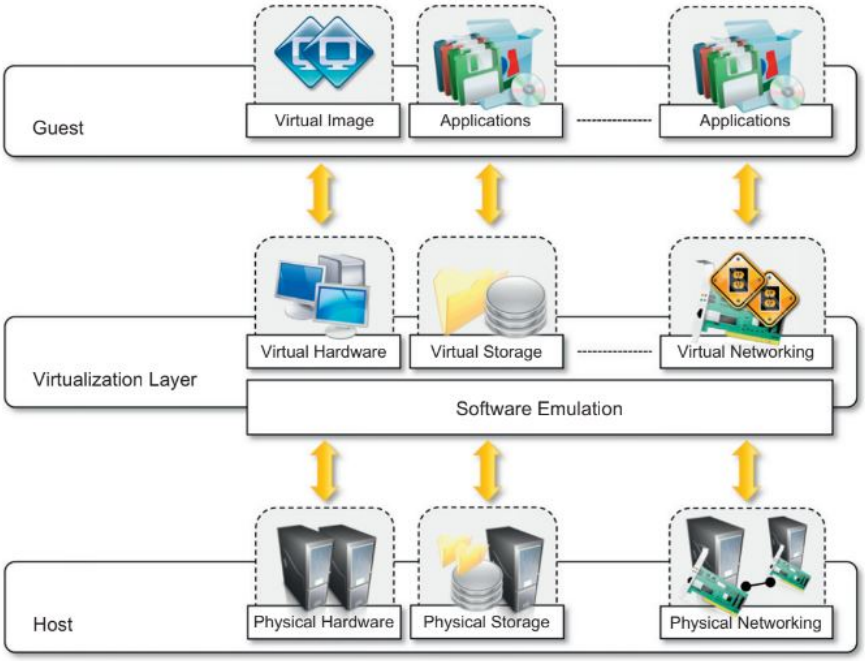
2.2.1 Virtualização

Segundo Buyya, Vecchiola e Selvi (2013) a virtualização pode ser vista como uma grande variedade de tecnologias e conceitos destinados a fornecer um ambiente intangível, seja hardware ou sistema operacional virtual para executar aplicações. Este recurso é mais utilizado na virtualização de elementos de hardware que desempenham um papel fundamental no fornecimento eficiente de soluções de infraestrutura como serviço (IaaS) para computação em nuvem.

A virtualização é um conceito amplo que se refere à criação de uma versão virtual de algo, seja hardware, software, armazenamento, ou rede. Segundo Buyya, Vecchiola e Selvi (2013) Em um ambiente virtualizado há três componentes principais: *guest*, *host*, e camada de virtualização. O *Guest* representa o componente do sistema que interage com a camada de virtualização e não com o *host* como normalmente aconteceria. O *host* representa o ambiente original em que o

guest deve ser gerenciado. A camada de virtualização é responsável por recriar o ambiente diferente em que o *guest* irá operar. Esse esquema pode ser virtualizado na Figura 5.

Figura 5: Virtualização.



Fonte: Extraída de Buyya, Vecchiola e Selvi (2013)

2.2.2 Modelos de Implantação

Nesta seção são descritos os modelos de implantação de computação em nuvem. São eles nuvens públicas, nuvens privadas, nuvens híbridas e nuvens comunitárias.

2.2.2.1 Nuvens públicas

De acordo com Taurion (2009) um modelo de nuvem pública não é necessariamente gratuito mas sim uma nuvem que pode ser acessada pela internet, o custo deste modelo vai depender do provedor do serviço. As nuvens públicas tem mais acessibilidade e um menor custo para utilização, porém ainda existem preocupações com confiabilidade e portabilidade.

As nuvens públicas podem oferecer e disponibilizar serviços para qualquer

usuário contanto que ele possua conexão com a internet, ou seja, qualquer cliente pode inserir suas credencias e detalhes de faturamento e utilizar os serviços. Segundo Buyya, Vecchiola e Selvi (2013) a principal característica deste modelo é a muti-locação. Estas nuvens são projetadas para atender uma grande quantidade de usuários embora normalmente em ambientes separados e isolados para fornecer um monitoramento eficaz das atividades. Deste modo uma parte significativa da infraestrutura é dedicada a monitorar os recursos da nuvem.

Segundo Buyya, Vecchiola e Selvi (2013) a infraestrutura de uma nuvem publica é normalmente composta por um ou mais *datacenters* que podem ser geograficamente dispersos, com objetivo de prover um serviço de melhor qualidade dependo da localização dos usuários.

2.2.2.2 Nuvens Privadas

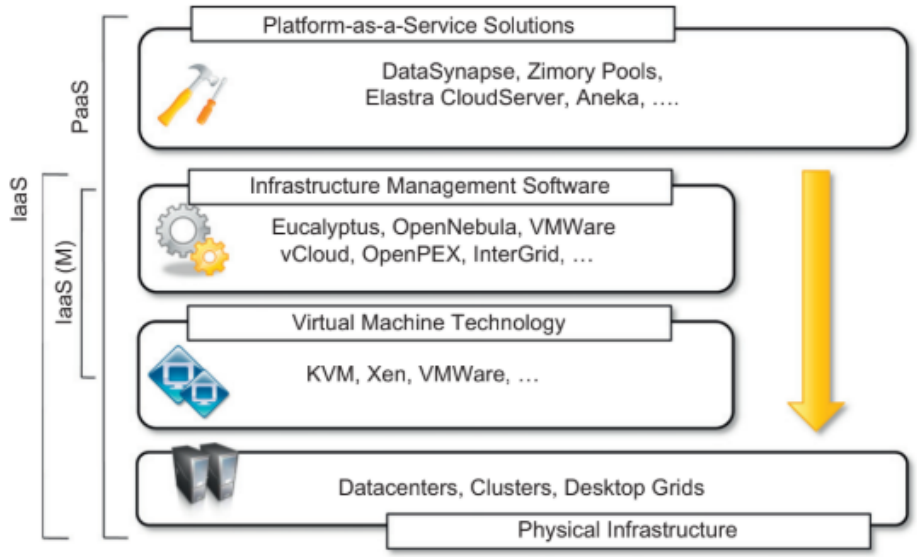
Segundo Taurion (2009) o modelo de nuvem privada é quando a nuvem é propriedade de um única empresa, e esta controla quais aplicações são executadas e onde. Este modelo implementa mecanismos de confiabilidade e segurança mais severos além de normalmente estarem protegidas por um *firewall*. Deste modo as preocupações de segurança são menos críticas neste cenário.

O modelo de nuvem privada é a solução perfeita quando é necessário manter o processamento de informações dentro das instalações da empresa, ou quando é necessário trabalhar com a infraestrutura de hardware e software existente.

De acordo com Buyya, Vecchiola e Selvi (2013), nuvens privadas são sistemas distribuídos virtuais executados em uma infraestrutura restrita e fornecem aos usuários internos um provisionamento dinâmico de recursos de computação. Este modelo tem como principal vantagem manter internamente as principais operações de negócios. A Figura 6 fornece uma visão abrangente das soluções juntamente com uma referência a um dos softwares mais populares usado para implantar nuvens privadas, na camada inferior da pilha de software são descritas as tecnologias de máquina virtual, como Xen , KVM e VMware, servem como fundamentos da nuvem.

Nuvem privada refere-se a um modelo de computação em nuvem no qual os serviços de TI são provisionados em uma infraestrutura de TI privada para o uso dedicado de uma única organização. Uma nuvem privada geralmente é gerenciada por meio de recursos internos.

Figura 6: Nuvem Privada.



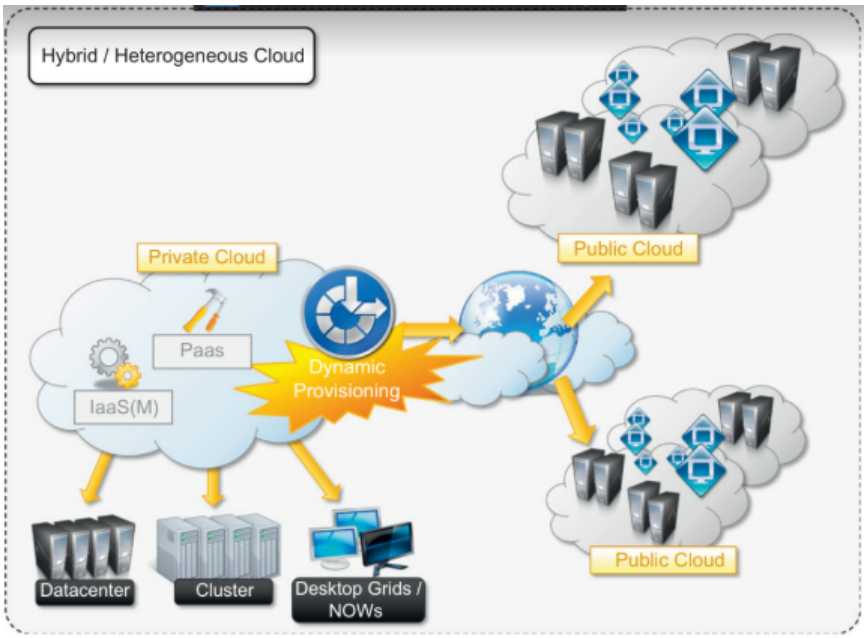
Fonte: Extraída de Buyya, Vecchiola e Selvi (2013)

2.2.2.3 Nuvens Híbridas

Segundo Buyya, Vecchiola e Selvi (2013) as nuvens híbridas permitem que as empresas explorem as infraestruturas de TI existentes mantenham informações confidenciais nas instalações, aumentem e diminuam o provisionando de recursos externos liberando-os conforme a necessidade. As preocupações de segurança então limitadas apenas à parte pública da nuvem que pode ser usada para executar operações com restrições menos rigorosas, mas que ainda fazem parte da carga de trabalho do sistema.

A figura 7 fornece uma visão geral de uma nuvem híbrida que segundo Buyya, Vecchiola e Selvi (2013) pode ser definida como um sistema distribuído heterogêneo resultante de uma nuvem privada que integra serviços ou recursos adicionais de uma ou mais nuvens públicas.

Figura 7: Nuvem Hibrida.



Fonte: Extraída de Buyya, Vecchiola e Selvi (2013)

2.2.2.4 Nuvens comunitárias

As nuvens comunitárias são sistemas distribuídos criados pela integração dos serviços de diferentes nuvens para atender às necessidades específicas de uma indústria, uma comunidade ou um setor empresarial. Os usuários de uma nuvem comunitária compartilham os mesmos objetivos e necessidades.

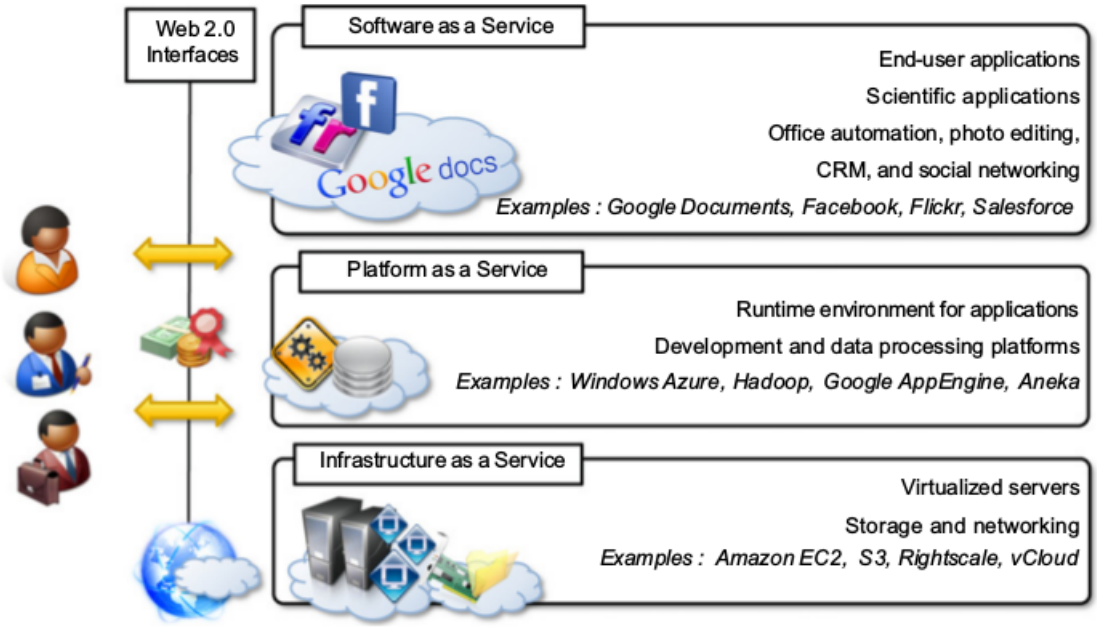
Segundo Buyya, Vecchiola e Selvi (2013) as nuvens comunitárias são caracterizadas por um domínio multi-administrativo, envolvendo diferentes modelos de implantação (público, privado e híbrido), e é especificamente projetado para atender às necessidades de um setor específico.

2.2.3 Modelo de serviço

Segundo Buyya, Vecchiola e Selvi (2013) atualmente é possível classificar os modelos de serviços de computação em nuvem em três categorias principais, que são: Infraestrutura como serviço (SaaS) que é aplicado no Google Docs e Facebook, por exemplo, Plataforma como serviço (PaaS) e Software como serviço aplicado em ferramntas como Microsoft Azure e a Handoop, por exemplo, e (IaaS) que pode ser visto. Estas categorias estão relacionadas conforme visto na Figura

8.

Figura 8: Serviços de Nuvem.



Fonte: Extraída de Buyya, Vecchiola e Selvi (2013)

2.2.3.1 Modelo SaaS

O modelo software como serviço (SaaS) oferece a entrega de softwares que fornecem acessos a aplicativos pela Internet como um serviço baseado na Web. Segundo Buyya, Vecchiola e Selvi (2013) neste modelo os usuários não precisam realizar instalações, nem pagar custos iniciais consideráveis para comprar o software e as licenças necessárias para utilizar o serviço. Para a utilização desse sistema basta acessar o site do aplicativo, inserir as credenciais de acesso e os detalhes de faturamento para usar o aplicativo instantaneamente. Já para o fornecedor os detalhes e recursos específicos do aplicativo de cada cliente são mantidos na infraestrutura e disponibilizados sob demanda.

2.2.3.2 Modelo PaaS

Segundo Buyya, Vecchiola e Selvi (2013) o modelo PaaS fornece uma plataforma de desenvolvimento e implementação para executar aplicativos em nuvem. As soluções de PaaS podem oferecer um *middleware* para o desenvolvimento de

aplicativos junto com a infraestrutura ou simplesmente fornecer aos usuários um software já instalado. As soluções de PaaS apresentam como principal vantagem a redução do custo de desenvolvimento, implantação e gerenciamento de aplicativos além da capacidade de integrar serviços em nuvem de terceiros oferecidos por outros fornecedores aproveitando melhor a arquitetura.

De acordo com Veras (2012) o conceito de PaaS está relacionado a utilização de ferramentas para desenvolvimento de *software* oferecidas por provedores ondes podem ser desenvolvidas aplicações utilizando a internet como meio de acesso. Pode-se dizer que este modelo é baseado na utilização de um plataforma de desenvolvimento terceirizada.

2.2.3.3 Modelo IaaS

Segundo Buyya, Vecchiola e Selvi (2013) o modelo IaaS é o segmento mais utilizado para computação em nuvem, pois pode oferecer infraestrutura sob demanda. Este modelo oferece desde um único servidor até infraestruturas inteiras incluindo dispositivos de rede, balanceadores de carga e bancos de dados.

Deste modo a principal tecnologia utilizada neste modelo é a virtualização de *hardware* responsável por fornecer uma ou mais VMs configuradas e interconectadas. As máquinas virtuais também constituem os componentes que são implantados e precificados de acordo com os recursos específicos do hardware virtual: memória, número de processadores e armazenamento em disco.

As soluções IaaS trazem todos os benefícios da virtualização de hardware: particionamento de carga de trabalho, isolamento de aplicativos, *sandboxing* e ajuste de hardware. Do ponto de vista do provedor de serviços, o IaaS permite explorar melhor a infraestrutura de TI e fornece um ambiente mais seguro para executar aplicativos de terceiros.

2.2.4 Ferramenta de Gerenciamento de Nuvem

Ferramentas de gerenciamento de nuvem são *softwares* e tecnologias usadas para monitorar e operar serviços, aplicativos e dados que residem na nuvem. Atualmente existe uma grande variedade de soluções para controlar uma infraes-

trutura de nuvem, tanto para nuvens privada quanto para nuvens públicas.

As ferramentas de gerenciamento de nuvem abordam o desafio de simplificar e otimizar as tarefas complexas envolvidas no gerenciamento de sistemas e infraestrutura baseados em nuvem híbrida, privada e pública.

Segundo Vogel e Griebler et al. (2016) escolher apropriadamente uma ferramenta de nuvem é importante para obter os melhores resultados, e esta decisão deve ser feita de acordo com os recursos da ferramenta e suas restrições, além de visar os pontos-chave que são suporte para flexibilidade e resiliência, já que permitem estimar o nível de robustez da ferramenta.

De acordo com Vogel e Griebler et al. (2016) quase todas as ferramentas de gerenciamento de nuvem suportam a realização de tarefas administrativas através de interface de usuário UI(*User Interface*), esta interface está acessível através de um navegador web. Ha também uma interface de linha de comando mais utilizada pelos administradores da nuvem, para um controle de terminal mais rápido e fácil. Tendo em vista que o cenário onde o modelo proposto por este trabalho será testado, utiliza o modelo IaaS, portanto serão descritas algumas das principais ferramentas voltadas para o mesmo.

O OpenNebula é uma plataforma de gerenciamento *open source* para gerenciar nuvens privadas, públicas e híbridas em um modelo IaaS. Os principais usos desta plataforma são soluções de virtualização de *datacenters* e gerenciamento de nuvens. Esta ferramenta também oferece uma grande variedade de recursos, como por exemplo, arquitetura modular e extensível, *Drivers* personalizáveis para os principais subsistemas e API para integração com outras ferramentas.

O CloudStack é uma plataforma IaaS para gerenciar recursos de uma infraestrutura de computação em nuvem. Esta ferramenta funciona com uma variedade de *hipervisores* e tecnologias semelhantes possibilitando que uma única nuvem possua vários virtualizadores. Também possuí alto escalonamento podendo gerenciar um grande numero de servidores mesmo geograficamente dispersos além do servidor de gerenciamento ser dimensionado de forma quase linear, eliminando a necessidade de servidores de gerenciamento no nível do *cluster*.

O OpenStack é uma plataforma de código aberto para gerenciamento de de nuvens públicas e privadas, capaz de gerenciar múltiplas infraestruturas virtualizadas. Esta ferramenta é composta por uma série de componentes móveis diferentes, e suporta a adição e outros, para melhor atender as necessidades dos usuários. O armazenamento pode ser tanto local como distribuído. O OpenStack é considerado uma solução modular e granular porque permite implementar individualmente todos os serviços de infraestrutura.

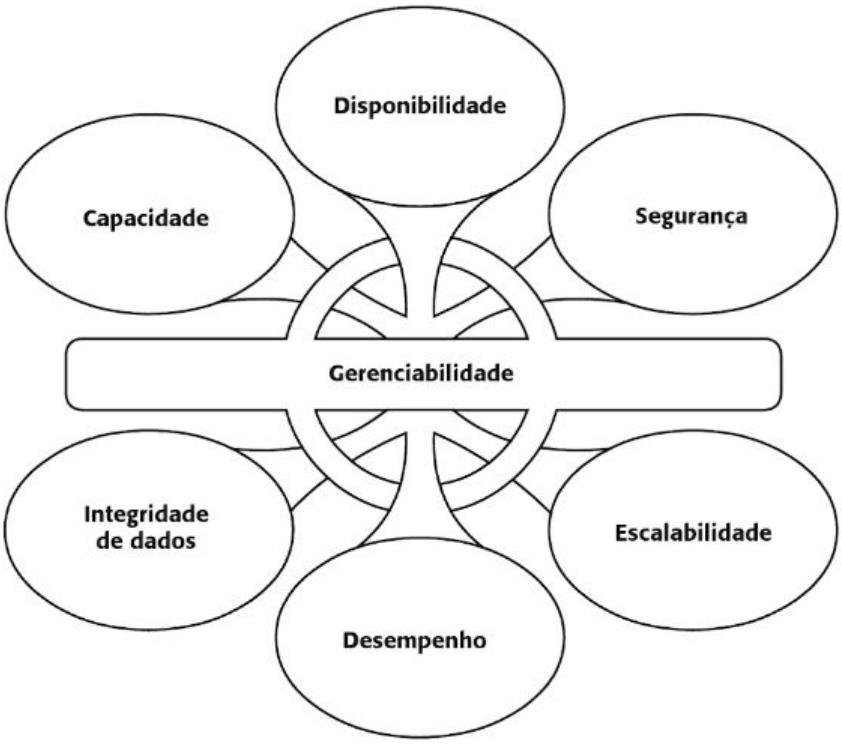
2.3 MONITORAMENTO DE AMBIENTES COMPUTACIONAIS

Embora os serviços de TI sejam o principal motivo para existência dos *datacenters*, os ativos e operações não relacionados à TI abrangem uma grande parte das operações de sua infraestrutura. As operações dos *datacenters* modernos dependem cada vez mais do monitoramento e análise de dados referentes aos aspectos de seu ambiente para garantir a integridade e a confiabilidade dos equipamentos de TI.

2.3.1 Requisitos chave para monitoramento de *datacenters*

O funcionamento ininterrupto de um *datacenter* é fundamental para a eficiência e entrega dos serviços. Segundo Somasundaram e Shrivastava (2009), é necessária uma infraestrutura eficiente para garantir a disponibilidade das informações e serviços. A Figura 9 ilustra as características chaves dos elementos que devem ser monitorados em um *datacenter*.

Figura 9: Características-chaves dos elementos de um *datacenter*



Fonte: Extraída de Somasundaram e Shrivastava (2009)

Abaixo serão descritos os elementos da Figura 9 de acordo com Somasundaram e Shrivastava (2009).

- Disponibilidade: todos os elementos da infraestrutura de um *datacenter* devem ser projetados para garantir alta disponibilidade, uma vez que a interrupção de um desses serviços normalmente resulta em prejuízo para a organização.
- Segurança: devem ser estabelecidos políticas e procedimentos e um gerenciamento eficiente de acessos, para garantir a integridade do *datacenter*.
- Escalabilidade: O *datacenter* deve permitir a alocação de recursos computacionais sob demanda sem interromper a operação da infraestrutura. Além de um planejamento para futuras expansões.
- Desempenho: Todos os elementos do *datacenter* devem operar com desempenho otimizado, atendendo as requisições o mais rápido possível.

- Integridade: diz respeito a implementação de mecanismos e códigos para correção de erros, para evitar que os dados sejam corrompidos.
- Capacidade: um *datacenter* requer uma controle preciso da quantidade de recursos que possui. Desta forma quando a quantidade de requisições de serviço aumentarem ele deve ser capaz de operar sem interrupções ou perda de eficiência.
- Gerenciabilidade: um *datacenter* busca constantemente amentar sua eficiência, através de uma melhor gerenciabilidade, que por sua vez pode gerar automação de recursos e diminuição da necessidade de intervenções humanas em sua infraestrutura.

Segundo Joia (2015) a infraestrutura de um *datacenter* necessita de contatante monitoramento, e atualizações. Além de a necessitar de manutenção periódica devido a fatores como:

- Aumento do número de usuários.
- Escalabilidade dos sistemas.
- Existência de sites dispersos geograficamente.
- Acesso remoto ao programa e aos sistemas.
- O aumento dos níveis de segurança.
- Conflitos de padrões entre diferentes sistemas.

2.3.2 Sistema de Refrigeração de *Datacenter*

Atualmente os sistemas de climatização para *datacenters* requerem uma solução de monitoramento cada vez mais eficiente para para garantir a otimização da energia bem como desempenho, confiabilidade e segurança. Segundo Yogendra e Pramod (2012) e necessária uma combinação de medições de temperatura em tempo real juntamente com o tratamento de *logs* desse sistema para se ter uma otimização do resfriamento do data center.

De acordo com Yogendra e Pramod (2012), um histórico de *logs* de monitoramento do sistema de refrigeração de um *datacenter* é importante para permitir um análise dos seguintes itens: carga, variações de temperatura e consumo de energia do sistema. Desse modo, através dos dados resultantes do monitoramento é possível realizar comparações com base em análises estatísticas para determinar tendências e fornecer alertas antecipados sempre que algum item apresentar alguma anormalidade.

De acordo com Yogendra e Pramod (2012) o gerenciamento ineficiente de *datacenters* pode resultar em várias implicações negativas devido a um baixo fluxo de ar no ambiente ou desligamento inesperado do sistema de climatização. O gerenciamento térmico tem uma importância critica para ambientes com servidores. Por outro lado quando bem executado pode reduzir custo operacional da infraestrutura.

2.3.3 Monitoramento de Servidores

Servidores são computadores robustos utilizados para prover serviços necessários para o funcionamento de um rede ou organização. Devido a sua grande importância em uma rede, essas máquinas são concentradas em estruturas projetadas para garantir seu funcionamento constante. O monitoramento de servidores é o processo de revisar e analisar um servidor para disponibilidade, operações, desempenho, segurança e outros processos relacionados a operações.

Quando o monitoramento de um servidor não é feito de maneira adequada, o hardware fica vulnerável a uma série de eventos que podem prejudicar a disponibilidade e a integridade da infraestrutura, um exemplo disto é o superaquecimento de componentes.

2.3.4 Gerenciamento de Capacidade

Para Lima (2014) é importante monitorar a capacidade computacional da infraestrutura de um *datacenter*, visando as possíveis atualizações de hardware e software. Este gerenciamento pode ser feito através da analise de gráficos e relatórios do sistema, que se faz necessário obter o balanceamento da carga de

trabalho dos servidores.

Segundo Somasundaram e Shrivastava (2009) as operações de *datacenter* requerem recursos adequados de armazenamento e processamento de uma grande quantidade de dados. Quando os requisitos aumentam o gerenciamento deve ser capaz de fornecer capacidade extra, sem interromper a disponibilidade.

2.3.5 Monitoramento Energético

Atualmente os *datacenters* requerem uma grande quantidade de recursos computacionais para atenderem as atuais demandas por recursos computacionais. Segundo Koomey (2011), hoje os data centers modernos consomem cerca de 1,3% da oferta mundial de eletricidade, e este nível deverá aumentar para 8% até 2020. De acordo com Google green, 2014, o Google sozinho consumiu 2,26 milhões de MWh em 2010.

De acordo com Fit (2014) o monitoramento energético tem como principal função detectar os maiores consumidores de energia em um ambiente *datacenter*. Desta forma é possível realizar uma análise cautelosa, com base nos dados obtidos através do monitoramento, e determinar as medidas para redução do consumo e custo operacional da infra-estrutura.

Segundo Veras (2012) para dimensionar o consumo energético de um *datacenter* é necessário poder mensurar a quantidade de energia para alimentar sistema de refrigeração, *no-breaks* e a carga de TI. Desta forma é possível obter precisão para planejar a redundância energética e o consumo total da infraestrutura.

O *Green Grid* é um consórcio global formado por diversas companhias de TI (incluindo Intel, Dell, VMware, AMD) com o objetivo de definir e propagar melhores práticas relacionadas à eficiência no consumo de energia em *datacenters*. Este órgão desenvolveu duas métricas para medir a eficiência energética dos datacenters são elas, PUE (*Power Usage Effectiveness*) e o DCiE (*DATACENTER Efficiency*). Sendo a primeira a mais utilizada.

A PUE é uma das principais métricas utilizadas para entender como está funcionando o fornecimento de energia nos equipamentos de TI em um *datacen-*

ter. A métrica é melhor aplicada para analisar as tendências em uma instalação individual ao longo do tempo e medir os efeitos de diferentes decisões de projeto e operacionais dentro de uma instalação específica. A equação usada na métrica PUE esta ilustrada na Figura 10.

Figura 10: Equação PUE.

$$PUE = \frac{Total\ Facility\ Energy}{IT\ Equipment\ Energy}$$

Fonte: Extraída de Avelar e Azevedo et al. (2012)

Total facility energy é definida como a energia dedicada exclusivamente ao data center (por exemplo, a energia medida no medidor da concessionária de um centro de dados dedicado ou no medidor para um data center ou sala de dados em uma instalação de uso misto), enquanto a *IT equipment energy é definida como a energia consumida pelo equipamento que é usado para gerenciar, processar, armazenar ou rotear dados dentro do espaço de computação.*

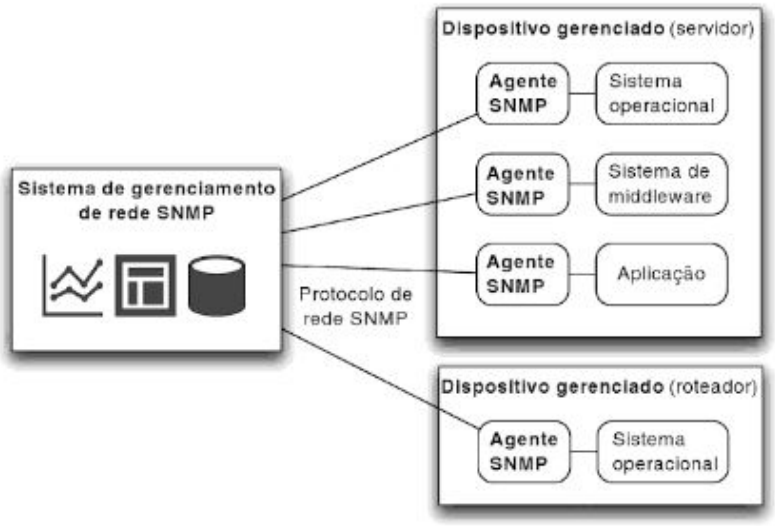
2.3.6 SNMP

O SNMP (*Simple Network Management Protocol*) é um protocolo amplamente utilizado para monitoramento e gerenciamento de redes de computadores, além atualmente ser suportado por diversos dispositivos, como impressoras e microcontroladores etc. Segundo GURGEL e BRANCO et al. (2014) é um protocolo assíncrono de requisição e resposta é uma das formas mais eficientes para gerenciar o estado da infraestrutura de um *datacenter* devido a sua simplicidade. Ele permite que algumas máquinas sejam definidas com gerentes, que vão receber informações dos demais ativos da rede, os agentes.

Segundo Kurose, Ross e Zucchi (2013) o SNMP é utilizado para transmissão de informações e comandos entre um servidor que serve como unidade gerenciadora, e um agente instalado nos dispositivos da rede. Deste modo qualquer ativo da rede pode se comunicar através do SNMP, já que ele é um protocolo padrão do mercado. Sendo assim é possível administrar sistemas heterogêneos através das informações coletadas, além de analisar estatisticamente o desempe-

nho da infraestrutura. A Figura 11 ilustra a arquitetura do protocolo, onde o sistema de gerenciamento de rede se comunica com o agente que por sua vez se comunica com o sistema operacional ou dispositivo que será monitorado através do protocolo TCP/IP.

Figura 11: Arquitetura SNMP.



Fonte: Extraída de Humble e Farley (2014)

Segundo Humble e Farley (2014) o SNMP é composto pelos seguintes componentes: sistema físico, agentes e sistema de gerenciamento de redes. O protocolo serve conexão entre os dois últimos, como mostrado na figura 11.

2.3.7 Monitoramento de Segurança

Atualmente a Infraestrutura de um *datacenter*, bem como os dados e informações trafegados em suas instalações são de importância crítica, ou seja, sendo a preservação da integridade, o que torna a segurança fundamental. Segundo Lima (2014),para dispor de um ambiente com segurança e estabilidade, se fazem necessárias alguma providências, uma delas é monitorar o ambiente como um todo, pois através da analise de *logs* e monitoramento de ativos, podem-se tomar as melhores providencias para executar ações corretivas.

De acordo com a norma de segurança ISO (2013) O monitoramento de segurança em ambientes computacionais tem como objetivo, detectar atividades não autorizadas no que diz respeito a processamento de informação. A normativa tam-

bém orienta que sejam monitorados e documentados todos os eventos referentes a segurança da informação, através da geração e documentação de *logs*.

Segundo Kurose, Ross e Zucchi (2013) a meta do gerenciamento de segurança é definir um controle de acesso aos recursos do TI. Além de sugerir o uso de *firewalls*, para auxiliar no monitoramento e controlar pontos de acesso a rede.

De acordo com ISO (2013) o monitoramento e gerenciamento de acessos se faz necessário para gerenciar e prevenir que indivíduos não autorizados possam obter ou comprometer o grande volume de informações trafegadas e armazenadas em *datacenters*. Esta norma orienta que todos os recursos de processamento de informações sejam gerenciados com base nos requisitos de negócios e segurança da informação.

A ISO (2013) orienta que dentro das organizações, seja redigida a documentação de uma política de acesso a informação, com o objetivo de restringir as funções do sistema e o acesso as informações. A norma também convém que sejam restringidos horários de acesso aplicações de importância critica com objetivo de fornecer segurança adicional, deixando a operação inacessível quando possível.

Tendo em vista as orientações anteriores, pode-se concluir que uma infraestrutura adequada a ISO (2013), seja restrito apenas a acessos autorizados, e que sistemas e aplicações gerenciadas sejam submetidos aos seguintes cuidados:

- Gerenciamento de acesso dos usuários.
- Proteção contra acesso não autorizado para qualquer sistema ou aplicação rodando na infraestrutura.
- Não comprometer os sistemas cujo os recursos de informações são compartilhados.

2.4 SMART DATACENTERS

Os *Smart Datacenters* oferecem um controle automatizado e dinâmico de infraestruturas computacionais, e tem como principal objetivo diminuir a crescente

complexidade de gerenciamento das mesmas, através de abordagens autonômicas, monitoramento proativo e reativo. Deste forma é possível diminuir a necessidade de intervenção humana e otimizar os recursos computacionais o melhor possível.

Segundo Ebbers e Archibald et al. (2011) os principais motivos para almejar um *smart datacenter* são reduções de custo operacional e sustentabilidade. Além disso o aumento do consumo energético e questões ambientais podem vir a reduzir o crescimento das infraestruturas de *datacenter* tornando o estudo de abordagens de gerenciamento inteligente essenciais.

De acordo com Ebbers e Archibald et al. (2011) o custo do KWh aumentou ligeiramente, enquanto o consumo energético dos *datacenters* vem aumentado significativamente. Deste modo pode-se concluir que o custo operacional referente a energia elétrica dos servidores é maior que o aumento no preço da energia elétrica. Tendo isso em vista as organizações estão investindo em virtualização e automação.

2.4.1 Computação Autônoma

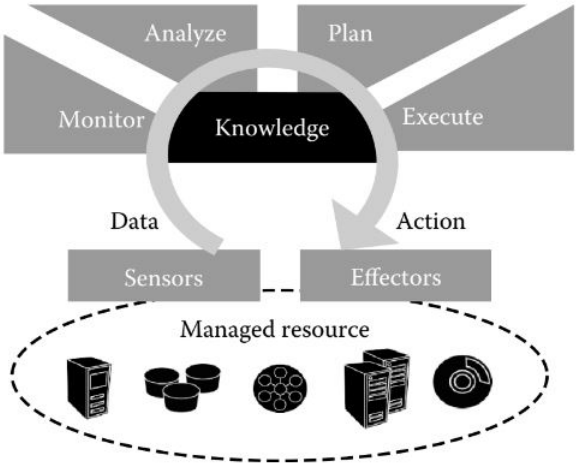
Segundo Parashar e Hariri (2006) a computação autonômica propõe o uso de sistemas inteligentes que oferecem auto-gerenciamento, ou seja, podem agir reativamente, analisar e perceber mudanças e executar ações. Esta abordagem visa controlar dinamicamente funções de uma rede ou sistema, sem intervenções humanas.

Segundo Norouzi e Bauer (2015) *Autonomic Computing* (AC) visa abranger, a noção de autogestão em sistemas distribuídos e complexos, onde a intervenção do administrador no gerenciamento do sistema é reduzida ou minimizada. A Figura 12 ilustra um exemplo de um sistema de controle, onde gerenciadores autônomos monitoram detalhadamente os recursos, realizam uma análise, planejam ajustes e os executam, utilizando tanto informações de administradores, quanto regras e políticas definidas por eles e aprendidas pelo sistema.

A computação autonômica é a capacidade de um computador de gerenciar a si mesmo automaticamente por meio de tecnologias adaptáveis que aprimo-

ram os recursos de computação e reduzem o tempo exigido pelos profissionais de computação para resolver as dificuldades do sistema e outras manutenções, como atualizações de software.

Figura 12: Computação Autonômica



Fonte: Extraída de Parashar e Hariri (2006)

2.4.2 Monitoramento Pró Ativo

O monitoramento proativo é uma parte fundamental em um *datacenter* inteligente. Segundo Schulz (2016) pode ser utilizado para monitorar e gerenciar servidores, armazenamento e dispositivos de rede através de ações proativas em vários eventos como desligamento de recursos de energia ou de equipamentos que estiverem em risco, além de gerenciamento de dados incluindo backup, *snapshots*, replicação e movimentação de dados para operações de rotina, o que contribui para fornecer alta disponibilidade.

2.4.3 Dispositivos Para monitoramento inteligente

Para aumentar a capacidade de monitoramento e coleta de dados referente aos diversos elementos que compõe um *datacenter* são utilizados dispositivos baseados em computação embarcada, por exemplo: microcontroladores, sensores e câmeras de segurança. Nesta seção são apresentados dispositivos e componentes para auxiliar no monitoramento e gerenciamento de segurança, energia e temperatura ambiente de um *datacenter*.

2.4.3.1 Sistemas embarcados

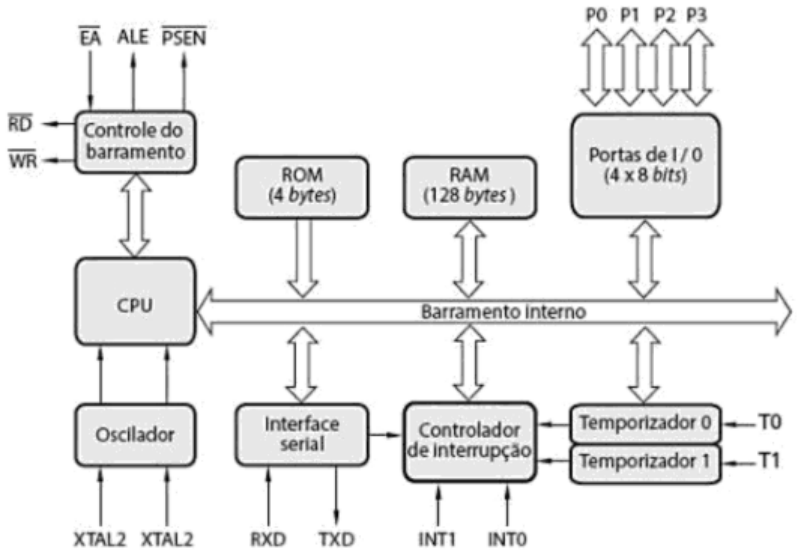
Segundo Lamb (2015) computação embarcada trata-se de sistemas ou dispositivos com um propósito especifico, ou seja, são desenvolvidos para executar uma ou algumas funções dedicadas. Em razão disto possuem componentes mais simplificados o que torna seu preço bastante acessível, deste modo se encontram presentes em diversos dispositivos as nossa volta.

Segundo Almeida, Moraes e Seraphim (2017) sistemas embarcados são conjuntos eletrônicos microprocessados, que uma vez programados possuem uma função especifica, mas normalmente esta pode ser alterada. Um exemplo disso é a impressora que mesmo possuindo um processador que poderia ser utilizado para outra função possui uma tarefa especifica.

2.4.3.2 Microcontroladores

Atualmente os microcontroladores vem sendo muito utilizados em sistemas embarcados e aplicações de automação. A diminuição do tamanho e do custo destes dispositivos os torna uma opção mais econômica, para monitoramento e controle de sistemas. De acordo com SENAI (2014), microcontroladores são dispositivos com circuitos compostos por microprocessador, memórias ROM e RAM e conversor digital/analógico.

Figura 13: Estrutura de um microcontrolador



Fonte: Extraída de SENAI (2014)

A Figura 13 ilustra a estrutura interna de um microcontrolador, composta por CPU que é usada para executar as operações programadas, uma memória RAM volátil utilizada para armazenar temporariamente variáveis, memória ROM não volátil, além entradas e saídas.

No âmbito de *Smart Datacenters*, os microcontroladores entram no contexto da automação do monitoramento e gerenciamento dos elementos que compõe sua infraestrutura, através do uso da computação embarcada. Uma vez que uma das opções mais eficientes para se obter um monitoramento preciso do ambiente é utilizar uma rede de sensores, para coletar dados referentes a corrente elétrica e temperatura. O microcontrolador é muito utilizado para fazer a comunicação com um sistema distribuído tratando e enviando os dados coletados.

2.4.3.3 Monitoramento com Sensores

Para contribuir com o monitoramento e gerenciamento inteligente de um *datacenter*, um método eficiente segundo Portocarrero e Delicato et al. (2017) é a utilização, das redes de sensores sem Fio (*Wireless Sensor Networks - WSNs*) consistem em redes compostas de diversos pequenos sensores equipados com recursos de detecção, processamento, armazenamento e comunicação sem fio. No entanto as WSNs possuem recursos de computação limitados, e normalmente são alimentados por baterias, o que pode acabar se tornando um obstaculo no auto-gerenciamento de um estrutura.

Segundo Geng (2014) sensores de temperatura são fundamentais em ambientes *datacenter*, uma vez que servidores geram um quantidade considerável de calor e seus componentes são vulneráveis a superaquecimento. A sua principal função é fornecer aviso antecipado sobre temperaturas extremas, pontos quentes ou pontos frios e podem ajudar a identificar um desiquilíbrio na temperatura ambiente.

Os sensores de fumaça também se tornaram muito importantes nas *datacenters* atuais para preservar a integridade dos equipamentos de TI, que normalmente possuem um custo elevado. Segundo Geng (2014) os sensores de temperatura mais utilizados nas infraestruturas atuais são aqueles baseados em

amostragem de ar pois possuem uma maior sensibilidade.

2.4.4 Internet das Coisas

Segundo Lee e Lee (2015) a Internet das Coisas (IoT), também chamada de Internet de Tudo ou da Internet Industrial, é um novo paradigma tecnológico concebido como uma rede global de máquinas e dispositivos capazes de interagir entre si.

Devido ao aumento do uso de dados e necessidades de técnicas de gerenciamento mais eficientes, os *datacenters* precisam prepara suas infraestruturas para o uso de IoT. Segundo Bouhaï e Saleh (2017) o termo internet das coisas se refere a uma rede cada vez mais disseminada uma vez que diversos materiais podem ser conectados e controlados através da mesma.

Para Bouhaï e Saleh (2017) um dos maiores obstáculos para o crescimento de internet das coisas é a segurança dos dados, ou seja, a proteção dos dados enviado/recebidos por um objeto conectado. Assim como um computador, qualquer objeto conectado pode estar sujeito a *hacking*, aquisição, instalação de *spyware*, etc. Com a impossibilidade de controlar e limitar o desenvolvimento desse ecossistema, é necessário procurar e sugerir estratégias de segurança para proteger a redes e os objetos conectados e preencher as lacunas de segurança detectadas.

2.5 MODELO CONCEITUAL

De acordo com Turban e Sharda et al. (2009) modelo conceitual em TI tem como objetivo apresentar uma imagem clara referente a uma infraestrutura ou sistema de computação, demonstrando os principais conceitos e suas associações, além de esclarecer o vocabulário e os termos de domínio. O principal objetivo do modelo conceitual é criar um sistema coerente de objetos propriedades e relações, e responder as seguintes perguntas referentes ao objeto de estudo; o que o sistema deve fazer? como ele deve se comportar? e como ele deve se parecer?

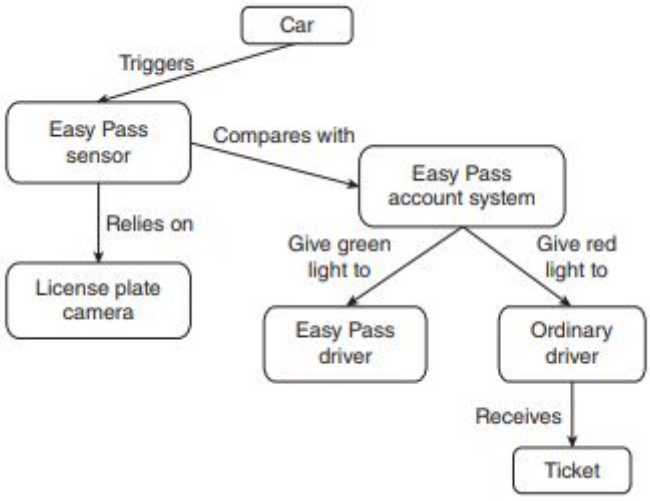
Para Brocke e Rosemann (2013) o modelo conceitual tem a função de passar uma imagem objetiva de uma organização ou sistema de TI, e tonar-se uma base para explicá-los. Além disso o modelo precisa atender a determinados crité-

rios para que possa servir como contribuição, são eles: capacidade de aprendizagem, funcionalidade e usabilidade. Para explicar estes modelos são utilizados os chamados mapas conceituais onde os nós dos gráficos capturam os conceitos ou elementos do sistema e os arcos direcionados (setas) implicam interações entre elementos conectados.

Segundo Sokolowski, Turnitsa e Diallo (2008) a modelagem conceitual também pode ser percebida como uma maneira de capturar os elementos de um sistema ou infraestrutura e a interação dos mesmos, de modo a oferecer um roteiro que contribua na visualização e entendimento do sistema. Quanto melhor o modelo conceitual se relacionar com os modelos mentais existentes dos usuários, mais fácil será utiliza-lo para explicar o que se pretende fazer com a aplicação.

De acordo com Sokolowski e Banks (2010) o principal foco do modelo conceitual está em informar as principais características e qualidades de um sistema específico. Deste modo um bom modelo deve explicar com alguns parágrafos ou imagens o que é o sistema e qual sua função conforme ilustrado na Figura 14 é apresentado um exemplo de mapa conceitual que é definido como um diagrama que ilustra as relações entre os conceitos.

Figura 14: Mapa Conceitual.



Fonte: Extraída de Sokolowski e Banks (2010)

O mapa visto na figura 14 apresenta a seguinte relação: (1) um carro aci-

ona o sensor *Easy Pass* que depende de uma câmera de matrícula, (2) o sensor Easy Pass compara algumas informações com o sistema de contas *Easy Pass*, (3) o *Easy* O sistema de contas de passe dá luz verde aos *drivers* do *Easy Pass* e um sinal vermelho aos *drivers* comuns, e (4) os motoristas comuns recebem um bilhete de tráfego para não pagar o pedágio.

2.6 TRABALHOS RELACIONADOS

Para obter referências de modelos e arquiteturas de monitoramento e gerenciamento para *smart datacenters* se fez necessária uma pesquisa por trabalhos relacionados, para observar detalhes que ainda não foram estudados e agregá-los como um diferencial no presente trabalho.

Portanto foi realizada uma pesquisa bibliográfica aprofundada por trabalhos relacionados a monitoramento e gerenciamento inteligente, ou que auxiliem na definição de *smart datacenter* ligando os termos através de um *string* de busca, a qual foi aplicada a duas bases de dados *Scopus* e *Science Direct*. Nelas foram adicionados os termos essenciais para o presente trabalho, bem como seus sinônimos.

O objetivo de utilizar uma *string* de busca para encontrar trabalhos relacionados, é encontrar o máximo de artigos que atendam aos seguintes requisitos de inclusão:

- Se o trabalho propõe, testa ou implementa uma arquitetura de monitoramento e gerenciamento inteligente para *datacenters*.
- Se monitora e gerencia autonomicamente os elementos essenciais para o funcionamento eficiente de um *datacenter* moderno.
- Se o trabalho diz respeito ao controle da infraestrutura de um *smart datacenter*.

No entanto a *String* de busca utilizada encontrou 377 trabalhos nas bases Scopus, e *Science Direct*, sendo que alguns deles possuem certa relação com o presente trabalho. Deste modo também forma elaborados e utilizados os seguintes requisitos de exclusão:

- Monitoramento estático, isso é o trabalho monitora a infraestrutura de um *datacenter*, porém sem o uso de abordagens inteligentes.

- Monitoramento a nível de aplicação, isso é quando o trabalho aborda monitoramento e gerenciamento com base em dados coletados a nível de aplicação.

- E quando o trabalho não diz respeito a monitoramento de infrestruturas de *datacenters*.

Nas seções abaixo serão apresentados alguns trabalhos relacionados encontrados na literatura.

2.6.1 *Autonomic Management for Energy Efficient Datacenters*

A pesquisa de Norouzi e Bauer (2015) tem como objetivo desenvolver uma gestão autonômica para ajudar a reduzir o consumo de energia de um *datacenter*, aderindo a acordos de nível de serviço (SLA) e expectativas de desempenho. O problema da pesquisa é definir quais as questões essenciais que precisam ser abordadas antes de implementar o sistema de gerenciamento de energia. Por exemplo: quais são objetos gerenciáveis no *datacenter*.

Os autores consideraram uma organização hierárquica de gerenciamento autonímico baseado na posição física dos elementos gerenciados. Também introduziram uma abordagem geral para um sistema de gerenciamento autônomo. Os princípios centrais que orientam o modelo de gerenciamento são: uma abordagem de transmissão de mensagens e gerentes autônomos que conduzem a política. A abordagem foi avaliada em um *datacenter* virtual usando um simulador, desta forma foram observados resultados em 5 cenários.

Cenário 1. Sem gerenciamento: O *datacenter* possui dois sistemas HPC (*High-performance computing*) em execução, um com 30 nós de computação e uma carga de trabalho de 730 *jobs* e outro com 20 nós de computação e uma carga de trabalho com 173 *jobs*.

Cenário 2. Existe um gerenciador no nível do sistema, que possui um perfil de política de SLA. Esse cenário é executado para o pequeno sistema HPC de 20

nós de computação. O objetivo é avaliar o impacto do perfil da política de SLA na potência e no desempenho.

Cenário 3. Exatamente como o cenário 2, exceto o perfil de política Verde para o nível de sistema AM.

Cenário 4. Possui um gerenciador autônomo no nível de sistema e outro nível do data center. O principal objetivo é considerar como o nível de gerenciamento autonômico do data center afeta o comportamento.

Cenário 5. Neste cenário, ou autores assumem que a política disponível para o gerenciamento autonômico no data center indica que um sistema deve ser "bloqueado"essencialmente para diminuir o processamento, com objetivo de diminuir o consumo energético.

Os resultados obtidos por Norouzi e Bauer (2015) por meio dos testes executados nos 5 cenários foram: A carga de trabalho executada no cenário 1 causa aumento da temperatura e o simulador não consegue calcular a energia consumida. Os cenários 2 e 3 apresentam resultados semelhantes, no entanto o dois consomem menos energia devido ao uso da política de computação verde. Como mostrado no cenário 4, a camada superior AM, sendo verde, causa o mesmo comportamento enquanto o nível AM do sistema é Verde. A comparação dos Cenários 1 e 5 mostra que a hierarquia de gerenciamento de três níveis proposta com determinadas políticas controla o comportamento do data center em termos de minimizar o consumo de energia.

2.6.2 *Towards an Agent-Based Symbiotic Architecture for Autonomic Management of Virtualized Datacenters*

O artigo de Liu e Da Silva et al. (2012) propõe uma arquitetura baseada em agentes para gerenciamento autônomo de nuvem, onde recursos e máquinas virtuais são associados a agentes de trabalho que monitoram mudanças em seus ambientes locais e interagem entre si, tomando suas próprias decisões e executando ações adaptativas supervisionadas por um conjunto de processos de gerenciamento.

Nesta arquitetura, os agentes monitoram os recursos físicos e às máquinas

virtuais de um data center, monitorando continuamente os eventos de interesse em seus ambientes locais, interagindo com outros agentes de maneira *peer-to-peer*, tomando decisões de gerenciamento de recursos de acordo com suas regras locais, e coordenando suas ações de forma reativa e proativa sob a supervisão de uma rede de processos gerenciais.

A arquitetura proposta por Liu e Da Silva et al. (2012) oferece uma base para o desenvolvimento de um modelo de monitoramento e gerenciamento inteligente, uma vez que se utiliza da computação autonômica para solucionar a crescente complexidade de gerenciar um data center moderno, buscando diminuir a necessidade de intervenção humana.

2.6.3 *Efficiency Metrics for Qualification of Datacenters in Terms of Useful Workload*

O trabalho de Munteanu e Debusschere et al. (2013) propõe duas métricas diferentes de eficiência para a qualificação de *datacenters* em termos de otimização de processos. O estudo busca através de um abordagem autonômica diminuir o custo energético da infraestrutura sem perda de poder computacional. Os autores buscam selecionar métricas para quantificar o uso de recursos de energia, resfriamento e cargas de trabalho.

A primeira métrica, EUE (kWh), necessita de modelos analíticos ou caracterizações experimentais de servidores, mas apresenta uma ferramenta precisa para a qualificação ou otimização do sistema de gerenciamento de energia. A segunda métrica, EUE (cpu), é mais geral, pode ser usada sem modelos ou experimentos específicos e é baseada em métricas já conhecidas. Ele apresenta uma ferramenta eficaz para o *benchmarking* do *datacenter* de computação em nuvem.

Os autores concluíram que em comparação com todas as outras principais métricas analíticas e numéricas, a métrica EUE propõe uma maneira alternativa de gerenciar ou comparar o IDC. É demonstrado que todas as outras métricas não são suficientes ou adequadas para gerenciamento de energia ou *benchmarking* da IDC.

2.6.4 *Self-organizing Sensing Infrastructure for Autonomic Management of Green Datacenters*

O estudo de Viswanathan, Lee e Pompili (2011) tem como objetivo propor uma abordagem de gerenciamento autonômico para e otimização do sistema de temperatura de um *datacenter* através de uma rede de sensores auto-gerenciáveis, que coleta amostras do ambiente em tempo real para monitorar oscilações e anomalias dentro do ambiente *datacenter*, composta pelos seguintes itens:

- Câmeras térmicas.
- Sensores escalares de temperatura e umidade.
- Sensor multicamada para medir o fluxo de ar.

O cenário da pesquisa foi o Centro de Computação Autônoma (CAC) da *National Science Foundation* (NSF).

O artigo está relacionado ao gerenciamento autonômico do ambiente de um *datacenter* e propõe resolver o desiquilíbrio térmico em relação a sua infraestrutura. Através dos dados obtidos pelo monitoramento da rede de sensores, os autores concluíram que, existem pontos em que ocorre uma maior geração de calor devido a Distribuição não uniforme de carga de trabalho entre servidores e a heterogeneidade do hardware, o que ocasiona superaquecimento e comprometimento do funcionamento dos recursos. No entanto, em pontos excessivamente refrigerados ocorre desperdício de energia devido ao resfriamento ineficiente e aumento desnecessário do custo operacional do *datacenter*.

2.6.5 *Server Virtualization in Autonomic Management of Heterogeneous Workloads*

O artigo de Steinder e Whalley et al. (2007) fala sobre o uso da tecnologia de virtualização de servidores no gerenciamento autônomo de *datacenters*, executando uma mistura heterogênea de cargas de trabalho. O trabalho apresenta um sistema que gerencia diferentes cargas de trabalho e suas metas de desempenho para demonstrar sua eficácia por meio de experimentos e simulação reais do sis-

tema. A pesquisa visa resolver problemas com o gerenciamento e balanceamento de cargas de trabalho em uma infraestrutura que possui hardware heterogêneo.

De acordo com os autores, a virtualização de servidores permite um melhor gerenciamento de cargas de trabalho em servidores, também introduz desafios consideráveis para seu uso eficaz. O trabalho estuda formas de configurar requisitos de infra-estrutura para fazer uso efetivo dos mecanismos de automação disponíveis.

O artigo de Steinder e Whalley et al. (2007) apresenta um sistema que permite gerenciar cargas de trabalho heterogêneas em um conjunto de máquinas de servidores heterogêneos usando mecanismos de automação fornecidos pelas tecnologias de virtualização de servidores.

2.6.6 *Energy Efficient Decision Making in Data Centers with Multiple Cooling Methods*

O artigo de Mousavi e Berezovskaya et al. (2017) propõe um método de gerenciamento para o sistema de refrigeração de um *datacenter*, que pode reagir adequadamente às mudanças de condições, como temperatura externa, temperatura ambiente do servidor, cargas de trabalho do equipamento de TI e temperatura das CPUs. O principal objetivo desta pesquisa é reduzir o consumo de energia do sistema de refrigeração através de sua operação adaptativa.

Visto que em um *datacenter* onde existe um mal gerenciamento de temperatura ambiente, a infraestrutura esta sujeita a falhas que podem resultar na indisponibilidade dos serviços. O trabalho de Mousavi e Berezovskaya et al. (2017) permite através de um sistema multi-agente reagir adequadamente às mudanças nas condições, como temperatura externa, temperatura ambiente do servidor, cargas de TI e temperatura das CPUs.

O estudo explora a cooperação de métodos de resfriamento dentro de um *datacenter* do ponto de vista de otimização de energia, se fizeram necessários mecanismos precisos de previsão de mudanças na temperatura da sala do servidor, temperatura de CPUs e consumo de energia de cada método de resfriamento.

Para coletar uma quantidade apropriada de dados, os autores executaram

a ferramenta de simulação por quatro vezes sob condições diferentes. Run1 e 2 simularam a sala do servidor com o método de ar livre (Global Fans) para a estação quente e fria, respectivamente. Em contrapartida, o Run 3 e 4 simulavam a sala do servidor com o método resfriado a ar com base líquida (SEE cooler) para a estação quente e fria consecutivamente. Em todas as execuções, a temperatura externa na estação quente foi de 25 C e na estação fria foi de -10 C.

Os autores observaram que, a ferramenta de simulação pode calcular a temperatura final de cada CPU, sala do servidor e o consumo de energia de cada componente, assim como todo o sistema em um período específico de tempo e para uma porcentagem específica de carga de TI. Com base nos valores calculados, um sistema de controle multiagente pode decidir qual dos métodos de resfriamento é o mais adequado para ser usado sob certas condições (por exemplo, estações quentes ou frias). Os autores concluíram que que a técnica proposta tem potencial para ser utilizada em situação real para fins de tomada de decisão automática.

2.6.7 *On the Use of Fuzzy Modeling in Virtualized Data Center Management*

O artigo de Xu e Zhao et al. (2007) apresenta um sistema autônomo de gerenciamento de recursos de dois níveis que permite o provisionamento autonômico e adaptável de recursos de acordo com a SLA (Service Level Agreement), especificando compensações dinâmicas da qualidade e do custo do serviço. O estudo apresenta um sistema de controle baseado em lógica fuzzy, que aplica a modelagem para caracterizar a relação entre a carga de trabalho do aplicativo e a demanda de recursos. Um protótipo do sistema foi implementado em um ambiente *datacenter* virtualizado.

Os autores implementaram um protótipo de sistema de gerenciamento de recursos de dois níveis proposto em um *testbed* de *datacenter* virtualizado. o trabalho utilizou aplicações típicas de *e-business* com cargas de trabalho sintéticas e rastreamentos reais para avaliar a modelagem difusa no controlador local e a alocação de recursos no controlador global. O artigo apresenta resultados que mostram que a abordagem proposta pode efetivamente alocar recursos para contêineres

virtuais sob cargas de trabalho que mudam dinamicamente.

O trabalho de Xu e Zhao et al. (2007) monitora periodicamente a carga de trabalho e o desempenho de aplicações,além do uso dos recursos utilizados para virtualização. Os autores utilizam métricas para a medição de desempenho as quais geralmente são obtidas diretamente no acordo de nível de serviço. Um exemplo, é a taxa de transferência (número de transações concluídas por segundo) ou o tempo médio de resposta do serviço. O trabalho apresenta uma modelagem adaptativa empregada pelo controlador local no qual o modelo é atualizado repetidamente com base nas informações monitoradas *online*.

2.6.8 An Intelligent Power Consumption Model for Virtual Machines Under CPU-intensive Workload in Cloud Environment

O artigo de Wu, Lin e Peng (2017) tem como objetivo analisar as assinaturas de energia de diferentes máquinas virtuais de configuração heterógeneas através de experimentos. O estudo aborda o proeminente problema do crescente consumo energético por parte dos *datacenters* de computação em nuvem, e o desafio de otimizar esse consumo sem que haja perda de poder computacional, além disso, de acordo com o estudo ocorre uma perda de precisão quando feito apenas o monitoramento energético convencional.

Os autores propões um modelo de energia para VMs (maquinas virtuais) denominado CAM , que pode se adaptar à reconfiguração de VMs e fornecer estimativas precisas de energia sob carga de trabalho intensiva da CPU. Tendo isso em vista a pesquisa busca medir com precisão o consumo de energia de um *datacenter* através de uma abordagem de monitoramento por softwares.

Os autores concluem que o modelo CAM também é preciso em estimar a potência em servidores físicos que hospedam várias VMs. Nesse caso, o erro máximo da CAM é de 4,04% e o erro médio é inferior a 1%. Diferente dos modelos baseados em máquinas físicas, o modelo pode fornecer estimativas de energia precisas e em tempo real para VMs.

2.6.9 *Smart Temperature Monitoring for Data Center Energy Efficiency*

O estudo de Qu e Li et al. (2013) tem como objetivo através da implantação de implantação de sensores, coletar informações de temperatura, de modo a ajustar a fonte de refrigeração do *datacenter* de maneira eficiente, e desta forma determinar o posicionamento ideal dos sensores. Assim a carga do sistema de refrigeração, pode ser minimizada com a ajuda da analise dos dados coletados, além de detectar e evitar pontos de aquecimento

Através de uma série de simulações os autores analisaram as variações de temperatura causadas por diferentes cargas de trabalho em cada *rack* de um *datacenter*, e desenvolveram um algorítimo para otimizar o uso do sistema de refrigeração e determinar o posicionamento ideal e maximizar a eficiência dos sensores.

Os resultados das simulações feitas no estudo de Qu e Li et al. (2013) mostraram que o algoritmo de otimização desenvolvido pelos autores poderia fornecer instruções sobre o número adequado de sensores a serem implantados em um rack e encontrar melhores temperaturas para adaptar a fonte de refrigeração

2.6.10 *Smart Data Center Monitoring System Based On Internet of Things*

A pesquisa de Fahrianto e Anggraini et al. (2017) tem como objetivo desenvolver um sistema de monitoramento inteligente baseado em IoT (*Internet of Things*). O trabalho enfatiza a importância dos *datacenters*, e de manter sua alta disponibilidade. A equipe observou que no decorrer de um ano ocorreram incidentes no *datacenter* devido à instabilidade de tensão e corrente enviada a fonte de alimentação, danificando o equipamento.

O sistema de monitoramento inteligente, monitora a anormalidade de energia utilizando o sensor de corrente elétrica SCT 013 e também o desvio da temperatura do ambiente e utiliza os seguintes componentes:

- Raspbery Pi3 usado como unidade de processamento e conexão wi-fi com arduino e o servidor de banco de dados.
- Sensor SCT 013, que monitora mede e digitaliza a corrente do cabo PLN,

usando o arduino.

- Arduino usando como conversor digital analógico e enviar os dados como dados seriais.
- O sensor de temperatura e umidade DHT-22 é usado para capturar a temperatura na sala do servidor.
- *Raspberry* pi envia os dados para o servidor de banco de dados.
- Servidor de banco de dados envia os dados para o servidor da web e visualiza os dados.
- Os dados coletados pela arquitetura de sensores são enviados ao banco de dados, e podem ser consultados pelo usuário do sistema através de uma interface web.

O sistema de monitoramento desenvolvido pelos autores pode capturar e monitorar corrente elétrica, temperatura e umidade do *datacenter*. Em seu desenvolvimento o autor utiliza várias tecnologias como sistemas embarcados, banco de dados e acesso a dados e gráficos através interface web.

2.6.11 *Non-invasive Cyber-Physical System for Data Center Management*

O artigo de Rossi e Rizzon et al. (2017) apresenta um *Cyber-Physical System* (CPS), e propõe uma nova estrutura para monitorar um *datacenter*. O CPS fornece monitoramento e resfriamento passivo/ativo gerenciável para os servidores, além de constar com uma unidade de coleta de energia termoelétrica é usada para fornecer energia. O objetivo da proposta é aumentar a eficiência de um *datacenter* de computação em nuvem.

O CPS, é uma combinação de um sistema, um sensor sem fio para monitoramento e um *cooler* ativo para o processador, os autores se referem a ele como dissipador de calor inteligente, que serve como um nó de coleta de dados, para fornecer controle remoto de parâmetros de saúde sob o paradigma da IoT. O dispositivo de monitoramento é alimentado com energia livre gerada por um sistema de Recuperação de Energia Termoelétrica (TERS) que os autores concluíram que

pode ser auto-sustentável, sob as condições disponíveis dentro de um *datacenter*. O TERS converte o calor dissipado pelo núcleo da CPU do data center em energia elétrica que é armazenada em um supercapacitor e alimenta o dispositivo de monitoramento.

Os autores realizaram um estudo de caso para avaliação de desempenho do sistema e validação do *framework* proposto. O sistema de Rossi e Rizzon et al. (2017) inclui um software simulador usado para prever a evolução da condição do servidor. Foi concluído que o mesmo pode ser usado para fornecer dados a um administrador do sistema, o que possibilita decidir a melhor estratégia para controlar todo o dissipador de calor inteligente implantado, para alterná-los para uma funcionalidade ou para outra e para fornecer comandos de controle ao gerenciador de carga de trabalho do datacenter.

2.6.12 *Toward a Meta-model for Elasticity Management in Cloud Applications*

A elasticidade é uma característica da computação em nuvem referente a flexibilidade de um serviço, ou seja, que permite o redimensionamento de recursos como processamento e armazenamento por exemplo. O estudo de Hiba e Belguidoum (2017) tem como objetivo oferecer um modelo genérico de gerenciamento autonômico de elasticidade, através de duas abordagens: MDA (*Model-Driven Architecture*) para fornecer o modelo e uma abordagem MAPE-K loop para automatizar o processo de gerenciamento de elasticidade.

Segundo Hiba e Belguidoum (2017) a abordagem MDA pode ser vista como uma solução para o problema do gerenciamento automatizado de elasticidade. Já o método MAPE-K, coleta detalhes de um sistema direcionado, para analisar esses detalhes e determinar se algo precisa ser alterado. Além de criar um plano ou sequência de ações que especifique as mudanças necessárias, e executa ações para atender às necessidades do usuário final ou do negócio.

A proposta principal baseia-se na classificação das estratégias de elasticidade e baseia-se no ciclo de controle de três fases: observação, decisão e ação.

- Fase de observação na qual um monitoramento em tempo real é realizado

para detectar instantaneamente qualquer evento ocorrido.

- Fase de decisão que permite estabelecer uma estratégia de elasticidade que resolve (como reação contra) o evento detectado.

- Fase de ação em que a estratégia proposta é executada.

Deste modo os autores descreveram um modelo de gerenciamento autonômico de elasticidade de recursos, que pode ser adaptado a diferentes ambientes. Em um infraestrutura de computação em nuvem onde são hospedados uma série de serviços e aplicações, uma abordagem autonômica de controle da elasticidade do poder computacional, é o primeiro passo para buscar a diminuição do custo operacional de um datacenter.

2.6.13 *Toward Efficient Autonomic Management of Clouds: A CDS-based Hierarchical Approach*

O trabalho de Martin, Kandasamy e Chandrasekaran (2018) propões usar o conceito de CDS (Connected Dominating Set), para o posicionar efetivamente os gerenciadores autônomos em uma infraestrutura de nuvem. O objetivo do estudo é oferecer uma abordagem hierárquica, baseada em CDS capaz de reduzir a sobrecarga de comunicação, evitar informações redundantes e fornecer uma plataforma para o gerenciamento efetivo de toda a infraestrutura.

Os autores observaram que o gerenciamento da grande quantidade de recursos rodando em um ambiente de computação em nuvem, exige o uso de gerentes com capacidades autônomas, de modo a lidar com um ambiente dinamicamente mutável. Tendo isso em vista o trabalho apresenta uma organização hierárquica dede gerentes autonômicos para controlar os recursos da nuvem.

Os autores obtiveram como resultado um possível layout dos nós nos quais devemos posicionar os AMs para facilitar o processo de gerenciamento dos data centers distribuídos e minimizar o custo de comunicação entre os nós. A conclusão do trabalho, foi que Empregar uma distribuição hierárquica de Gerentes Autônomos garante que os nós sejam atendidos a partir da camada mais próxima, reduzindo também o consumo de energia.

2.6.14 *An Intelligent and Integrated Architecture for Datacenters with Distributed Photonic Switching*

O estudo de Vassoler e Ribeiro (2017), apresenta um projeto de implementação e avaliação de uma arquitetura em três camadas automatizada por um controlador SDN (Software Defined Network) aumentado. Ele é capaz de reconfigurar a camada de links físicos e orquestrar a migração de (VMs) com base nas cargas de trabalho dos servidores físicos. A arquitetura também possui um mecanismo eficiente de roteamento implementado como uma função de rede virtual sobre uma topologia de rede de centro de dados centrada no servidor. O objetivo da pesquisa é automatizar ambientes de data center, desde a reconfiguração de links físicos de rede até o gerenciamento de VMs.

O artigo introduziu o desenho, implementação e avaliação do TRIIIAD, uma arquitetura inteligente para datacenter, composta por três camadas. A camada intermediária, ou camada de encaminhamento, é a rede de transporte de dados. A camada híbrida reconfigurável representa os dispositivos capazes de reconfigurar os links entre os elementos da rede física. E o plano vertical é responsável pelo controle, gerenciamento e orquestração.

Os autores concluíram que a implementação do TRIIIAD e a integração do processo de orquestração de nuvem no controlador SDN foi fundamental para garantir a estabilidade da plataforma. Já o escalonador baseado no uso de recursos do servidor (CPU, memória e trafêgo), promove um balanceamento de carga justo, ou seja, proporcional à capacidade de cada servidor na rede.

2.6.15 *BaNHFaP: A Bayesian Network Based Failure Prediction Approach for Hard Disk Drives*

O estudo de (CHAVES; PAULA; LEITE; QUEIROZ; GOMES; MACHADO, 2016) tem como objetivo a prevenção de falhas (*Hard Disk*) HD, através de atributos de monitoramento inteligente, como análise de relatórios e auto-monitoramento e desta evitar interrupções antes que ocorram. O artigo apresenta um método para previsão de falhas em unidades de disco rígido que utilizam Redes Bayesianas.

Os autores utilizam o método BaNHFaP, que contém os seguintes módulos:

pré-processamento, que implementa seleção de recursos e processo de categorização, que discretiza atributos inteligentes contínuos e estimação de parâmetros, para calcular as distribuições de probabilidade condicional para cada nó na rede.

O trabalho Chaves e Paula et al. (2016) se faz importante em um ambiente computação em nuvem, pois apresentou dados robustos referentes a análise de prevenção de falhas de HDs. Visto que os serviços executados em um *datacenter*, devem ser ininterruptos evitar falhas antes que ocorram pode fazer parte de uma abordagem de gerenciamento inteligente.

2.6.16 *Smart Datacenter Electrical Load Model for Renewable Sources Management*

Visto que os *datacenters* são um dos ambientes que mais consomem energia, o estudo de Caux, Rostirolla e Stolf (2018) tem como objetivo apresentar um módulo de gerenciamento inteligente de tarefas, cada tarefa j recebida pelo servidor do *datacenter* contém as seguintes informações: tj, que representa o tempo de execução da tarefa j em uma máquina de referência; memj que é a memória requisitada, rj representa o tempo de liberação da tarefa (o momento em que a tarefa pode começar a ser executada) e finalmente dj que representa o prazo (ou data de vencimento) desta tarefa. Desta forma é possível manter a qualidade de serviço e reduzir o custo operacional energético, balanceando a carga de trabalho e utilizando energia renovável.

A abordagem de algoritmo genético apresentada pelos autores foi capaz de reduzir em até 73% as sobrecargas impostas ao equipamento de TI, e aumentar apenas 1,8% o consumo de energia, respeitando a política fornecida pelo gerenciador.

2.6.17 Discussão dos trabalhos relacionados

O quadro 3 sintetiza uma visão geral dos trabalhos relacionados incluídos no presente projeto e suas principais diferenças diante da pesquisa proposta. Na primeira coluna constam os autores e ano de publicação do trabalho, na segunda coluna constam seus objetivos, na terceira os elementos monitorados em cada

trabalho, na quarta a abordagem autonômica utilizada e na quinta o cenário da realização da pesquisa.

O trabalho de Norouzi e Bauer (2015) propõe monitorar e diminuir o consumo energético de um *datacenter*, utilizando políticas de monitoramento autonômico e testando-as em 5 cenários simulados distintos com o objetivo de reduzir o consumo energético de uma infraestrutura, enquanto o presente trabalho busca propor um modelo conceitual de monitoramento e gerenciamento para *smart datacenter*, realizando a implantação referente ao consumo energético e o gerenciamento da temperatura dos servidores evitando o superaquecimento.

o presente trabalho visa propor um modelo conceitual focado em todos os elementos que fazem parte da infraestrutura de um *datacenter*, além de definir requisitos para determinar que uma infraestrutura seja inteligente. Outro aspecto é implantar parte do modelo no que se refere ao consumo energético e ao gerenciamento da temperatura dos componentes dos servidores.Enquanto o trabalho de Fahrianto e Anggraini et al. (2017) propõe e implanta um sistema de monitoramento para *smart datacenter* baseado em IoT, monitorando temperatura, umidade e corrente elétrica através de uma rede de sensores e microcontroladores, além de enviar as informações coletadas em tempo real para um banco de dados e disponibilizar uma interface web para consulta.

O estudo de Liu e Da Silva et al. (2012) tem o objetivo de diminuir a complexidade do gerenciamento de uma infraestrutura de nuvem computacional propondo uma arquitetura de controle inteligente de recursos físicos e virtuais baseada em agentes que monitoram os eventos e interagem entres si. Enquanto o presente trabalho propõe um modelo conceitual que abranja métodos de gerenciamento de poder computacional para *smart datacenter* e abordará melhores práticas referentes a este elemento da infraestrutura, no entanto não haverá implantações referentes a esse escopo.

A pesquisa de Munteanu e Debusschere et al. (2013) propõe métricas para medir a eficiência energética de um *datacenter* por meio de um balanceamento de carga de trabalho inteligente, buscando a redução do custo operacional deste elemento, além de propor uma maneira alternativa de gerenciar e comparar infraes-

truturas. Já o presente trabalho propõe em seu modelo conceitual diminuir o consumo energético dos servidores, utilizando abordagens dentro do conceito *smart datacenter* e testar sua eficiência na infraestrutura computacional do LARCC, portanto, nesta pesquisa serão analisadas métricas referentes ao consumo e custo energético, e se cabe a implantação de alguma delas no cenário estudado.

O trabalho de Viswanathan, Lee e Pompili (2011) propõe uma abordagem de gerenciamento autonômico para otimização do sistema de temperatura em um *datacenter* através de uma rede de sensores de temperatura auto-gerenciáveis além de câmeras térmicas estrategicamente posicionadas. Desta forma é possível identificar os chamados pontos de calor, e evita-los prevenindo o superaquecimento de componentes e o mau uso do sistema de refrigeração. Já o persente trabalho procura implantar a parte do modelo de monitoramento e gerenciamento de *smart datacenter* relativa ao controle de temperatura dos servidores, tomando ações pró-ativas para evitar problemas como superaquecimento do hardware dos seus servidores.

O estudo de Steinder e Whalley et al. (2007) tem como objetivo a otimização dos recursos computacionais de um *datacenter* através do gerenciamento inteligente da carga de trabalho dos servidores, utilizando um sistema que gerencia diferentes cargas para que metas de desempenho sejam cumpridas e os recursos otimizados. O modelo conceitual do presente trabalho propõe método para gerenciamento inteligente de recursos computacionais dentro do conceito de *smart datacenter*, estudando métodos e ferramentas que possam vir a otimizar o desempenho da infraestrutura do LARCC.

O trabalho de Mousavi e Berezovskaya et al. (2017) tem o objetivo de reduzir o consumo energético do sistema de refrigeração de um *datacenter* utilizado monitoramento e gerenciamento pró-ativo e reativo a temperatura dos equipamentos de TI. O modelo conceitual proposto no presente trabalho aborda este escopo e visa evitar o superaquecimento dos servidores do LARCC através do monitoramento pro-ativo e reativo da temperatura dos servidores executando ações adaptativas para preservar a integridade do hardware.

O estudo de Xu e Zhao et al. (2007) propõe e implementa o protótipo de um

sistema de gerenciamento baseado em lógica Fuzzy, para provisionar autonomicamente a carga de trabalho dos servidores em um ambiente *datacenter* virtualizado, através do monitoramento periódico e análise de desempenho. Já o modelo conceitual apresentado propõe métodos de gerenciamento inteligente de carga de trabalho dentro do conceito de *smart datacenter*, buscando a otimização dos recursos computacionais, embora não serão feitas implementações dentro deste escopo.

O trabalho de Wu, Lin e Peng (2017) tem como objetivo realizar experimentos, para analisar assinaturas energéticas de máquinas virtuais que possuem configurações heterogêneas e propor um modelo que forneça estimativas de energia sobre carga de trabalho intensiva da CPU, além de medir com precisão o consumo energético dos servidores. Enquanto o modelo conceitual proposto no presente trabalho irá propor monitoramento inteligente do consumo energético dos servidores, e testá-lo através da implantação da parte do modelo relativa ao consumo energético.

O presente trabalho irá testar parte do modelo conceitual proposto monitorando de forma inteligente a temperatura dos servidores e seus componentes, visando evitar o superaquecimento de hardware que pode vir a causar a perda de equipamentos. Enquanto o estudo de Qu e Li et al. (2013) tem como objetivo controlar o sistema de refrigeração de um ambiente *datacenter*, através da análise de uma rede de sensores de temperatura, com o objetivo de ganhar eficiência no uso deste recurso, além de determinar qual o melhor posicionamento para cada sensor.

O estudo de Rossi e Rizzon et al. (2017) propõe um CPS (*Cyber Physical System*), combinação de sistema, sensor sem fio e monitoramento de um *cooler* ativo para o processador do servidores, além disso, foi realizado um estudo de caso para avaliação de desempenho do sistema e validação do *framework* proposto. O CPS é utilizado para fornecer monitoramento ativo e passivo gerenciável para os servidores, e conta com uma unidade para armazenar energia termoelétrica e reutiliza-la. Enquanto o presente trabalho propôs testar parte do modelo conceitual monitorando de forma inteligente a temperatura do servidores e seus componentes, dentro do conceito de *smart datacenter*, e desta forma evitar superaquecimento e avariações em seus componentes.

O trabalho de Hiba e Belguidoum (2017) tem como objetivo oferecer um modelo genérico para gerenciamento autonômico que permite redimensionar recursos como processamento e armazenamento. Para isso é utilizado o método MAPE-K, por meio deste método é possível criar uma sequência de ações que foca em atender as necessidades do usuário final redimensionando recursos de forma dinâmica. O modelo conceitual proposto no presente trabalho considera o redimensionamento de recursos conforme a necessidade em um ambiente *smart datacenter*, com o objetivo de obter melhor otimização do poder computacional, no entanto não haverá implantações dentro deste escopo.

O estudo de Martin, Kandasamy e Chandrasekaran (2018) utiliza um conceito conhecido como CDS (*Connected Dominating Set*), para analisar e determinar o posicionamento de gerenciadores autônomos em um infraestrutura de computação em nuvem, fornecendo uma organização hierárquica e assim reduzir o risco de sobrecargas nos equipamentos de telecomunicações. Enquanto o modelo conceitual de monitoramento e gerenciamento para *smart datacenter* proposto no presente trabalho irá abordar teoricamente o controle dos recursos de telecomunicações de forma inteligente, visando o uso otimizado deste recurso.

Quadro 3: Trabalhos relacionados

Trabalhos	Objetivo	Elementos Monitorados	Abordagem Autonômica	Cenário
Trabalho atual	Propor um modelo de monitoramento inteligente	Foram selecionados após a pesquisa	Modelo e implementação parcial	Datacenter Físico
Norouzi Forough e Bauer (2015)	Testar eficiência energética de um datacenter	Energia de um datacenter	Testes de gerenciamento	Datacenter simulado
Fahrianto Feri e Anggraini (2017)	Implementar um sistema de Monitoramento Inteligente Baseado em (IoT)	Corrente elétrica, temperatura e umidade	Implementação de um sistema completo	Datacenter Físico
Liu Qi e Da Silva (2012)	Diminuir a complexidade de gerenciamento de um datacenter	Recursos Físicos e VMs	Propõe arquitetura de gerenciamento	Datacenter Simulado
Munteanu et al. (2013)	Propor métricas de eficiência	Custo energético, cargas de trabalho	Diminuir o custo energético sem perder poder computacional	Datacenter Simulado
Viswanathan Hariharasudhan e Lee (2011)	Propor uma abordagem	Temperatura ambiente	Gerenciamento autonômico e detecção de pontos de calor	Datacenter Físico
Steinder Malgorzata e Whalley (2007	Otimizar carga de trabalho	Recursos computacionais	Mecanismos de automação	Simulação de ambientes
Mousavi Arash e Berezovskaya (2017)	Reduzir consumo energético do sistema de refrigeração	Sistema de Refrigeração	Métodos reativo para controle de temperatura	Datacenter Fìsico
Xu et al. (2007)	Otimizar carga de trabalho	Recursos computacionais	Provisionamento autonômico de recurso	Datacenter virtualizado
Wu Wentai e Lin (2017)	Analisar assinaturas de energia	Energia de um datacenter	Método CAM para monitorar consumo energético de VMs	Datacenter virtualizado
Qu et al. (2013)	Ajuste eficiente de refrigeração	Sistema de Refrigeração	Analisando dados de uma rede de sensores	Datacenter Físico
Rossi Maurizio e Rizzon (2017)	Ajuste eficiente de refrigeração	Sistema de Refrigeração	Analisando dados de uma rede de sensores	Datacenter Físico
Hiba SaddamHocine e Belguidoum (2017)	Gerenciamento de elasticidade	Recursos computacionais	gerenciamento autonômico de elasticidade	Ambiente de testes
Martin John Paul e Kandasamy (2018)	Redução de sobrecarga	Recursos computacionais	Provisionamento autonômico de recursos	Ambiente de testes
Vassoler Gilmar L e Ribeiro (2017	Automatizar ambientes de data center	Rede datacenter	mecanismo eficiente de roteamento	Datacenter Físico
Chaves Iago C e de Paula (2016)	Prevenção de falhas de HD	Recursos computacionais	Monitoramento e análise inteligente de hardware	Datacenter Físico

CAPÍTULO 3: ANÁLISE DE RESULTADOS

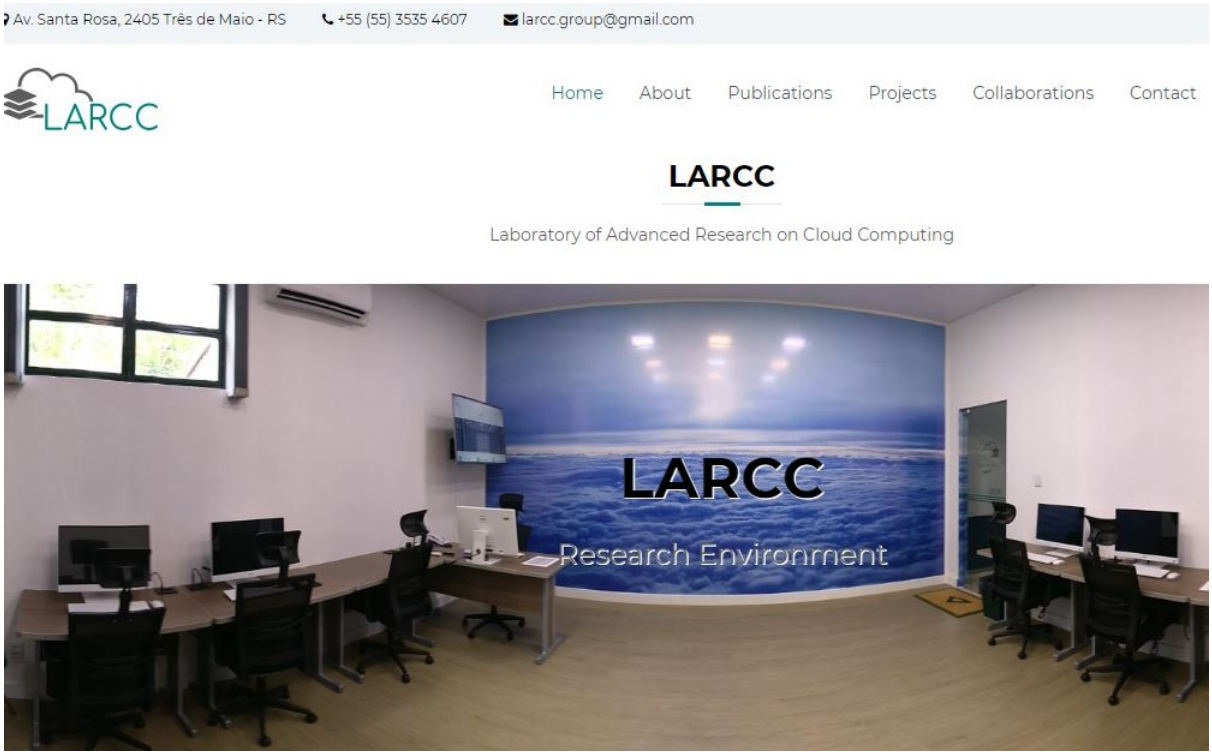
Neste Capítulo foram apresentados e analisados todos os resultados obtidos no presente trabalho, são eles: o levantamento da infraestrutura física e rede lógica, levantamento de requisitos de classificação de infraestrutura com base na norma ANSI/TIA 942, desenvolvimento do modelo conceitual para monitoramento e gerenciamento de *Smart Datacenters*, e validação prática dos respectivos modelos referentes a temperatura e energia.

3.1 LARCC

O LARCC (Laboratório de Pesquisas Avançadas para Computação em Nuvem) está localizado no campus da SETREM (Sociedade Educacional Três de Maio) e tem como coordenador o Prof. Dr. Dalvan Griebler. O principal objetivo do laboratório é disponibilizar uma infraestrutura de TI que viabilize a execução de pesquisas científicas na Faculdade, e possibilite um ambiente para aprendizado prático com equipamentos de TI de alto desempenho.

Deste modo, os estudantes que fazem parte do LARCC tem a possibilidade de executar testes e desenvolver suas pesquisas em servidores de alta performance, ou apenas utilizar de um ambiente preparado e bem equipado para a pesquisa. A Figura 15 mostra a página inicial do site do laboratório, que está disponível no endereço: http://larcc.setrem.com.br/. Nela são encontradas informações sobre o laboratório, seus projetos além de acesso as publicações de artigos desenvolvidos pelos estudantes do LARCC.

Figura 15: LARCC.

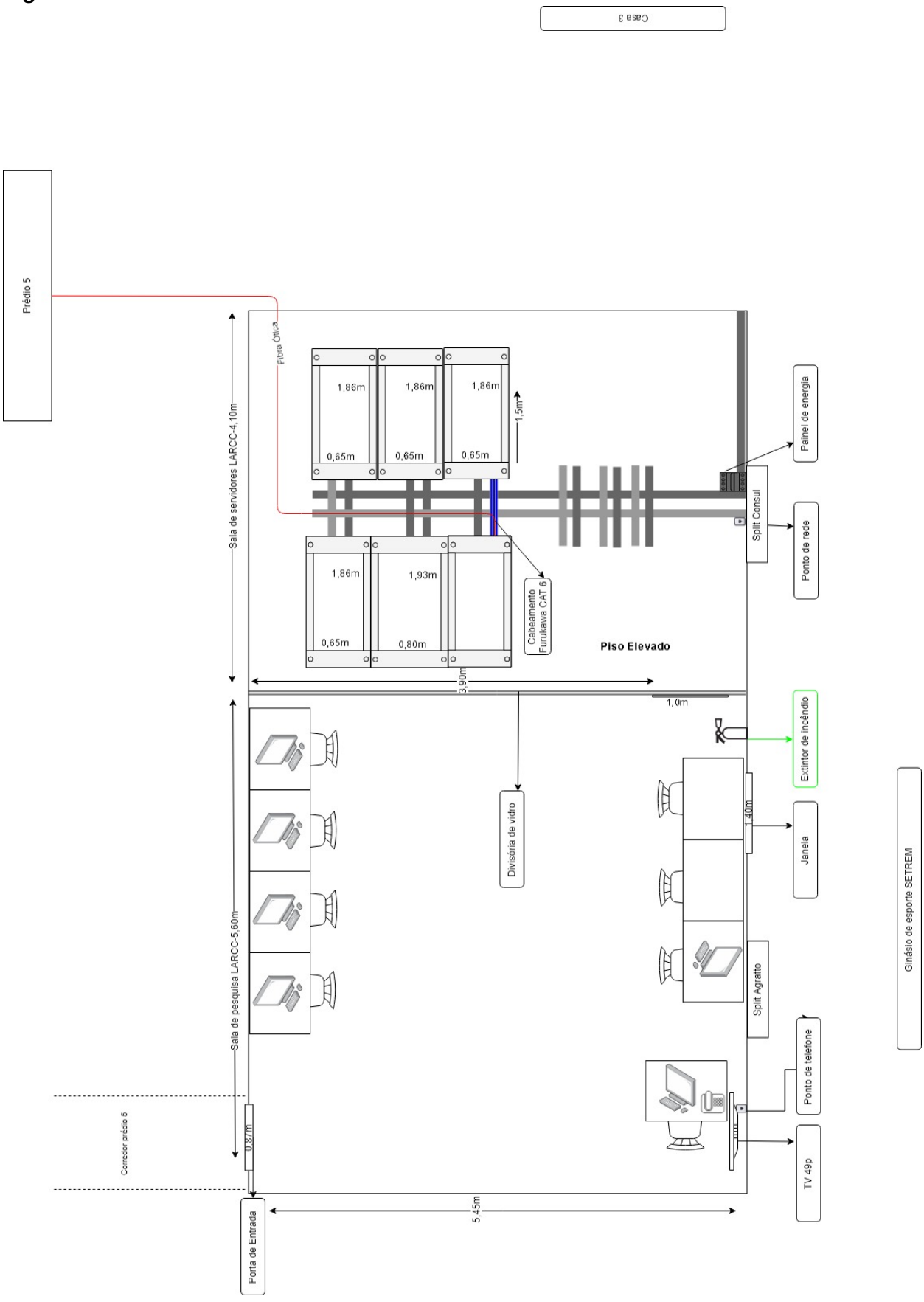


Atualmente o LARCC tem como linha de pesquisa os seguintes tópicos: Computação em nuvem e seus modelos de serviço, infraestrutura como serviço (IaaS), plataforma como serviço (PaaS), software como serviço (SaaS) além de Sistemas distribuídos (alto desempenho, replicação, alta disponibilidade e redundância), programação para redes (protocolos de aplicação), eficiência energética para data-center e nuvem privada e mineração de dados e aprendizado de máquina para agricultura.

3.2 LEVANTAMENTO DE INFRAESTRUTURA FÍSICA

Foi realizado um levantamento da infraestrutura física do LARCC ilustrado na Figura 16, com o objetivo de compreender a estrutura do laboratório e planejar de maneira inteligente o monitoramento e o gerenciamento de todos os elementos do seu ambiente *datacenter*. Nesta verificação são consideradas as principais normas referentes a instalação e gestão de *datacenters* e com base nelas as melhorias que podem vir a serem implementadas.

Figura 16: Levantamento da Infraestrutura Atual



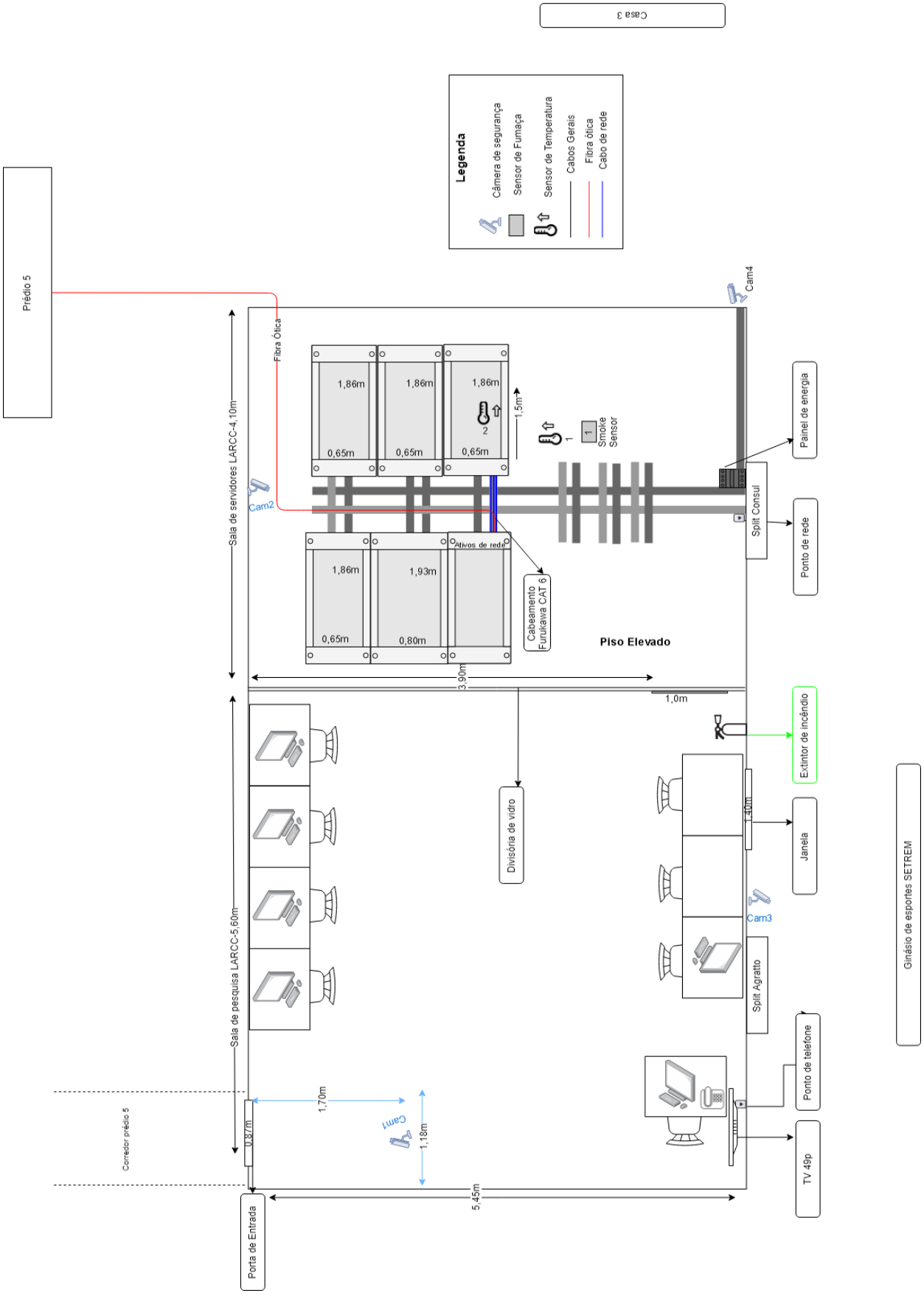
O espaço físico do LARCC está dividido em um ambiente de pesquisa equipado para proporcionar aos estudantes conforto e estrutura para a realização de estudos científicos, o qual conta com 6 computadores, Wi-Fi restrita aos estudantes do laboratório, climatização etc. E uma sala para os servidores que funciona como *datacenter*, o qual possui acesso físico restrito e está equipado e climatizado para suportar a infraestrutura de rede, telecomunicação e recursos os computacionais do laboratório.

Para desenvolver este levantamento físico foi realizado um estudo das principais normas que orientam a instalação e administração dos elementos que compõe um *datacenter*, são elas: ANSI TIA 942 para instalação e classificação de *datacenter*, para ISO 27002 segurança da informação e ASHRAE tc 9.9 para climatização de ambientes. Com base nesta análise foram levantados os requisitos que a infraestrutura do laboratório cumpre e os que podem ser implementados para melhorá-la nestes aspectos e assim fornecer um monitoramento e gerenciamento mais inteligente.

O ambiente *datacenter* do laboratório está constantemente sendo equipado e melhorado para armazenar o vasto poder computacional a disposição do LARCC e garantir a disponibilidade e integridade dos equipamentos. O ambiente possui um piso elevado o qual pode evitar acumulo de água e ocultar e proteger a maior parte do cabeamento de rede e de energia os quais são separados em diferentes eletrocalhas como ilustrado na Figura 17.

Com base nestas normas, a Figura 17 ilustra o posicionamento dos elementos existentes na infraestrutura do laboratório e onde devem ser posicionados aqueles que ainda não foram implementados. Além disso, são ilustradas medidas e distâncias recomendas entre os equipamentos.

Figura 17: Levantamento da Infraestrutura Proposta



A climatização da sala é feita por um ar condicionado split que funciona em tempo integral, mantendo a temperatura dentro das normas que se referem a este aspecto do *datacenter*, para evitar o superaquecimento de servidores e seus componentes o que torna este sistema fundamental. Para garantir manter seu funcionamento constante a solução mais utilizada é a utilização de sensores de temperatura, a Figura 17 sugere o posicionamento destes aparelhos que segundo a norma ASHRAE tc 9.9 2016 devem ficar a 1,5m do chão.

Estes ambientes são separados por um divisória de vidro que serve para restringir o acesso físico ao *datacenter* apenas a pessoas com autorização. Além disso, a Figura 17 ilustra o posicionamento de quatro câmeras de vigilância que serão utilizadas para complementar o gerenciamento e o monitoramento de acesso a infraestrutura. Estas câmeras estão instaladas de modo a cobrir pontos importantes do laboratório:

- A cam 1 está posicionada na entrada principal do laboratório e tem como objetivo monitorar e se necessário identificar quem tenha acessado o laboratório.

- A cam 2 tem o objetivo de monitorar a sala dos servidores identificando acessos não autorizados ao ambiente, dada a importância e o poder computacional nele instalados, além de detectar falhas que possam ser identificadas visualmente como a queda do sistema de refrigeração, por exemplo.

- A cam 3 esta posicionada externamente monitorando a janela do ambiente de pesquisa do laboratório com objetivo de identificar uma eventual tentaiva de entrada não autorizada.

- A cam 4 está posicionada externamente na parede dos fundos laboratório, possuindo um visão ampla do ambiente externo e do caminho da fibra ótica utilizada para o link de *internet*.

A norma ANSI TIA 942 convém que um *datacenter* tier 1 deve contar com um sistema de detecção de incêndio em seu ambiente, embora nesta categoria

não seja necessário detectores em cada rack. A Figura 17 sugere o posicionamento de um detector de fumaça na sala dos servidores do LARCC, no entanto este posicionamento traz o risco de detectar a fumaça quando os componentes do servidores já estiverem avariados, por tanto deve trabalhar em conjunto com outros sensores.

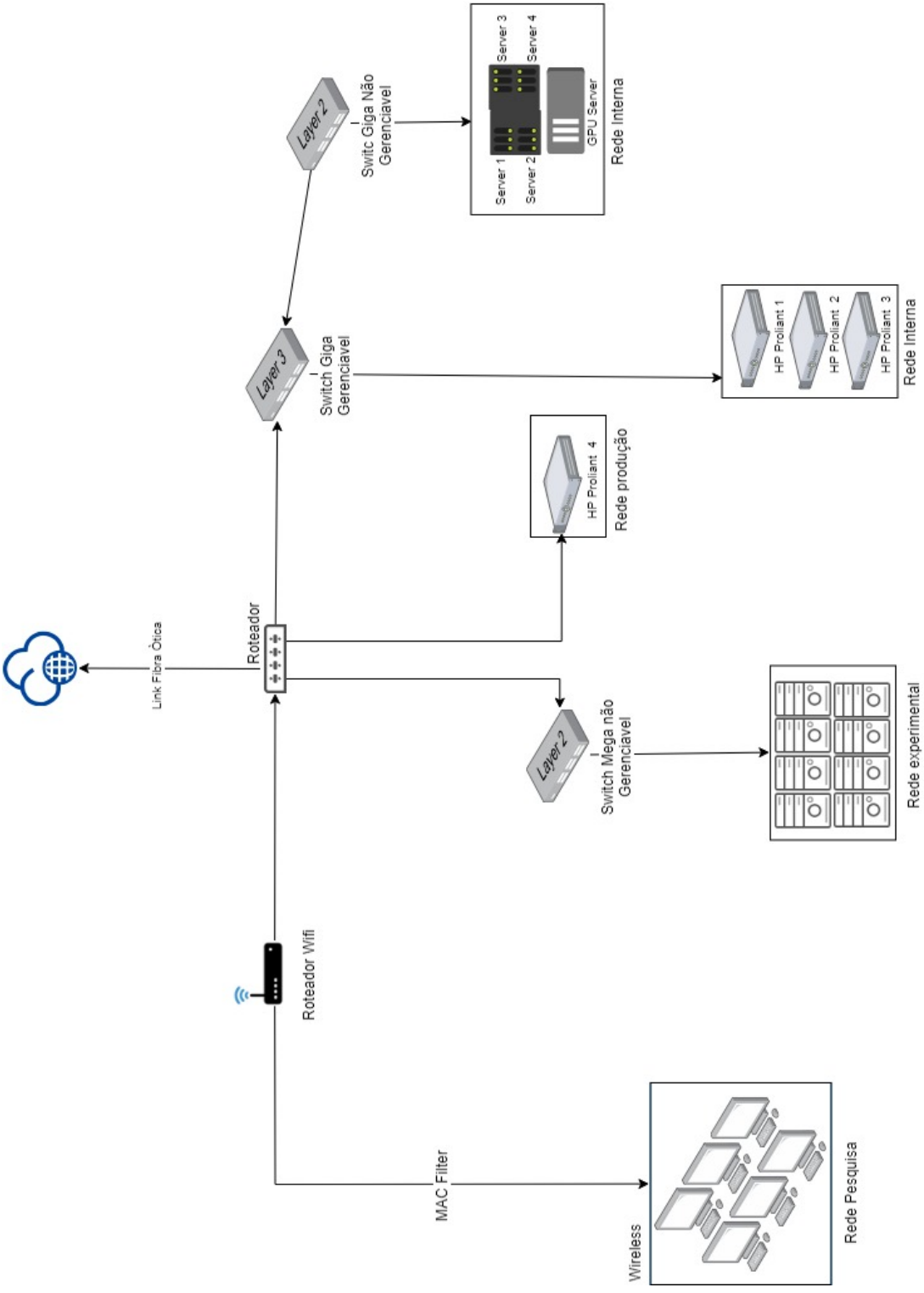
3.3 LEVANTAMENTO LÓGICO DA INFRAESTRUTURA

Para a realização da análise da infraestrutura de TI do LARCC e o planejamento de um modelo de monitoramento e gerenciamento inteligente que seja eficiente para a administração dos elementos, foi desenvolvido um levantamento lógico da rede do laboratório afim de listar seus elementos e identificar como eles estão interligados. Este estudo é fundamental para determinar como devem ser instaladas ferramentas, sensores e outros dispositivos que irão contribuir para tornar o *datacenter* do LARCC inteligente.

O LARCC possui um link de internet de 35 mbps disponibilizado através de cabeamento de fibra ótica conectado diretamente a uma RB (routerboard) Mikrotic do laboratório, equipamento utilizado para gerenciamento e roteamento da rede, e onde são ligados os principais ativos da rede como o roteador wifi utilizado no ambiente de pesquisa e switch principal utilizado no *datacenter* por exemplo.

A rede do LARCC esta segmentada da seguinte forma: uma rede separada para o servidor onde são executados os serviços utilizados no laboratório, duas redes internas para comunicação dos servidores, uma rede com 8 computadores dedicada exclusivamente para experimentos científicos e uma rede wireless para o ambiente de pesquisa onde os estudantes podem realizar seus estudos.

Figura 18: Levantamento da Lógico da Infraestrutura



Fonte: LARCC

3.4 LEVANTAMENTO DE SERVIÇOS

Para planejar o monitoramento e gerenciamento inteligente do uso de recursos computacionais do LARCC foi desenvolvido o levantamento de quais serviços estão rodando na infraestrutura do laboratório, e como está dividida está carga de trabalho. Os serviços de TI utilizados no LARCC são, Openldap, NFS, Zabbix e BackupPC, ambos executados em contêineres separados no servidor mustang 4.

O modelo do servidor HP proliant DL385 G6 que tem como configuração dois processadores 2x AMD Opteron 2425 2100 MHz Six-Core 6MB L3, Memória 32G DDR2 800 MHz, HD 8x 146 GB, 5 placas de rede, fonte 2x 460W 100-240V 6.0-3.0A (each), atualmente é suficiente para execução dos serviços de TI do laboratório.

3.5 CLASSIFICAÇÃO ATUAL DO DATACENTER

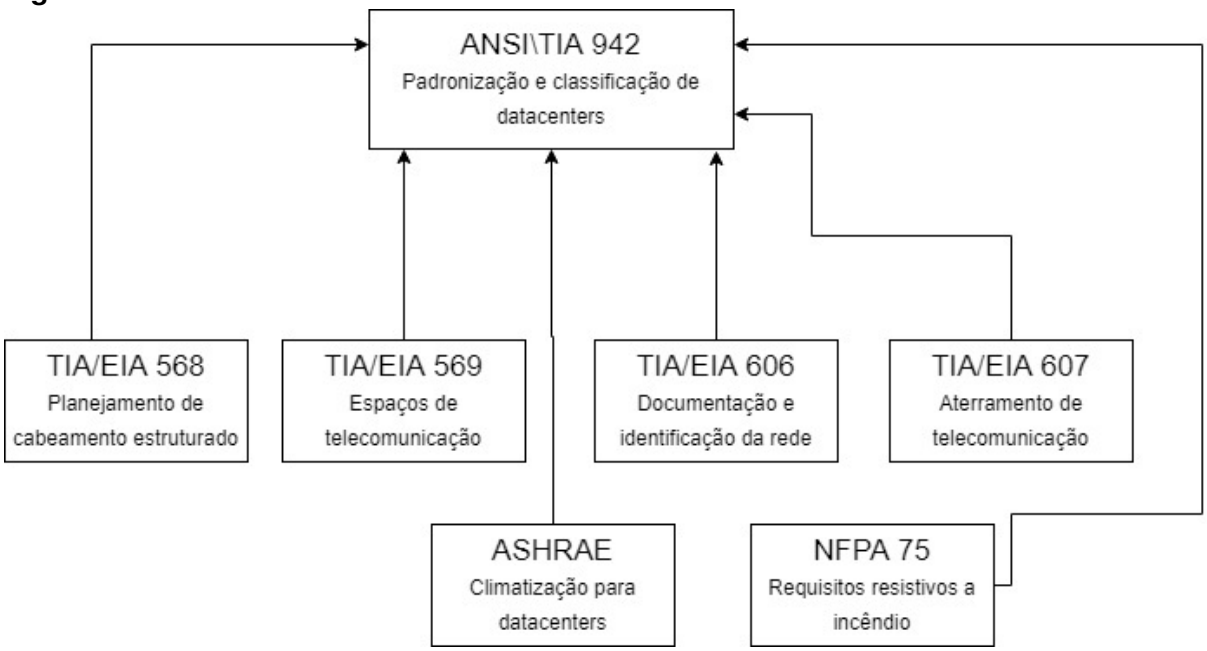
Para determinar a classificação atual do *datacenter* estudado, foi realizado um estudo aprofundado da norma ANSI TIA 942 A, que classifica as infraestruturas em quatro categorias, são elas: tier 1 que trata da capacidade básica, tier 2 que já apresenta alguns componentes redundantes, tier 3 que oferece um sistema auto sustentado e tier 4 que não possui tolerância a falhas no entanto existem poucas infraestruturas certificadas nesta categoria. O objetivo deste estudo é verificar quais são os requisitos atendidos pelo LARCC, e qual o caminho a ser percorrido para obter uma classificação.

A norma também apresenta algumas requisições importantes independente da categoria do *datacenter*, como por exemplo, suporte à substituição de componentes do sistema de energia e resfriamento. Além disto, as portas devem ter no mínimo 2,4 m de altura e 1,1 m de largura para portas simples e 1,8 m de largura para portas duplas. Estas medidas devem ser tomadas, pois existem equipamentos que não passariam por entradas menores, ocasionando problemas futuros.

A ANSI TIA 942 apresenta uma visão geral dos elementos de um *datacenter* e utiliza de um série de outras normas para apresentar detalhes específicos que são requisitados para a classificação dos seguintes elementos da infraestru-

tura: arquitetura da sala, equipamentos mecânicos principalmente o sistema de refrigeração, a rede elétrica e os equipamentos de telecomunicação. A avaliação destes componentes determina em qual tier a infraestrutura de TI se encaixa. A Figura 19 ilustra um diagrama simples das normas analisadas para a realização deste objetivo.

Figura 19: Análise de Normas.



Com o estudo e a análise das normas ilustradas na Figura 19 foi realizado o levantamento de requisitos para a classificação de *datacenter*. Os dados levantados foram tabulados de modo a exibir quais são os requisitos para cada categoria de *datacenter* de acordo com a ANSI TIA 942 e quais deles são cumpridos pela infraestrutura de TI do LARCC.

A Tabela 4 mostra todos os requisitos mecânicos requeridos dentro da infraestrutura de um *datacenter*, e como devem ser cumpridos dentro de cada um dos quatro tiers. As primeiras linhas apresentam quais são os requisitos de um modo geral, por exemplo, o nível de redundância para equipamentos mecânicos, ou seja como o sistema de refrigeração deve se comportar dentro de cada categoria em caso de requerido em cada categoria ou se existe uma forma de drenagem de água no ambiente.

Os elementos mecânicos de um *datacenter* são: sistema de refrigeração (HVAC) equipamento de umidificação e desumidificação, sistemas de contenção de incêndio e pressurização (O *datacenter* deve ser pressurizado positivamente para reduzir a infiltração de ar das áreas circundantes).

Em seguida a tabela aborda os requisitos do sistema de refrigeração do ambiente, os quais dizem respeito a redundância, alimentação de energia e gerenciamento deste equipamento, a dissipação de calor e por fim os requisitos de contenção de incêndio para equipamentos mecânicos como sistemas de detecção por exemplo.

Quadro 4: Tabela de classificação de requisitos mecânicos

Mecânico	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Geral				
Redundância para equipamentos mecânicos	Não requer	Perda de refrigeração	Não causa perda de resfriamento, mas pode elevar a temperatura	Não causará perda de resfriamento
Sistema de encanamento de água	Permitido mas não recomendado	Permitido mas não recomendado	Não permitido	Não permitido
Pressurização positiva	Não requer	Sim	Sim	Sim
Drenagem de água	Sim	Sim	Sim	Sim
Exige um gerador reserva	Não requer	Sim	Sim	Sim
Sistema de refrigeração				
Unidades redundantes de ar condicionado	Não requer	Uma unidade de AC redundante	Qtd. de Unidades AC suficientes para manter a área crítica	Qtd. de Unidades AC suficientes para manter a área crítica
Energia para sistema de refrigeração	Caminho único	Caminho único	Múltiplos caminhos	Múltiplos caminhos
Controle de umidade	Não requer	Sim	Sim	Sim
Dissipação de calor				
Sistema de refrigeração a água	Caminho único	Caminho único	Sistema de condensação de água	Sistema de condensação de água
Liberação de calor	Caminho único	Caminho único	Sistema de condensação a água	Sistema de condensação a água

Contenção de fogo				
Sistema de detecção de incêndio	Sim	Sim	Sim	Sim
Sistema de contenção de incêndio	Quando requisitado	Pré-ação (quando necessário)	Pré-ação (quando necessário)	Pré-ação (quando necessário)
Sistema de contenção de gases	Nenhuma exigência	Nenhuma exigência acima de AHJ	agentes limpos listados na NFPA	agentes limpos listados na NFPA
Sistema de Detecção de Fumaça	Nenhuma exigência	Sim	Sim	Sim
Sistema de Detecção de Vazamentos de água	Nenhuma exigência	Sim	Sim	Sim

A Tabela 5 traz a análise e classificação dos equipamentos mecânicos na infraestrutura do LARCC de acordo com os requisitos propostos pela ANSI TIA 942, a segunda coluna mostra quais requisitos a infraestrutura do laboratório já cumpre, a terceira coluna mostra quais requisitos ela deve cumprir após a implantação do modelo proposto neste estudo e por fim a quarta coluna mostra quais requisitos o laboratório pretende alcançar no futuro.

Quadro 5: Análise e Planejamento de Requisitos Mecânicos

Requisitos	Antes	Depois	Pretendido
Redundância para equipamentos mecânicos	Não possui	Tier 1	Tier 1, Tier 2
Sistema de encanamento de água	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Pressurização positiva do ambiente	Tier 1	Tier 1	Tier 1
Drenagem de água	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Exige um gerador reserva	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Unidades redundantes de ar condicionado	Tier 1	Tier 1	Tier 2
Energia elétrica para equipamentos	Tier1	Tier1	Tier1, Tier 2
Controle de umidade	Tier 1	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Sistema de refrigeração a água	Não possui	Não possui	Tier 1, Tier 2, Tier 3, Tier 4
Liberação de calor	Não possui	Não possui	Tier 1, Tier 2, Tier 3, Tier 4

Sistema de detecção de incêndio	Não está de acordo	Tier 1	Tier, Tier 3
Sistema de contenção de incêndio	Tier 2	Tier 2	Tier 2
Sistema de contenção de gases	Tier 1	Tier 1	Tier 1
Sistema de Detecção de Fumaça Antecipada	Tier 1	Tier 2, Tier 3, Tier 4	Tier 2, Tier 3, Tier 4
Sistema de Detecção de Vazamento de Água	Tier 1	Tier 1	Tier 1

A Tabela 6 apresenta os requisitos de telecomunicação para *datacenter* de acordo com a norma ANSI TIA 942 para e como devem ser cumpridos para estarem de acordo com cada uma das categorias. Um exemplo disso é a necessidade de um segundo provedor de internet com o objetivo de aumentar a segurança e oferecer uma maior disponibilidade nos serviços, que não é um requerimento em tier 1 estrutura básica, mas é exigido nas demais categorias.

Os requisitos apresentados na tabela 6 referente a telecomunicação de *datacenters* dizem respeito ao cabeamento, racks e ativos de rede, além dos os espaços físicos básicos que são: *Entrace Room* (ER) espaço de interconexão do cabeamento estruturado, Main *Distribution Area* (MDA): local onde se encontra a conexão central do Data Center e de onde se distribui o cabeamento estruturado e Horizontal *Distribution Area* (HDA): área utilizada para conexão com a área onde fica os equipamentos.

Quadro 6: Tabela de classificação de requisitos de telecomunicação

Telecom	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Cabeamento, racks, gabinetes e caminhos compatíveis com a norma	Sim	Sim	Sim	Sim
Entrada do cabo link de acesso	Não requer	Sim	Sim	Sim
Serviços de provedor de acesso redundante	Não requer	Não requer	Sim	Sim
Entrace Room (ER)	Não requer	Não requer	Não requer	Sim
Main Distribution Area (MDA)	Não requer	Não requer	Não requer	Sim
Áreas de distribuição intermediárias redundantes	Não requer	Não requer	Não requer	Sim

Cabeamento e vias de backbone redundante	Não requer	Não requer	Sim	Sim
Horizontal Distribution Area (HDA)	Não requer	Não requer	Não requer	Sim
Roteadores e switches devem ter alimentação redundante	Não requer	Não requer	Sim	Sim
Patch panels e cabos de rede devem ser rotulados conforme a norma ANSI / TIA-606-B	Sim	Sim	Sim	Sim
Armários e prateleiras devem ser rotulados na parte frontal e traseira	Sim	Sim	Sim	Sim
Patch cords e jumpers devem ser rotulados em ambas as extremidades	Não requer	Sim	Sim	Sim
Documentação de patch panel e cabo de conexão compatível com ANSI/TIA-606-B	Não requer	Não requer	Sim	Sim

A Tabela 7 traz a análise e classificação dos equipamentos de telecomunicação da infraestrutura do LARCC de acordo com os requisitos propostos pela ANSI TIA 942, a segunda coluna mostra quais requisitos a infraestrutura do laboratório já cumpre, a terceira coluna mostra quais requisitos ela deve cumprir após a implantação do modelo proposto neste estudo e por fim a quarta coluna mostra quais requisitos o laboratório pretende alcançar no futuro.

Os requisitos em que não houve uma conclusão quanto ao cumprimento do mesmo por parte da infraestrutura do LARCC, foram preenchidos como "em análise".

Quadro 7: Análise e Planejamento de Requisitos de Telecomunicação

Requisitos	Antes	Depois	Pretendido
Cabeamento, racks, gabinetes e caminhos compatíveis com a norma	Não possui	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4

Entrada do cabo linkde acesso	Não possui	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Serviços de provedor de acesso redundante	Não possui	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Entrace Room (ER)	Em análise	Em análise	Em análise
Main Distribution Area(MDA)	Em análise	Em análise	Em análise
Áreas de distribuição intermediárias redundantes	Em análise	Em análise	Em análise
Cabeamento e vias de backbone redundante	Não possui	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Horizontal Distribution Area (HDA)	Não possui	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Roteadores e switches possuem fontes de alimentação redundantes	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Patch panels e cabeamento devem ser rotulados conforme a norma ANSI / TIA-606-B	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Armários e prateleiras devem ser rotulados na parte frontal e traseira	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Patch cords e jumpers a serem rotulados em ambas as extremidades	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Documentação de patch panel e cabo de conexão compatível com ANSI/TIA-606-B	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4

Foi desenvolvida uma tabela de levantamento de requisitos de instalações elétrica para *datacenters* de acordo com a norma ANSI TIA 942. Para esta norma

convém que a empresa distribuidora de energia na cidade deve fornecer um serviço capaz de atender toda a demanda da infraestrutura do ambiente.

È importante salientar que quanto mais alta a tier maior o consumo energético da infraestrutura, portanto o cumprimento dos requisitos mostrados na tabela 8 não representa diretamente eficiência energética, mas sim maior nível de redundância e menor chance de *downtime*.

A ANSI TIA 942 apresenta as seguintes nomenclaturas para definir o nível de redundância da parte elétrica disponível na infraestrutura:

- N: o sistema atende aos requisitos básicos e não possui 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.
- 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.
- 2N: fornece duas unidades, módulos, caminhos ou sistemas completos para cada um necessário para um sistema básico. Falha ou manutenção de uma unidade, módulo, caminho ou sistema inteiro não interromperá as operações.

Desta forma o cumprimento destes requisitos pode aumentar o tempo de *uptime* do *datacenter* em caso de quedas de energia prolongadas. A Tabela 8 apresenta a primeira parte dos requisitos gerais energia redundante pra manutenções, pontos de falha toleráveis (emendas em cabos de energia por exemplo) e o cabeamento de energia, esta divisão foi feita dada a quantidade de requisitos nesta categoria apontados pela norma.

Quadro 8: Tabela de classificação de requisitos de instalação elétrica (parte 1)

Energia	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**

Geral				
Sistema que permita manutenção sem afetar a disponibilidade	Não requer	Gerador e sistema de no-break	Sim, mas não requer unidade de distribuição	Em todo sistema de distribuição
Pontos de falha toleráveis	Múltiplos	Múltiplos	Único	Não permitido
Análise do sistema de energia (Documentação)	Estudo de curto-circuito atualizado, coordenação e análise de arco voltaico	Estudo de curto-circuito atualizado, de coordenação e análise de arco voltaico	Estudo de curto-circuito atualizado, de coordenação, análise de arco voltaico e de fluxo de carga	Estudo de curto-circuito atualizado, de coordenação, análise de arco voltaico e de fluxo de carga
Cabos de energia para equipamentos	Alimentação de cabo único com capacidade de 100%	Alimentação de cabo único com capacidade de 100%	Alimentação de Cabo Redundante com 100% de capacidade no cabo ou cabos restantes	Alimentação de Cabo Redundante com 100% de capacidade no cabo ou cabos restantes
Quadro de Comando Principal				
Serviço	Serviço Compartilhado	Serviço Compartilhado	Serviço Dedicado	Serviço Dedicado
Construção	Quadro de painéis com parafuso em disjuntores	Quadro de painéis com parafuso em disjuntores	Quadro de painéis com parafuso em disjuntores	Quadro de painéis com parafuso em disjuntores
Supressão de Surtos	Não requer	Não requer	Sim	Sim
Sistema de fonte de alimentação ininterrupta				
Redundância	N	N	N+1	2 N
Topologia	Módulos Simples ou Paralelos	Módulos Simples ou Paralelos	Módulos Redundantes Distribuídos ou Sistema de Blocos	Módulos Redundantes Distribuídos ou Sistema de Blocos

Desvio automático	Não requer	Sim com alimentador não dedicado para bypass automático	Sim com alimentador não dedicado para bypass automático	Sim com alimentador não dedicado para bypass automático
Arranjo de Bypass de Manutenção	Não requer	Alimentador de bypass de manutenção não dedicado para a central de saída da UPS	Alimentador de bypass de manutenção não dedicado	Alimentador de bypass de manutenção não dedicado
Distribuição de energia de saída	Placa do painel incorporando disjuntores magnéticos térmicos padrão	Placa do painel incorporando disjuntores magnéticos térmicos padrão	Quadro de distribuição incorporando disjuntor removível	Quadro de distribuição que incorpora o disjuntor removível
Sequência de bateria	String dedicada para cada módulo	String dedicada para cada módulo	String dedicada para cada módulo	String dedicada para cada módulo
Tipo de Bateria	Válvula de 5 anos regulada por chumbo ácido ou volante	Válvula de 10 anos regulada por chumbo ácido ou volante	Válvula de 15 anos regulada por chumbo ácido ou volante	Válvula de 20 anos regulada por chumbo ácido ou volante
Tempo de backup mínimo da bateria	5 minutos	7 minutos	10 minutos	15 minutos
Sistema de monitoramento de bateria	Não requer	Não requer	Nível de corda pelo sistema de UPS	Sistema automatizado centralizado
Unidade de Distribuição de Energia				
Transformador	Alta eficiência padrão	Alta eficiência padrão	K-Rated alta eficiência	K-Rated alta eficiência
Interruptor de Transferência Automática				
Dispositivo de sobrecorrente	Não requer	Não requer	Disjuntor	Disjuntor
Procedimento Bypass de Manutenção	Não requer	Não requer	Manual guiado com intertravamento mecânico	Operação automática

Saída	Não requer	Não requer	Disjuntor duplo	Disjuntor duplo

A Tabela 9 traz a análise e classificação da infraestrutura elétrica do LARCC parte 1 de acordo com os requisitos propostos pela ANSI TIA 942, a segunda coluna mostra quais requisitos a infraestrutura do laboratório já cumpre, a terceira coluna mostra quais requisitos ela deve cumprir após a implantação do modelo proposto neste estudo e por fim a quarta coluna mostra quais requisitos o laboratório pretende alcançar no futuro.

Os requisitos em que não houve uma conclusão quanto ao cumprimento do mesmo por parte da infraestrutura do LARCC, foram preenchidos como "em análise".

Quadro 9: Análise e Planejamento de Requisitos de Energia (parte 2)

Requisitos	Antes	Depois	Pretendido
Sistema que permita manutenção sem afetar a disponibilidade	Tier 1	Tier 1, Tier2	Tier 1, Tier2, Tier 3
Pontos de falha	Tier 1, Tier2	Tier 1, Tier2	Tier 1, Tier2
Análise do sistema de energia	Não possui	Tier 1, Tier2	Tier 1, Tier2
Cabos de Força para Equipamentos	Tier 1, Tier2	Tier 1, Tier2	Tier 1, Tier2
Serviço	Tier 1, Tier2	Tier 1, Tier2	Tier 1, Tier2
Construção	Tier2, Tier3, Tier 4	Tier 2, Tier 3, Tier 4	Tier2, Tier3, Tier 4
Supressão de Surtos	Tier 1, Tier2	Tier 1, Tier2	Tier3, Tier 4
Redundância	Tier 1, Tier2	Tier 1, Tier2	Tier 3
Topologia	Tier 1, Tier 2	Tier 1, Tier 2	Tier 1, Tier 2
Desvio automático	Tier 1	Tier 1	Tier 2, Tier 3, Tier 4
Arranjo de Bypass de Manutenção	Tier 1	Tier 1	Tier 2, Tier 3, Tier 4
Distribuição de energia de saída	Em análise	Em análise	Em análise

Sequência de bateria	Não possui	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Tipo de Bateria	Não possui	Tier 1, Tier 2, Tier 3, Tier 4	Tier 1, Tier 2, Tier 3, Tier 4
Tempo de backup mínimo da bateria	Tier 1	Tier 2	Tier 4
Sistema de monitoramento de bateria	Não possui	Tier 3	Tier 3
Transformador	Tier 1, Tier 2	Tier 1, Tier 2	Tier 1, Tier 2
Dispositivo de sobrecorrente	Não possui	Não possui	Tier 3,Tier 4
Procedimento Bypass de Manutenção			
Saída	Tier 1, Tier 2	Tier 1, Tier 2	Tier 1, Tier 2

A Tabela 10 apresenta a segunda parte dos requisitos para instalações elétricas em *datacenters* descritos na ANSI TIA 942 de 2012 para cada uma das Tiers definada na norma. Entres eles estão o aterramento, sistema de desligamento de emergência (EPO), Monitoramento energético, sala de baterias, testes e manutenção do equipamento.

Quadro 10: Tabela de classificação de requisitos de instalação elétrica

Energia	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Aterramento				
Sistema de proteção contra raios	Com base na análise de risco de acordo com a NFPA 780	Com base na análise de risco de acordo com a NFPA 780	Sim	Sim
Dispositivos elétricos de iluminação neutros	Não requer	Não requer	Sim	Sim
Infraestrutura de aterramento do datacenter	Conforme exigido pelo ANSI / TIA-607-B	Conforme exigido pelo ANSI / TIA-607-B	Conforme exigido pelo ANSI / TIA-607-B	Conforme exigido pelo ANSI / TIA-607-B
Sistema de desligamento de emergência (EPO)				

Instalação	Se requerido pelo AHJ, com protetor de tampa e etiqueta de aviso	Se requerido pelo AHJ, com protetor de tampa e etiqueta de aviso	Se requerido pelo AHJ, com protetor de tampa e etiqueta de aviso	Se requerido pelo AHJ, com protetor de tampa e etiqueta de aviso
Modo de teste	Não requer	Não requer	Sim	Sim
Alarme	Não requer	Não requer	Sim	Sim
Botão de interrupção	Não requer	Não requer	Conforme permitido pelos códigos locais	Conforme permitido pelos códigos locais
Monitoramento Central de Energia				
Pontos de Monitoramento	Não requer	Utilitário UPS Generator	Entradas saídas, equipamentos, transferência e corrente Utilitário UPS Generator	Entradas e saídas, equipamentos, transferência, corrente cargas e surtos
Método de Notificação	Não requer	Console da sala de controle	Console da sala de controle, pager, e-mail e / ou mensagem de texto	Mensagem do console da sala de controle, pager, email para várias instalações
Sala de Baterias				
Separado das UPS	Não requer	Não requer	Sim	Sim
Cabos de bateria individuais isolados uns dos outros	Não requer	Não requer	Sim	Sim
Vidros resistentes para visualização	Não requer	Não requer	Não requer	Sim
Teste				
Teste de aceitação de fábrica	Não requer	Não requer	Sistemas UPS e Geradores	Sistemas UPS e Geradores, controles de geradores, ASTS

Teste do disjuntor do local	Não requer	Não requer	Teste de resistência de contato	Teste de Injeção Primária e Resistência de Contato de todos os disjuntores
Comissionamento	Não requer	Nível de componente	Nível de componente e de sistema	Nível de componente, de sistema e teste de interrupção
Manutenção de Equipamento				
Funcionários de Operação e Manutenção	Fora do local. De plantão	Apenas mudança de dia no local. De plantão em outros momentos	24 horas no local M-F, plantão nos finais de semana	No local 24/7
Manutenção preventiva	Nenhuma exigência	Manutenção do gerador	Manutenção de gerador e UPS	Programa abrangente de manutenção preventiva
Programas de treinamento em instalações	Nenhuma exigência	Treinamento limitado pelo fabricante	Programa abrangente de treinamento	Programa de treinamento abrangente e operação manual

A Tabela 9 traz a análise e classificação da infraestrutura elétrica do LARCC parte 2 de acordo com os requisitos propostos pela ANSI TIA 942, a segunda coluna mostra quais requisitos a infraestrutura do laboratório já cumpre, a terceira coluna mostra quais requisitos ela deve cumprir após a implantação do modelo proposto neste estudo e por fim a quarta coluna mostra quais requisitos o laboratório pretende alcançar no futuro. Tais requerimento interferem diretamente no nível de contenção e capacidade de *uptime* da infraestrutura quando a mesma for exposta a eventos críticos relacionados a surtos elétricos.

Os requisitos em que não houve uma conclusão quanto ao cumprimento

do mesmo por parte da infraestrutura do LARCC, foram preenchidos como "em análise".

Quadro 11: Análise e Planejamento de Requisitos de Energia (parte 2)

Requisitos	Antes	Depois	Pretendido
Sistema de proteção contra raios	Tier 2	Tier 2	Tier 4
Dispositivos elétricos de iluminação neutros	Tier 1, Tier 2	Tier 2	Tier 3, Tier 4
Infraestrutura de aterramento do *datacenter*	Não possui	Não possui	Tier 1, Tier2, Tier 3 e Tier 4
Instalação	Não possui	Não possui	Tier 1, Tier2, Tier 3 e Tier 4
Modo de teste	Tier 1, Tier2	Tier 1, Tier2	Tier 3 e Tier 4
Alarme	Tier 1, Tier2	Tier 1, Tier2	Tier 3 e Tier 4
Botão de interrupção	Tier 3 e Tier 4	Tier 3 e Tier 4	Tier 3 e Tier 4
Pontos de Monitoramento	Tier 1	Tier 4	Tier 4
Método de Notificação	Tier 1	Tier 4	Tier 4
Separado das UPS	Tier 1, Tier2	Tier 1, Tier2	Tier 3 e Tier 4
Cabos de bateria individuais isolados uns dos outros	Tier 1, Tier2	Tier 1, Tier2	Tier 3 e Tier 4
Vidros resistentes para visualização	Tier 1, Tier2, Tier 3	Tier 1, Tier2, Tier 3	Tier 4
Teste de aceitação de fábrica	Tier 1, Tier2	Tier 1, Tier2	Tier 3 e Tier 4
Teste do disjuntor do local	Tier 1, Tier2	Tier 1, Tier2	Tier 3 e Tier 4
Comissionamento	Tier 1	Tier 1	Tier 2, Tier 3, Tier 4
Funcionários de Operação e Manutenção	Tier 1	Tier 1	Em análise
Manutenção preventiva	Tier 1, Tier2	Tier 1, Tier2	Tier 3 e Tier 4
Programas de treinamento em instalações	Tier 1	Tier 1	Em análise

Foi desenvolvida uma tabela com o levantamento de requisitos de arquitetura de *datacenter* de acordo com a norma ANSI TIA 942, para cada uma de suas categorias, os quais dizem respeito a estrutura física e localização do prédio. A norma requer que o edifício tenha resistência a ações climáticas como tempestades ou cargas eólicas por exemplo. Esta proteção e segurança são divididas em quatro categorias são elas:

- Arquitetonicamente, um data center de Tier 1 não possui proteção contra eventos físicos (intencionais ou acidentais), naturais ou provocados pelo homem, que podem ocasionar falhas ou downtime.
- As instalações da Tier 2 devem atender a todos os requisitos da Tier 1 além de incluir proteções mínimas adicionais contra alguns eventos físicos, intencionais ou acidentais, naturais ou provocadas pelo homem, que podem causar falha no data center.
- As instalações Tier 3 devem atender a todos os requisitos da Tier 2, possui proteção contra a maioria dos eventos físicos, intencionais ou acidentais, naturais ou provocados pelo homem, que podem causar falha ou downtime.
- Um *datacenter* Tier 4 considera todos os possíveis eventos físicos que poderiam causar falha no *datacenter*. Também fornece proteções específicas e em alguns casos, redundantes contra esses eventos. Além de considerar os possíveis problemas com desastres naturais, como eventos sísmicos, enchentes, incêndios, furacões e tempestades, bem como problemas potenciais com o terrorismo e funcionários insatisfeitos. As infraestruturas deste nível têm controle sobre todos os aspectos de suas instalações.

Devido a quantidade de requisitos relacionados a arquitetura de *datacenters* encontrados na ANSI TIA 942, optou-se pela divisão desta tabela em partes, deste modo melhorando e otimizando a leitura e análise da mesma. A Tabela 12 traz requisitos relacionados a localização física do ambiente *datacenter*, ou seja cuidados que devem ser tomados antes de escolher o local de construção do prédio (Distância mínima de zonas de alagamento, aeroportos e rodoviárias), requisitos de estacionamento, ocupação multi-tenat que diz respeito servidores inquilinos

permitidos no ambiente e os requisitos de contenção de incêndio baseados na norma NFPA 75.

Quadro 12: Tabela de classificação de requisitos de arquitetura (parte 1)

Arquitetura	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Cuidados com área de risco de inundação	Não requer	50 anos sem registro	50 anos sem registro, altitude de 91m	100 anos sem registro, altitude de 91m
Distância mínima vias navegáveis, interiores e costeiras	Não requer	Não requer	mínimo 91 m	mínimo 0,8 km
Distância mínima de rodoviárias e linhas ferroviárias	Não requer	Não requer	Maior que 91 m	Maior que 0,8 km
Distância mínima aeroportos	Não requer	Não requer	Maior que 1,6 km e menor que 48 km	Maior que 1,6 km e menor que 48 km
Estacionamento				
Áreas de estacionamento separadas para visitantes e funcionários	Não requer	Não requer	sim (com entradas separadas)	sim (fisicamente separados)
Distância de docas de carregamento	Não requer	Não requer	sim (com entradas separadas)	sim (com entradas separadas)
Distância do estacionamento dos visitantes	Não requer	Não requer	Separação mínima de 9,1 m com barreiras físicas	Separação mínima de 18,3 m com barreiras físicas
Ocupação multi-tenant dentro do edifício	Sem restrição	Permitido somente em ocupações não-perigosas	Permitido se forem data-centers ou empresas de telecomunicações	Permitido se forem data-centers ou empresas de telecomunicações
Construção civil				
Tipo de construção (IBC 2006)	Sem restrição	Sem restrição	Tipo IIA, IIIA, ou VA	Tipo IA ou 1B
Requisitos resistivos ao fogo				
Paredes externas resistentes	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 4 horas
Paredes internas resistentes	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 2 horas
Paredes sem aberturas	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 4 horas

Estrutura resistente	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 2 horas
Paredes divisórias interiores não para computador	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 4 horas
Paredes divisórias interiores de sala de computadores	Código admissível	Código admissível	Mínimo de hora	Mínimo de 1 hora
Caixas do eixo	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 2 horas
Telhados resistentes	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 2 horas
Caixas do eixo	Código admissível	Código admissível	Mínimo de 1 hora	Mínimo de 2 horas
Cumprir os requisitos da NFPA 75	Não requer	Sim	Sim	Sim

A Tabela 13 traz a análise e classificação da arquitetura do LARCC de acordo com os requisitos propostos pela ANSI TIA 942, a segunda coluna mostra quais requisitos a infraestrutura do laboratório já cumpre, a terceira coluna mostra quais requisitos ela deve cumprir após a implantação do modelo proposto neste estudo e por fim a quarta coluna mostra quais requisitos o laboratório pretende alcançar no futuro.

Os requisitos em que não houve uma conclusão quanto ao cumprimento do mesmo por parte da infraestrutura do LARCC, foram preenchidos como "em análise".

Quadro 13: Análise e Planejamento de Requisitos de Arquitetura (parte 1)

Requisitos	Antes	Depois	Pretendido
Cuidados com área de risco de inundação	Tier 1	Tier 1	Tier 2
Distância mínima vias navegáveis, interiores e costeiras	Tier 1, Tier 2	Tier 1, Tier 2	Tier 3
Distância mínima de rodoviárias e linhas ferroviárias	Tier 1, Tier 2	Tier 1, Tier 2	Tier 3
Distância mínima aeroportos	Tier 1, Tier 2	Tier 1, Tier 2	Tier 1, Tier 2

Áreas de estacionamento separadas para visitantes e funcionários	Tier 1, Tier 2	Tier 1, Tier 2	Tier 1, Tier 2
Distância de docas de carregamento	Tier 1, Tier 2	Tier 1, Tier 2	Tier 1, Tier 2
Distância do estacionamento dos visitantes	Tier 1, Tier 2	Tier 1, Tier 2	Tier 1, Tier 2
Ocupação *multi-tenant* dentro do edifício	Tier 1	Tier 1	Tier 2
Tipo de construção (IBC 2006)	Em análise	Em análise	Em análise
Paredes externas resistentes	Não possui	Não possui	Tier 1, Tier 2
Paredes internas resistentes	Não possui	Em análise	Tier 1, Tier 2
Paredes sem aberturas	Não possui	Em análise	
Estrutura resistentes	Não possui	Em análise	Tier 1, Tier 2
Paredes divisórias interiores não para computador	Não possui	Em análise	Tier 1, Tier 2
Paredes divisórias resistentes	Não possui	Em análise	Tier 1, Tier 2
Caixas do eixo	Não possui	Em análise	Tier 1, Tier 2
Telhados resistentes	Não possui	Em análise	Tier 1, Tier 2
Caixas do eixo	Não possui	Em análise	Tier 1, Tier 2
Cumprir os requisitos da NFPA 75	Não possui	Não possui	Tier 2, Tier 3, Tier 4

Com a análise da classificação da infraestrutura atual do LARCC, de acordo com os requisitos levantados da norma TIA 942 foi possível compreender a nível de abrangência do laboratório .

3.6 MODELO CONCEITUAL

Segundo Mukherjee e Banerjee et al. (2010) um *datacenter* possui apenas dois status: **normal**, quando todos os equipamentos ativos (tanto recursos

computacionais, quanto a infraestrutura elétrica mecânica e de telecomunicações) atendem todas as demandas sem risco de perda de qualidade de serviços, disponibilidade ou superaquecimento de componentes, e **crítico**, quando estes riscos ficam eminentes. O principal objetivo deste trabalho é o desenvolvimento de um modelo conceitual de gerenciamento e monitoramento para *smart datacenters* para orientar de modo inteligente como manter um infraestrutura no estado normal em tempo integral.

São chamados eventos críticos os imprevistos capazes de mudar o status de um *datacenter* de normal para crítico. Tendo em vista a complexidade atual das infraestruturas, a resolução manual de cada possível eventualidade que pode interferir no funcionamento correto dos equipamento torna-se inviável de ser executada manualmente. Dessa forma, métodos inteligentes de resolução são uma potencial solução para automatizar a resolução de problemas, sendo então um dos principais pontos deste modelo.

Como parte do modelo foi desenvolvida uma tabela de eventos que podem mudar o status de um *datacenter* de normal para crítico, os quais foram levantados a partir do estudo de trabalhos relacionados e das normas referentes a instalação, classificação, monitoramento e gerenciamento de infraestruturas de TI complexas. A tabela 14 mostra além dos eventos quais podem ser suas causas, que tipo de problema podem causar na infraestrutura.

Dentre os eventos críticos mostrados na Tabela 14 estão, alterações bruscas na carga de trabalho que podem ser originadas a partir de falha humana (má operação dos recursos), desbalanceamento da carga de trabalho e execução de processos não planejados (Rotinas de backup mal planejadas por exemplo). Outro evento crítico muito comum são as quedas de energia prolongadas que podem vir a ocorrer devido a problemas com o fornecimento de energia ou eventos climáticos, gerando *downtime* da infraestrutura quando excede a capacidade dos geradores ou no-breaks.

Outro problema relacionado a energia são as oscilações que podem vir a avariar a entrada de força dos equipamentos, e desencadear outro evento, a falha do sistema de refrigeração que também pode ter origem no funcionamento

do sistema mecânico. Além disso, a Tabela 14 traz os eventos críticos relacionados aos recursos de TI, que podem vir a interromper a comunicação, ciber crime no caso de um ataque de DDOS por exemplo que pode vir a causar *downtime* do servidor e o mau funcionamento dos ativos de rede, hardware e operação dos serviços.

Quadro 14: Tabela de Eventos Críticos

Eventos críticos	**Origem**	**Consequência**
Alterações bruscas na carga de trabalho	Falha humana, balanceamento de carga e execuções de processos não planejados	Lentidão e travamento do equipamento
Quedas de energia prolongadas	Problemas na concessionária eventos climáticos	Downtime
Oscilações na energia	Mal funcionamento de geradores, no-breaks	Avariações de componentes
Falha no sistema de refrigeração	Falha mecânica ou no sistema de alimentação	Superaquecimento
Interrupções no link de internet	Problemas com provedor de internet	Falha de comunicação
Ciber crime/DDOS	Ataques malintencionados	Comprometimento de dados e informações
Falha no equipamento de TI	Má operação ou exposição a eventos críticos	Downtime
Falha nos ativos de rede	Má operação	Downtime
Falha Operacional	Acesso não autorizado	Downtime e avariações
Mal funcionamento de sistemas de gerenciamento	Má operação, downtime do servidor	não receber informações do sistema
Interferências do meio ambiente	Eventos climáticos	Downtime e avariações

Também foram levantados o mau funcionamento do próprio sistema de

monitoramento que pode vir a se tornar um evento crítico visto que sem ele não é possível detectar os problemas relacionados ao *datacenter*. E por fim a interferência do meio ambiente já que eventos climáticos extremos também podem causar *downtime* e avariações.

A Tabela 15 mostra os principais eventos críticos levantados,objetivando propor formas de fazer com que o *datacenter* saia do status crítico e volte ao status normal. No modelo de monitoramento e gerenciamento inteligente proposto no presente trabalho, esta normalização deve ser feita da maneira mais autonômica possível, desta forma a segunda coluna propõe formas de detecção autonômica (identificar e analisar e informar os problemas) e a terceira coluna propõe soluções que normalizarão a infraestrutura automaticamente.

Quadro 15: Tabela de normalização inteligente

Eventos críticos	**Detecção autônoma**	**Resolução autônoma**
Alterações bruscas na carga de trabalho	Monitorar/informar utilização dos recursos de TI	Balancear automaticamente a carga de trabalho
Quedas de energia prolongadas	Monitorar no-breaks e entradas de energia	Reduzir carga de trabalho e manter o sistema funcionando com baterias e gerado o maior tempo possível
Oscilações na energia	Monitorar entradas de energia	Desligar equipamento para evitar avariações
Falha no sistema de refrigeração	Monitoramento da temperatura ambiente ou equipamento	Controle remoto do sistema de refrigeração reduzir capacidade computacional
Interrupções no link de internet	Priorizar o sistema uptime do monitoramento	Link redundante
Ciber crime/DDOS	Monitoramento de serviços de rede	Identificar anomalias fechar portas/ ou desligar equipamento temporariamente

Falha no equipamento de TI	Monitorar todos os componentes e informar anomalias	Transferir carga de trabalho, evitar exposição frequente a eventos críticos
Falha nos ativos de rede	Adicionar redundância a ferramenta de monitoramento	Dedicar baterias/ gerador para os principais ativos de rede
Falha Operacional	Monitoramento de acessos	Gerenciamento de acessos
Mal funcionamento de sistemas de gerenciamento	Priorizar uptime do sistema de monitoramento	Espelhar sistema em nuvem
Interferências do meio ambiente		*Disaster recovery*

Com base nas tabelas 14 Levantamento de eventos críticos e n 15 normalização inteligente, foi elaborado o diagrama do modelo conceitual proposto neste trabalho, abordando e dividindo em categorias os principais elementos presentes nas infraestruturas de *datacenters*, são eles: segurança, energia, rede, climatização e servidores.

Estes elementos foram levantados tendo como base as normas ANSI TIA 942 instalação e classificação de *datacenters* e a ISO 27002 segurança da informação. Para cada um deles foram analisados os seguintes pontos, os eventos que podem ocorrer, o conjunto de itens que devem ser monitorados e como deve ser realizado gerenciamento antônomo dentro de cada categoria. Além disso cada um destes aspectos foi classificado de modo deixar claro o por que foi adicionado ao modelo conceitual.

A maior parte eventos requerem ações para correção e normalização da infraestrutura pois potencialmente irão gerar falhas e downtime de equipamentos. Estes foram classificados tendo em vista os seguintes fatores, tipo, status e categoria, que por sua vez são classificados da seguinte forma:

- Tipo interno (IN): quando o evento é originado por uma falha, erro ou mal

funcionamento ocorrido dentro do espaço físico do *datacenter* (como o travamento de um switch por exemplo que irá gerar um evento interno de falha na rede).

- Tipo externo (EX): quando o evento é originado por uma falha externa ao *datacenter* moa que afetam diretamente seu funcionamento (Rompimento de cabo de fibra ou quedas de energia prolongadas por exemplo).

- Status Informação (IF): quando o elemento monitorado funciona com margem de segurança, ou seja, apresenta estabilidade e carga de trabalho adequada a sua capacidade.

- Status Alerta (AL): quando o elemento monitorado começa a ficar sobrecarregado ou seu funcionamento apresentar anormalidades que podem vir a se tornar eventos críticos falhas e *downtime*.

- Status Crítico (CR): quando o mal funcionamento, falha, parada ou até avariação de um equipamento é iminente.

- Categoria Tier 1 (T1): quando o evento é relacionado aos requerimento exigidos na Tier 1 da ANSI TIA 942, ou seja, é requerido em infraestruturas básicas de *datacenters*.

- Categoria Tier 2 (T2): quando o evento é relacionado aos requerimento exigidos na Tier 2 da ANSI TIA 942, ou seja, é requerido em infraestruturas de *datacenter* com redundância básica.

- Categoria Tier 3 (T3): quando o evento é relacionado aos requerimento exigidos na Tier 3 da ANSI TIA 942, ou seja, em infraestruturas com alta redundância.

- Categoria Tier 4 (T4): quando o evento é relacionado aos requerimento exigidos na Tier 4 da ANSI TIA 942, ou seja, em infraestruturas a prova de falhas.

O modelo conceitual proposto neste trabalho classifica o monitoramento da infraestrutura de *smart datacenters* visando o nível de leituras e funcionalidade dis-

ponibilizadas para cada item monitorado como por exemplo, utilização, temperatura e saúde, e esta classificação é dividida da seguinte forma:

- Monitoramento básico (B): monitora as funções básicas do item, além de gerar gráficos e relatórios simples.

- Monitoramento intermediário (I): monitora a maior parte dos componentes do item selecionado, gera gráficos e relatórios elaborados.

- Monitoramento avançado (A): informações completas sobre o item monitorados, ou seja, monitorara todos os aspectos que podem ser trabalhados e gerenciados e mostra de forma otimizada as informações gerando gráficos relatórios e logs.

O gerenciamento foi classificado tendo em vista o quanto cada elemento da infraestrutura se aproxima da ideia de *smart datacenter* podendo executar ações de controle que otimizem os processos sem a necessidade de intervenção humana. Tendo em vista o aumento crescente em complexidade e proporção nos *datacenters* atuais, a execução de ações proativas e reativas autonomicamente é um dos pontos mais importantes em uma infraestrutura inteligente.

- Gerenciamento manual (M): quando feito através de uma ferramenta ou sistema de gerenciamento acessado e operado manualmente, para verificar status e executar ações no *datacenter*, sendo fundamental um operador para controle da infraestrutura.

- Gerenciamento semi-autônomo (SA): qnviar alertas informando os eventos que ocorridos ou que possam vir a ocorrer dentro da infraestrutura de um *datacenter*.

- Gerenciamento autônomo (AT): executa ações autonomicamente, isto é, sem a necessidade de intervenção humana.

3.6.1 Monitoramento e gerenciamento da Climatização para Smart Datacenter

Segundo Mukherjee e Banerjee et al. (2010) leva apenas alguns segundos para que equipamentos de TI de alto desempenho utilizados nos atuais *datacenters* ultrapassem a temperatura de *redline* definida por seus fabricantes, comprometendo os componentes sensíveis a superaquecimento e o *uptime* das máquinas. Portanto se faz necessário um sistema de climatização eficiente e que atenda todos os componentes funcionando em uma temperatura segura em tempo integral, apesar do custo operacional energético gerado.

Nas atuais infraestruturas de *datacenters* se faz necessário um sistema de climatização em tempo integral visto que os servidores possuem componentes altamente sensíveis a temperaturas elevadas, além do aumento nas proporções das infraestruturas de computacionais, no entanto seu custo operacional energético vem aumentando exponencialmente. A Figura 20 representa o diagrama do modelo conceitual que aborda o monitoramento e gerenciamento inteligente da climatização de um *smart datacenter*,que foi dividido em duas partes, são elas a temperatura do ambiente e dos equipamentos de TI, que por sua vez são divididas em eventos, monitoramento e gerenciamento.

A Temperatura do ambiente abordada no modelo conceitual diz respeito a manter a temperatura dentro do *datacenter* ideal para que os equipamentos em operação não ultrapassem a *redline* definida pelo fabricante. O motivo da inclusão deste elemento no modelo é que o seu gerenciamento inteligente pode trazer as seguintes melhorias: considerável redução no risco de superaquecimento, redução do custo operacional energético, detecção de pontos quentes e frios, alertas de *downtime* ou insuficiência do sistema de refrigeração, bem como garantir que a temperatura ambiente se mantenha adequada, ou seja, dentro dos limites estipulados em norma. A norma ASHRAE é uma das mais utilizadas para definir políticas de climatização de ambientes *datacenter*, estipula temperaturas entre 18 e 25 C devido ao aumento na tolerância dos atuais componentes de hardware.

O gerenciamento manual destes itens demanda muito tempo e dependendo do tamanho da infraestrutura torna-se inviável, portanto vem sendo reali-

zadas cada vez mais pesquisas sobre gerenciamento inteligente da temperatura dos ambientes *datacenters*, com objetivo de automatizar o controle reduzir o custo operacional energético e minimizar ao máximo o risco de superaquecimento. O modelo conceitual aborda os seguintes eventos para temperatura ambiente de *datacenters*:

1- Falha no sistema de climatização, que consiste na ocorrência de problemas, falhas mecânicas ou interrupção na alimentação do equipamento utilizado para manter a temperatura ambiente dentro da *redline* estipulada pela norma ASHRAE, que quando ultrapassada o superaquecimento dos equipamentos é eminente. Este evento foi classificado como ((IN) interno pois ocorre dentro do ambiente do *datacenter*, (CR) crítico pois resulta no superaquecimento de todos os equipamentos de TI de alto desempenho, (T2-4) e categoria onde a Tier mínima que o evento é abordado é a 2 de uma maneira básica e vai até a 4 com redundância o suficiente para alta redução da chance de ocorrência).

2- Insuficiência do sistema de climatização consiste não na interrupção do recurso mas na detecção de pontos de calor no ambiente mesmo com o equipamento utilizado para manter a temperatura dentro da *redline* estipulada na norma ASHRAE operando em capacidade máxima, este evento pode ocorrer devido a picos de calor em um ponto especifico, ou crescimento da infraestrutura acima do alcance do ar condicionado. Este evento foi classificado da seguinte forma ((IN) tem origem interna, (CR) status crítico visto que pode interromper o execução dos processos, a disponibilidade do serviço originar superaquecimento dos componentes e *downtime* dos recursos computacionais, (T2-4) e por fim a categoria onde a Tier mínima que o evento é abordado é a 2 de uma maneira básica e vai até a 4 com redundância o suficiente para alta redução da chance de interrupção devido a redundância e equipamentos de climatização mais avançados).

O monitoramento da temperatura do ambiente *datacenter* tem como principal objetivo coletar informações sobre o funcionamento da climatização e se a mesma está sendo suficiente para manter os equipamento operando dentro das suas *redlines*, desta forma podendo executar ações preventivas reativas ou corretivas com base nestes dados.

No modelo foram levantados os seguintes itens a serem monitorados: a temperatura do ambiente que esta relacionada ao evento 1 e classificado como (B) básico normalmente pode ser realizado através da leitura de sensores instalados no ambiente. Monitoramento de pontos de calor que está relacionado ao evento 2 e foi classificado como (A) Avançado, uma vez que detectar pontos de calor específicos dentro do ambiente seja algo mais complexo, que pode ser realizado através de uma rede de sensores de temperatura instalados na infraestrutura ou a utilização de câmeras térmicas para elaborar um mapa de calor e por fim a temperatura interna dos racks também relacionado ao evento 2 e classificado como (I) intermediário também normalmente feita através de sensores porém muito sensíveis a mudanças nas temperaturas dos equipamentos.

O gerenciamento da temperatura ambiente do *datacenter* tem como objetivo tratar ou até mesmo evitar eventos críticos através de ações executadas autonomicamente, preferencialmente sem a necessidade de intervenção humana. No modelo conceitual proposto foram levantadas as seguintes ações de controle:

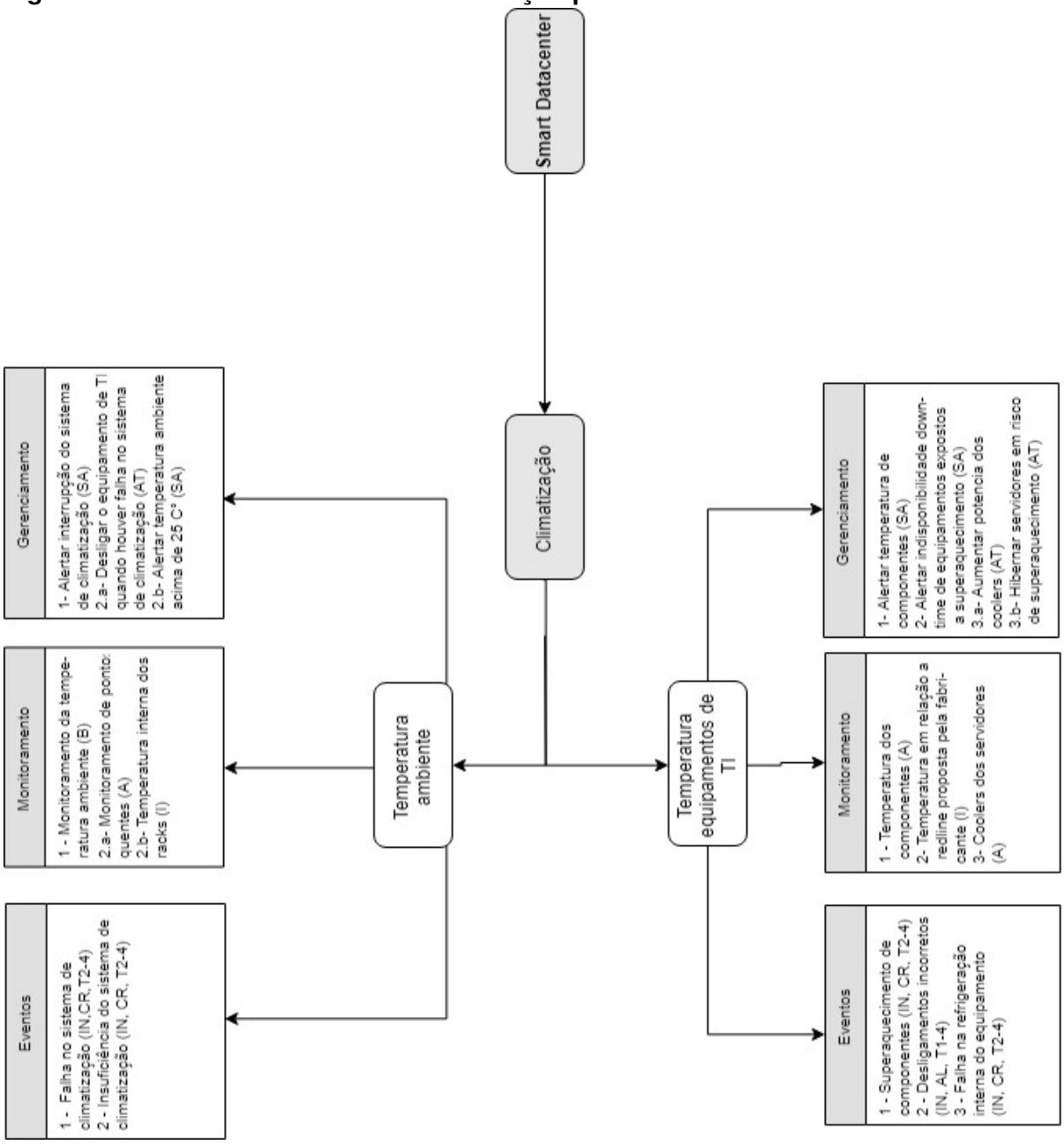
Alertar falha no sistema de climatização é uma ação direcionada ao evento 1 e classificada como semi-autônoma (SA), e tem por objetivo alertar os responsáveis pelo *datacenter*, paradas no equipamento responsável por climatizar o ambiente.

Hibernar equipamento de TI quando houver falha no sistema de climatização é uma medida de gerenciamento direcionada ao evento 2 ativada em cenários extremos apenas com objetivo de conter as consequências decorrentes do superaquecimento. Está ação foi classificada como (AT) autônoma, pois é executada automaticamente quando a temperatura do ambiente aumentar a ponto de gerar risco considerável a infraestrutura, ou seja, fique acima dos 25 C. O motivo da inclusão é que desligando os equipamentos preventivamente são evitadas consequências como desligamento incorreto, interrupção forçada e contenção de avariações de componentes.

Alertar temperatura ambiente acima de 25 C é uma ação direcionada ao evento 2 e classificado como (SA) Semi-autônomo, alerta os administradores do *datacenter* quando a temperatura ambiente ultrapassar bruscamente o limite es-

tipulado pela norma ASHRAE através deste alerta é possível executar uma ação antes da ocorrência de um evento crítico.

Figura 20: Modelo Conceitual de Climatização para Smart Datacenter.



A temperatura dos equipamentos de TI abordada no modelo conceitual proposto descreve os eventos, monitoramento e gerenciamento no nível de recursos computacionais, os quais possuem uma tolerância a temperaturas singular que varia de acordo com o fabricante. Este limite é chamado de *redline* e uma vez que o calor concentrado no equipamento ultrapasse-o, os resultados são interrupção

dos serviços, desligamentos forçados, mal funcionamento de *hardware*, e avariações em componentes. Os eventos levantados no modelo conceitual proposto para temperatura dos equipamentos de TI são:

1- Superaquecimento de componentes ocorre quando algum dos componentes que compões um elemento de computação ultrapasse a *redline* estabelecida pelo seu fabricante. Este evento foi classificado como ((IN) de origem interna pois os equipamentos ficam fisicamente alocados no *datacenter*, CR crítico pois tem potencial alto de gerar falhas, T2-4 onde a Tier mínima que o evento é abordado é a 2 que oferece contenção básica até a 4 que oferece redundância e contingência o suficiente para não ser afetada por esse evento).

2- Desligamentos incorretos, ocorre quando algum equipamento de TI é desligado em decorrência de superaquecimento que pode ser causado por exemplo por: sobrecarga do equipamento falha na sua refrigeração interna ou no equipamento de climatização do ambiente. Este evento foi classificado da seguinte forma ((IN) origem interna, (AL) status de alerta pois haverá interrupção de todos os serviços rodando naquela máquina (T1-4) a Tier mínima que o evento é abordado é a 1 infraestrutura básicas e vai até a 4 com redundância o suficiente evitar totalmente o evento).

3- Falha na refrigeração interna nos equipamento ocorre quando os coolers repensáveis por reduzir a temperatura interna dos recursos de TI reduzindo consideravelmente o tempo de aquecimento dos componentes. Este evento foi classificado da seguinte forma ((IN) O evento tem origem interna, (CR) status crítico pois além de interrupção gera prejuízo a organização, (T2-4) onde a Tier mínima que o evento é abordado é a 2 de uma maneira básica e vai até a 4 com redundância o suficiente para alta redução da chance de avariação).

O monitoramento da temperatura dos equipamentos de TI, tem como objetivo coletar informações sobre o temperatura de operação componentes dos equipamentos de TI, desta forma podendo detectar quando um servidor está sendo subutilizado apesentando uma temperatura muito baixa ou em risco de superaquecimento acima da *redline* do equipamento. No modelo conceitual proposto, foram levantados os seguintes itens a serem monitorados:

Monitoramento da temperatura dos componentes de TI sensíveis a superaquecimento, está relacionada a evento 1 e foi classificada como (A) avançada, pois é feito através de sensores internos existentes nos equipamentos de TI, e os dados coletados são utilizados para verificação de status e garantir a integridade do hardware e detectar superutilização do equipamento.

Monitoramento da temperatura em relação a *redline* proposta pela fabricante, deve ser feito individualmente devido a heterogeneidade de equipamento e a variação da *redline* dos mesmos, e esta relacionado ao evento 2 e foi classificado como (I) intermediário, pois é medido cruzando dados de todos os sensores de temperatura internos e geralmente acusa falhas de climatização.

Monitoramento dos collers realiza a leituras de status deste componente é a sua disponibilidade e potência, relacionada ao evento 3 e classificado como (Avançado) um vez que traz a leitura de dados referentes a um componente especifico de refrigeração responsável pela dissipação de calor interna dos equipamentos de TI.

O gerenciamento da temperatura dos equipamentos de TI em *smart datacenters* tem como principal objetivo evitar superaquecimento dos componentes e manter os equipamentos de TI trabalhando abaixo da *redline* estabelecida por seus fabricantes, além de conter as consequências decorrentes deste evento, preferencialmente com o mínimo de intervenção humana. No modelo conceitual proposto foram levantadas as seguintes ações:

Alertar temperatura dos componentes de equipamentos de TI consiste consistem em informar os administradores do *datacenter* quando um componente relacionado a recursos computacionais ultrapassa o limite seguro ou a temperatura limite da *redline* que varia dependendo do fabricante do equipamento, estes alertas são configurados para informar o problema ocorrido e agilizar a correção do evento. Esta ação está direcionada ao evento 1 e foi classifica como (SA) semi-autonômica pois informa o problema mas não o corrige sem intervenção.

Alertar indisponibilidade *downtime* de equipamentos expostos ao superaquecimento consiste em alertar os administradores do *datacenter* quando um equi-

pamento é deligado após algum de seus componentes ultrapassar a *redline* estabelecida por seu fabricante. Este evento foi direcionado ao evento 2 e classificado como (SA) semi-autonômico pois informa o responsável pela infraestrutura de TI quando a indisponibilidade de um equipamento é decorrente de um superaquecimento.

Aumentar a potência dos *coolers* dos equipamento de TI, consiste em gerenciar os componentes de refrigeração interna visto que o aumenta da sua potência pode reduzir ou manter a temperatura do hardware dos elementos de computação abaixo da *redline* definida por seus fabricantes, esta ação deve ser executada quando ocorrer um alerta de temperatura crítica, com alto potencial de desligamento do servidor. Esta ação está direcionada ao evento 3 e foi classificada como (AT) autonômico pois é proativa visando ipendir a ocorrência de um evento.

Hibernar servidores em risco de superaquecimento consiste em encerrar as processos executados em um equipamento e enviar um comando para que o mesmo entre em modo de hibernação, visto que desta forma sem carga de trabalho o hardware tende a resfriar, contendo consequências mais sérias como avariação do sistema devido a desligamentos incorretos ou hardware em consequência do aquecimento elevado dos componentes. É ativada quando recebe alertas de temperaturas críticas de acordo com o limite estipulado pelo fabricante ,ou seja, alto potencial de interrupção. Esta ação esta direcionada ao evento e 3 e foi classificada como (AT) autonômica visto que é disparada de maneira reativa a um evento.

3.6.2 Monitoramento e Gerenciamento de Redes para Smart Datacenters

As tecnologias de redes são um recurso de extrema importância nas infraestruturas de computação, visto que seu crescimento depende da flexibilidade da sua rede além de ser o recurso responsável pela comunicação interna e externa dos *datacenters*. A norma TIA 942 classifica redes de *datacenter* com base na sua disponibilidade e redundância de equipamentos, já que interrupção neste recurso representa *downtime* de todos os serviços disponibilizados pelos servidores.

Uma rede convencional de *datacenter* compreende os servidores que recebam as cargas de trabalho e respondem a solicitações de clientes; *switches* que

conectam dispositivos juntos, roteadores que executam funções de encaminhamento de pacotes, controladores que gerenciam o fluxo de trabalho entre dispositivos de rede, *gateways* que servem como junções entre as redes de data center e a Internet mais ampla e clientes que agem como consumidores da informação em pacotes de dados.

A Figura 21 representa o diagrama do modelo conceitual referente ao monitoramento e gerenciamento de redes para *smart datacenter*. Esta representação foi dividida em duas partes, são elas rede interna e externa pois são afetadas por eventos distintos que no caso do acesso externo a solução pode não estar nas mão do administrador da infraestrutura.

A rede interna aborda os recursos localizados no ambiente *datacenter*, ou seja, a gestão e redundância dos ativos de rede e a conexão local entre os equipamentos. Em uma infraestrutura inteligente, estes elementos tendem a oferecer um aumento na disponibilidade, o uso otimizado dos equipamentos além de disponibilizar alertas quando detectados eventos,como por exemplo, comunicação locais como falhas no cabeamento ou nas interfaces de rede dos servidores. Os eventos levantados no modelo para rede interna foram:

1- Mau funcionamento de interfaces de rede, ocorre quando determinada interface seja de um servidor ou ativo da rede apresenta lentidão ou perda de pacotes prejudicando a qualidade de serviço da infraestrutura. Este evento foi classificado como ((IN) interno pois tem origem dentro do ambiente *datacenter*, (AL) status de alerta já que não causa *downtime* mas sim perda em eficiência e qualidade de serviço, (T2-4) e categoria parte da Tier 2 redundância básica até a 4 onde existe chance mínima de ocorrência).

2- Falha de conexão interna, ocorre quando equipamentos de TI em uma mesma rede local LAN não se comunicam interferindo no funcionamento e provisionamento de serviços pode ser originado a partir de falha na interface de rede ou até no próprio equipamento, desta forma seu monitoramento e detecção é mais avançado. Este evento foi classificado da seguinte forma: ((IN) Interno pois tem origem dentro do ambiente *datacenter*, (CR) status crítico, visto que causa *downtime* além do monitoramento ser a nível de enlace e não físico então já que não

é possível conectar um cabo autonomicamente, (T2-4) Tier 2 até a 4, ou seja o aumento na redundância a interface afetada).

3- Falha de hardware nos ativos de rede, ocorre quado os equipamento utilizados para distribuição da rede sofrem interrupção devido a falha em seus componentes comprometendo a comunicação de toda a infraestrutura, alguns equipamentos de rede oferecem leitura de recursos como memória processamento e trafego cujo uma falha como travamento dispararia o evento. Este evento foi classificado como ((IN) Interno pois tem origem dentro do ambiente *datacenter*, ((CR) status crítico visto que causa *downtime* em uma série de interfaces de rede quando principalmente se tratando de switches ou roteadores, (T1-4) Tier 1 infraestrutura básica até a 4, com redundância o bastante para garantir o *uptime* de todos os servidores e serviços ligados a estes equipamentos).

4- *Downtime* dos equipamentos de rede ocorre quando os ativos de rede perdem a conexão, é disparado quando o mesmo para de responder ao protocolo ICMP, "ping"o qual foi classificado como ((CR) crítico visto que causa *downtime* em uma série de interfaces de rede quando tais equipamentos ficam indisponíveis devido a falta de energia, (T1-4) Tier 3 até a 4, ou seja o aumento na redundância energética exigida para garantir o *uptime* destes equipamentos).

O monitoramento da rede interna em smart datacenter tem como objetivo coletar principalmente dados sobre estes dois elementos, o funcionamento e a disponibilidade dos equipamentos de rede e interfaces de conexão tanto nos ativos quanto nos servidores. Visto que falha nestes recurso representa perda na qualidade do serviço ou *downtime* do *datacenter*. No modelo conceitual proposto no presente trabalho foram levantados os seguintes itens a serem monitorados:

Monitoramento da conexão entre os equipamentos do *datacenter*, que está relacionado ao evento 1 e foi classificado como (I) intermediário pois pode ser utilizado para detectar mau funcionamento e *downtime* de equipamentos. Disponibilidade de interfaces de rede também relacionado ao evento 1, e foi classificado como (I) tendo em vista que servidores e ativos de rede possuem mais de uma interface esse monitoramento tem objetivo de identificar se todas estão funcionando corretamente.

O monitoramento da conexão entre os ativos de rede consiste em verificar o envio de pacotes de um equipamento para outro, e desta forma constatando se a comunicação entre eles esta *up*, e está relacionado ao evento 1 e classificado como (I) intermediária já que esta leitura é realizada em mais de um *host* e informa quando um ou ambos não estão disponíveis, tem como objetivo informar quando a interface de rede responsável por essa conexão está funcional.

Monitoramento da disponibilidade das interfaces de rede consiste na leitura e coleta de dados a referente a cada uma dela, visto que nos servidores convencionais e nos principais ativos de rede possuem diversas, para fins de capacidade ou até mesmo redundância. Esta coleta está relacionada ao evento 2 e foi classificado como (I) intermediária devido a variedade de e heterogeneidade deste elemento em um *datacenter*, e tem como objetivo monitorar *uptime* e funcionamento de todas elas.

O monitoramento dos ativos de rede consiste na leitura constante dos status e da carga de trabalho dos elementos que compões o seu *hardware*, desta forma facilitando a detecção da causa de *downtime* ou baixa performance no desemprenho da rede ou dos recursos que dependam de um ativo em especifico. Esta coleta esta relacionada ao evento 3 e foi classificada como (A) avançado pois realiza a coleta das dados sobre todos os recursos do equipamento em questão.

O monitoramento do trafego da rede consiste na coleta da quantidade de dados trafegadas em cada um das interfaces de rede dos equipamentos internos do *datacenter* está relacionado ao evento 3 e foi classificado como (A) avançado tem como objetivo levantar dodos sobre o volume do trafego e capacidade dos equipamento de processa-los. Esta coleta de está relacionada ou evento 3 e foi classificada como (A) avançada pois é realizada em todas as interfaces de rede e os dados tem potencial de identificar a insuficiência dos equipamentos de rede.

O monitoramento da disponibilidade dos ativos de rede consiste em informar o *downtime* ou *uptime* dos principais equipamentos de rede do *datacenter*, tendo em vista as consequência geradas pela indisponibilidade dos mesmos, e que depende do nível de redundância da infraestrutura. Esta coleta esta relacionada ao evento 4 e foi classificada como (B) básica visto que se trata de uma requisição

feita com objetivo de verificar disponibilidade do recurso.

O gerenciamento inteligente da rede interna em um *smart datacenter* tem como objetivo alertar a ocorrência de eventos de forma preventiva de modo a evita-los garantindo o *uptime* e qualidade de serviço. Atualmente a grande maioria das ações de monitoramento e gerenciamento inteligente voltadas a infraestrutura de rede então limitados a alertar eventos, visto que o reparo de um ativo ou interface de rede sem intervenção humana ainda é inviável. Foram levantadas as seguintes ações de controle para este elemento:

Alertar mau funcionamento das interfaces consiste em informar aos administradores responsáveis pela infraestrutura quando ocorre perda de pacotes ou lentidão na transmissão ou recepção de dados direcionados a alguma interface de rede de algum equipamento que compõe o *datacenter*. Esta ação está direcionada ao evento 1 e foi classificada como (SA) semi-autônoma, já que informa quando uma interface estiver indisponível ou apresentando mau funcionamento que ocasione perda de velocidade ou pacotes, mas não corrige o problema gerado pelo evento.

Alertar falha de conexão entre equipamentos consiste em informar aos administradores responsáveis pela infraestrutura a ocorrência de falha de comunicação entre equipamentos que compõe os recursos computacionais do *datacenter*. Esta ação foi direcionada ao evento 2 e classificada como (SA) semi-autonômica, tem como objetivo alertar os administradores da infraestrutura quando um equipamento de rede como *switches* ou roteadores por exemplo estiverem indisponíveis, considerando que deva haver redundância no serviço responsável por enviar os alertas.

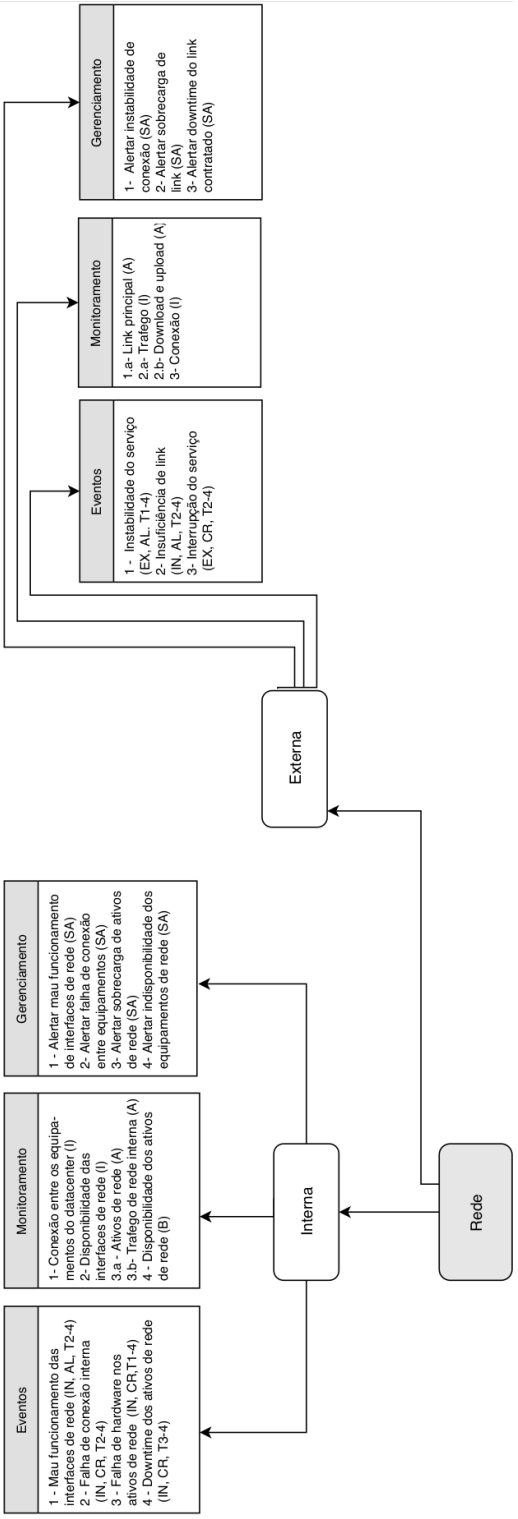
Alertar sobrecarga de ativos de rede consiste em informar aos administradores responsáveis pela infraestrutura quando algum equipamento de rede operando no limite em um período de tempo mais longo de tempo, uma vez que um equipamento operando muito perto da capacidade máxima por várias horas tem um potencial muito maior de sofrer interrupção, deste modo esta ação não é disparada simplesmente quando ocorrerem picos. Esta ação foi direcionada ao evento 3 e foi classificada como (SA) semi-autonômica pois informa a ocorrência do evento

mas não é uma ação corretiva.

Alertar indisponibilidade dos equipamentos de rede consiste em informar aos administradores da infraestrutura quando um dos ativos utilizados para distribuição da rede interna no *datacenter* estiver indisponível visto que a ocorrência deste evento tem potencial de causar *downtime* em uma série de equipamentos e serviços. Esta ação foi direcionada ao evento 4 e classificada como (SA) semi-autonômica já que informa a ocorrência do evento mas não se trata de uma ação corretiva.

O monitoramento e gerenciamento de redes externas abordado no modelo conceitual proposto no presente trabalho, tem como objetivo informar a ocorrência de eventos que afetam a comunicação do *datacenter* com a internet, que se faz necessária em todas as infraestruturas atuais, o que justifica a importância do monitoramento deste elemento. Se tratando de um recurso terceirizado oferecido por provedores, o gerenciamento do mesmo consiste em disparar alertas quando ocorrem eventos com potencial de gerar interrupção, já que eles são tratados e solucionados com o aumento da redundância e não através de ações inteligentes: Os eventos levantados para esta parte do modelo foram os seguintes:

Figura 21: Modelo Conceitual de Redes paras Samart Datacenter.



1- Instabilidade do serviço, ocorre quando a conexão contratada de um provedor apresenta instabilidade, ou seja, lentidão e perda de pacotes impactando diretamente no desempenho dos serviços que utilizam de conexão externa. Este evento foi classificado como ((EX) tem origem externa pois a instabilidade do ser-

viço é causada por problemas de rota ou no equipamento do provedor, (AL) foi definido status de alerta visto que interfere diretamente do desempenho e qualidade de alguns serviços mas não causa interrupção total na comunicação, (T2-4) a categoria parte da Tier 2 até a 4 que segundo a norma ANSI TIA 942 requerem link de internet redundante).

2- Insuficiência do link ocorre quando os picos ou utilização do pacote contratado do provedor são constantes e interferem diretamente na qualidade de serviços providos pelo *datacenter* e que utilizam de rede externa podendo afetar acordos de SLA. Este evento foi classificado como ((IN) tem origem interna uma vez que é gerado da falha em provisionamento ou de um planejamento de expansão equivocado tornando o link contratado insuficiente, (AL) status de alerta visto que não causa interrupção total no processos e pode ser resolvido com melhorias de provisionamento e estruturação da rede, (T2-4) a categoria parte da Tier 2 até a 4 que segundo a norma ANSI TIA 942 exige redundância e provisionamento adequando).

3- Interrupção do serviço ocorre no caso de indisponibilidade do link contratado que afeta toda a comunicação externa do *datacenter* afetando todos os serviços que utilizam deste recurso para serem executados e providos a usuários, além disso em uma infraestrutura acime de básica requer um link de internet redundante e contenção energética para equipamentos receptores do serviço. Este evento foi classificado como ((EX) tem origem externa pois a interrupção do serviço é causada por problemas de rota ou no equipamento do provedor, (CR) foi definido status de crítico visto que interfere diretamente do desempenho e a execução de serviços além de causar interrupção total na comunicação, (T2-4) a categoria parte da Tier 2 até a 4 que segundo a norma ANSI TIA 942 requerem link de internet redundante).

O monitoramento e gerenciamento de redes externas abordado no modelo conceitual proposto no presente trabalho, tem como objetivo informar a ocorrência de eventos que afetam a comunicação do *datacenter* com a internet, que se faz necessária em todas as infraestruturas atuais, o que justifica a importância do monitoramento deste elemento. Se tratando de um recurso terceirizado oferecido

por provedores, o gerenciamento do mesmo consiste em disparar alertas quando ocorrem eventos com potencial de gerar interrupção, já que eles são tratados e solucionados com o aumento da redundância e não através de ações inteligentes: Os eventos levantados para esta parte do modelo foram os seguintes:

1- Instabilidade do serviço, ocorre quando a conexão contratada de um provedor apresenta instabilidade, ou seja, lentidão e perda de pacotes impactando diretamente no desempenho dos serviços que utilizam de conexão externa. Este evento foi classificado como ((EX) tem origem externa pois a instabilidade do serviço é causada por problemas de rota ou no equipamento do provedor, (AL) foi definido status de alerta visto que interfere diretamente do desempenho e qualidade de alguns serviços mas não causa interrupção total na comunicação, (T2-4) a categoria parte da Tier 2 até a 4 que segundo a norma ANSI TIA 942 requerem link de internet redundante).

2- Insuficiência do link ocorre quando os picos ou utilização do pacote contratado do provedor são constantes e interferem diretamente na qualidade de serviços providos pelo *datacenter* e que utilizam de rede externa podendo afetar acordos de SLA. Este evento foi classificado como ((IN) tem origem interna uma vez que é gerado da falha em provisionamento ou de um planejamento de expansão equivocado tornando o link contratado insuficiente, (AL) status de alerta visto que não causa interrupção total no processos e pode ser resolvido com melhorias de provisionamento e estruturação da rede, (T2-4) a categoria parte da Tier 2 até a 4 que segundo a norma ANSI TIA 942 exige redundância e provisionamento adequando).

3- Interrupção do serviço ocorre no caso de indisponibilidade do link contratado que afeta toda a comunicação externa do *datacenter* afetando todos os serviços que utilizam deste recurso para serem executados e providos a usuários, além disso em uma infraestrutura acime de básica requer um link de internet redundante e contenção energética para equipamentos receptores do serviço. Este evento foi classificado como ((EX) tem origem externa pois a interrupção do serviço é causada por problemas de rota ou no equipamento do provedor, (CR) foi definido status de crítico visto que interfere diretamente do desempenho e a execução de

serviços além de causar interrupção total na comunicação, (T2-4) a categoria parte da Tier 2 até a 4 que segundo a norma ANSI TIA 942 requerem link de internet redundante).

O monitoramento da rede externo no modelo conceitual para *smart datacenter* proposto neste trabalho tem o objetivo de realizar uma coleta de dados referente a transmissão e recepção de dados para a internet, bem como a estabilidade e a capacidade do serviço contratado de atender os processos da infraestrutura. Foram levantados os seguintes elementos a serem monitorados:

O monitoramento do link principal consistem na leitura dos dados referente a transmissão e recepção do link contratado e identificar a disponibilidade e estabilidade do mesmo. Esta coleta está relacionada ao evento 1 e foi classificada como (A) avançada pois a leitura destes dados pode identificar o motivo de uma série problemas através de testes de conexão com a internet ou com o provedor,a falha neste elemento e se trata de um serviço terceirizado.

O monitoramento do trafego de rede consistem na coleta de dados referentes ao trafego de rede para a internet afim de identifica insuficiência, sobrecarga e instabilidade do link contratado. Esta coleta está relacionada ao evento 2 e foi classificada como (I) intermediária que é realizada a partir de testes de conexão para leitura do trafego e detectar a funcionalidade do recurso.

O monitoramento do *download* e *upload* consiste na coleta de dados referentes ao usos destes recursos com objetivo de detectar a velocidade contratada é suficiente para atender os processos que são executados no *datacenter*. Esta coleta esta relacionada ao evento 2 e foi classificada como (A) avançada uma vez picos na utilização do serviço não necessariamente significa interrupção ou insuficiência, tornando a analise mais complexa.

Monitoramento da conexão com a internet consiste na coleta de dados referentes a disponibilidade da conexão a internet disponível no *datacenter* independente do nível de redundância adotado na infraestrutura, visto que a origem do evento pode variar. Esta coleta esta relacionada ao evento 3 e foi classificada como (I) intermediária e pode ser realizada testando constantemente a conexão com a

internet e os elemento internos que a afetam.

O gerenciamento inteligente de rede externa abordado no modelo conceitual proposto consiste em alertar a ocorrência de eventos que em sua maioria tem origem externa já que este os eventos ocorridos neste elemento são adquiridos de um provedor. Foram levantadas as seguintes ações de gerenciamento para este elemento:

Alertar a instabilidade da conexão consiste em informar aos administradores responsáveis pela infraestrutura quando ocorre mau funcionamento e perda de pacotes direcionados a internet de modo a evitar a indisponibilidade do serviço. Esta ação esta direcionada ao evento 1 e foi classificada como (SA) semi-autonômica visto que sua execução não corrige o evento apenas informa a ocorrência eminente da mesma através da ferramenta de monitoramento e gerenciamento adotada.

Alertar sobrecarga de link consiste em informar aos administradores responsáveis pela infraestrutura quando o download ou *upload* contratados estão funcionando em capacidade máxima sem interrupção acima de 5 minutos para ter certeza que não se trata de um pico. Esta ação está direcionada ao evento 2 e foi classificada como (SA) semi-autonômica uma vez que sua execução alerta a ocorrência eminente de um problema através da ferramenta de monitoramento utilizada no *datacenter*.

Alertar *downtime* do link contratado consiste em informar aos administradores da infraestrutura quando este serviço estiver indisponível tendo em vista as consequências decorrentes desta fala de comunicação. Esta ação esta direcionada ao evento 3 e foi classificada como (SA) semi-autonômica uma vez que quando executada alerta a ocorrência eminente do evento mas não é utilizada corretivamente.

3.6.3 Monitoramento e Gerenciamento de Servidores para Smart Datacenters

Os *datacenters* foram desenvolvidos e continuam em constante evolução com o objetivo de oferecer um ambiente que suporte a concentração e alocação de

recursos computacionais em grande escala e de importância crítica para suas organizações. Os servidores são os computadores utilizados para prover tais serviços e são equipamentos que possuem requisitos específicos para possam funcionar corretamente, como climatização (devido a hardware sensível a superaquecimento) e energia estável (por serem requisitados para alta disponibilidade), para garantir o maior *uptime* possível.

O gerenciamento da infraestrutura de TI de um *datacenter* tem se tornado cada vez mais complexo devido a cargas de trabalhos cada vez maiores de processamento e armazenamento além de manter a disponibilidade de uma série de componentes vitais para o *uptime* dos recursos computacionais, (como processadores, memória RAM ou Disco rígido por exemplo), cujo o mau funcionamento pode vir comprometer a qualidade dos serviços providos. Embora os servidores convencionais possuam redundância para a maioria dos seus componentes, quando ocorrem avarias em algum deles continuar e isso não afete o *uptime*, o equipamento não estará em capacidade total e talvez não suporte um próximo evento.

A Figura 22 representa o diagrama do modelo conceitual referente ao monitoramento e gerenciamento de computação em um *smart datacenter*. Esta imagem ilustra a abordagem do modelo proposto, para com a infraestrutura de TI que foi dividida em armazenamento, memória e processamento, ou seja, o poder computacional da infraestrutura.

O armazenamento é um dos recursos mais importantes que compõe um *datacenter*, sendo que muitos deles são voltados unicamente para este fim, além disso o *hardware* utilizado para manter os dados e informações na infraestrutura requer monitoramento constante redundância e gerenciamento adequando para que não haja desperdício de recursos. Foram levantados os seguintes eventos para o modelo referente armazenamento:

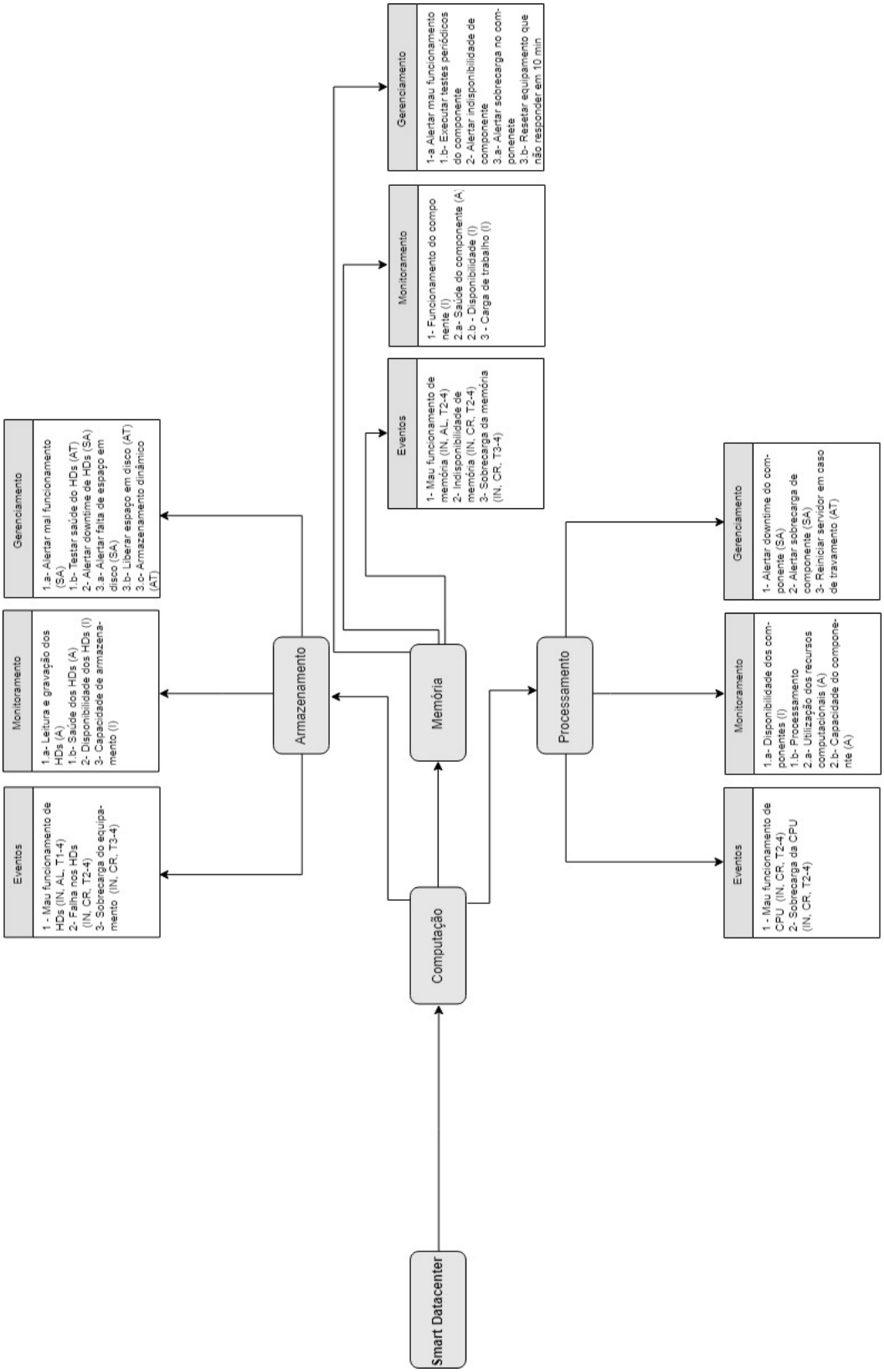
1- O mau funcionamento de HDs ocorre quando um ou mais discos rígidos utilizados para armazenamento apresentam algum tipo de defeito que prejudique sua performance, ou seja, leitura e gravação de dados, o que prejudica diretamente a qualidade de serviço e a vida útil do componente. Este evento foi classificado da seguinte forma ((IN), tem origem interna pois pois os equipamentos utilizados

para armazenamento fazem parte do ambiente (AL) foi definido status de alerta já que não representa *downtime* imediato do componente e a grande maioria dos servidores possuem mais de um disco, (T1-4) a categoria parte de T1 infraestrutura básica até a 4 onde existe alta redundância e disponibilidade).

2- Falha nos HDs ocorre quando este componente fica indisponível para leitura e escrita devido a mal funcionamento, falha de conexão, defeito ou avaria-ção. Este evento foi classificado da seguinte forma ((IN), tem origem interna pois pois os equipamentos utilizados para armazenamento fazem parte do ambiente (CR) foi definido o status crítico já que representa perda de capacidade, e ema alguns casos indisponibilidade de serviços e informações (T1-4) a categoria parte de T1 infraestrutura básica até a 4 onde existe alta redundância e disponibilidade).

3- Sobrecarga do equipamento ocorre quando os componentes de arma-zenamento disponíveis na infraestrutura tem de atender uma demanda maior que sua capacidade, geralmente sobrecarga deste recurso gera perda na qualidade de serviço. Este evento foi classificado da seguinte forma ((IN), tem origem interna pois pois os equipamentos utilizados para armazenamento fazem parte do ambi-ente (AL) foi definido status de alerta já que não representa *downtime* imediato do componente e a grande maioria dos servidores possuem mais de um disco, (T1-4) a categoria parte de T1 infraestrutura básica até a 4 onde existe alta redundância e disponibilidade).

Figura 22: Modelo Conceitual de Servidores para Smart Datacenter.



3.6.4 Monitoramento e gerenciamento de energia para smart datacenters

O tempo de *uptime* de um *datacenter* está diretamente relacionado ao seu abastecimento energético tendo em vista que todos os principais elementos da infraestrutura requerem um fonte constante de energia. No entanto este é um recurso terceirizado o que torna uma tarefa difícil gerenciar todos os aspectos e ter controle total do mesmo.

De acordo com Qu e Li et al. (2013) consumo de energia é uma preocupação crítica nos atuais *smart datacenters*, uma vez que uma seu consumo vem aumentando de forma crítica a cada ano tornando o custo operacional energético um fator preocupante, sendo em grande parte utilizada pelo sistema de climatização em tempo integral.

Portanto, o objetivo do gerenciamento inteligente energético para *Smart datacenters* tem como principal objetivo a otimização do recurso para redução do seu custo operacional que vem aumentando constantemente. E a gestão dos dispositivos de contenção como baterias, no-breaks e geradores por exemplo.

A Figura 23 representa o modelo conceitual de monitoramento de gerenciamento de energia para *smart datacenters*, o qual foi dividido em provisionamento de energia que consiste gerenciamento da alimentação energética dos equipamentos e TI e equipamentos de contenção que consiste no gerenciamento dos equipamentos responsáveis por conter a interrupção do recurso. Os eventos levantados para provisionamento energético são:

1- Oscilação de corrente elétrica ocorre quando os equipamentos eletrônicos do *datacenter* passam a receber energia em níveis reduzidos em relação a quantidade requerida pelos componentes, devido a problemas na distribuição do serviço, o que pode prejudicar a integridade de componentes eletrônicos e afetar a disponibilidade de equipamentos e serviços. Este evento foi classificado como ((EX) pois é originado de falha ou sobrecarga na concessionária de energia, (CR) definido status crítico visto que a exposição tem potencial de gerar prejuízos e interrupção na entrega de serviços, (T2-4) a categoria parte da Tier 2 com contenção e redundância básica até a 4 com infraestrutura que previne a ocorrência do evento).

2- Falha na fonte de energia ocorre quando há mal funcionamento nas fontes de alimentação dos servidores e equipamentos de TI, comprometendo a disponibilidade no caso da ausência de redundância, além disso o desligamento forçado de servidores pode causar avariações do sistemas operacionais utilizados no *datacenter*. Este evento foi classificado da seguinte forma ((IN) tem origem dento do ambiente *datacenter*, (CR) status crítico visto que pode interromper os serviços e ainda causar avarias, (T2-4) a categoria parte da Tier 2 com contenção e redundância básica até a 4 com infraestrutura que previne a ocorrência do evento.

3- Desligamento incorreto ocorre quando um servidor em funcionamento é deligado bruscamente em consequência de falhas na distribuição de energia, fonte de alimentação ou ainda mau gerenciamento dos equipamentos de contenção de surtos, a ocorrência deste evento tem potencial de avariação de sistemas ou componentes que são projetadas para trabalhar com estabilidade. Este evento foi classificado como ((IN), tem origem interna pois afeta os servidores alocados no ambiente *datacenter* (CR) status crítico visto que se redundância e contenção adequada pode interroper o funcionamento de um série de processos, (T2-4) a categoria parte da Tier 2 contenção e redundância básica até a 4 que representa infraestrutura a prova deste evento).

O monitoramento de provisionamento energético no modelo conceitual proposto neste trabalho tem como principal objetivo a leitura e coleta dos dados referentes a entrada de energia e disponibilidade da mesma para os equipamentos do *Smart datacenter*. Os item levantados para serem monitorados são:

- O monitoramento da entrada de energia em servidores consiste na leitura e coleta de dados referentes a energia recebida pelos equipamentos afim de verificar se o valor é ou não suficiente, e ainda se equipamento a esta recebendo. Esta coleta está direcionada ao evento 1 e foi classificada como (A) avançada tendo em vista a quantidade de equipamentos que devam ser verificados.

- O monitoramento do status das fontes de alimentação consiste na leitura de dados referentes as condições das fontes de alimentação energética dos ser-

vidores de modo a evitar riscos relacionados a falhas nas mesmas. Esta coleta está relacionada ao evento 2 e foi classificada como (A) avançada, devido a quantidade e heterogeneidade destes equipamentos nas infraestrutura de TI atuais.

- O monitoramento do *uptime* das fontes de alimentação consiste em identificar quando um destes equipamentos não está mais respondendo de modo a constatar se o evento causou desligamento do servidor ou se o mesmo encontra-se ligado apenas a uma das fontes no caso da máquina possuir redundância para este componente. Esta coleta esta relacionada ao evento 3 e foi classificada como (B) uma vez que consiste apenas na verificação de *uptime* da fonte.

O gerenciamento inteligente do provisionamento de energia para os equipamentos de TI no modelo conceitual proposto no presente trabalho tem como objetivo identificar, alertar e reagir a ocorrência de eventos relacionados a distribuição de energia que tenham potencial em causar avariações nos equipamentos e sistemas e causar do *downtime* prolongado de equipamentos. As ações de gerenciamento levantadas foram as seguintes:

Alertar anormalidades na corrente elétrica consistem em informar aos administradores responsáveis pela infraestrutura quando os níveis de energia recebidos pelos equipamentos eletrônicos estão acima ou abaixo do recomendável, de modo a auxiliar na prevenção das consciências geradas pelo evento. Esta ação está direcionada ao evento 1 foi classificada como (SA) semi-autonômica visto que quando executada informa a ocorrência do evento através da ferramenta de monitoramento instalada no *datacenter* além de não se tratar de uma ação corretiva.

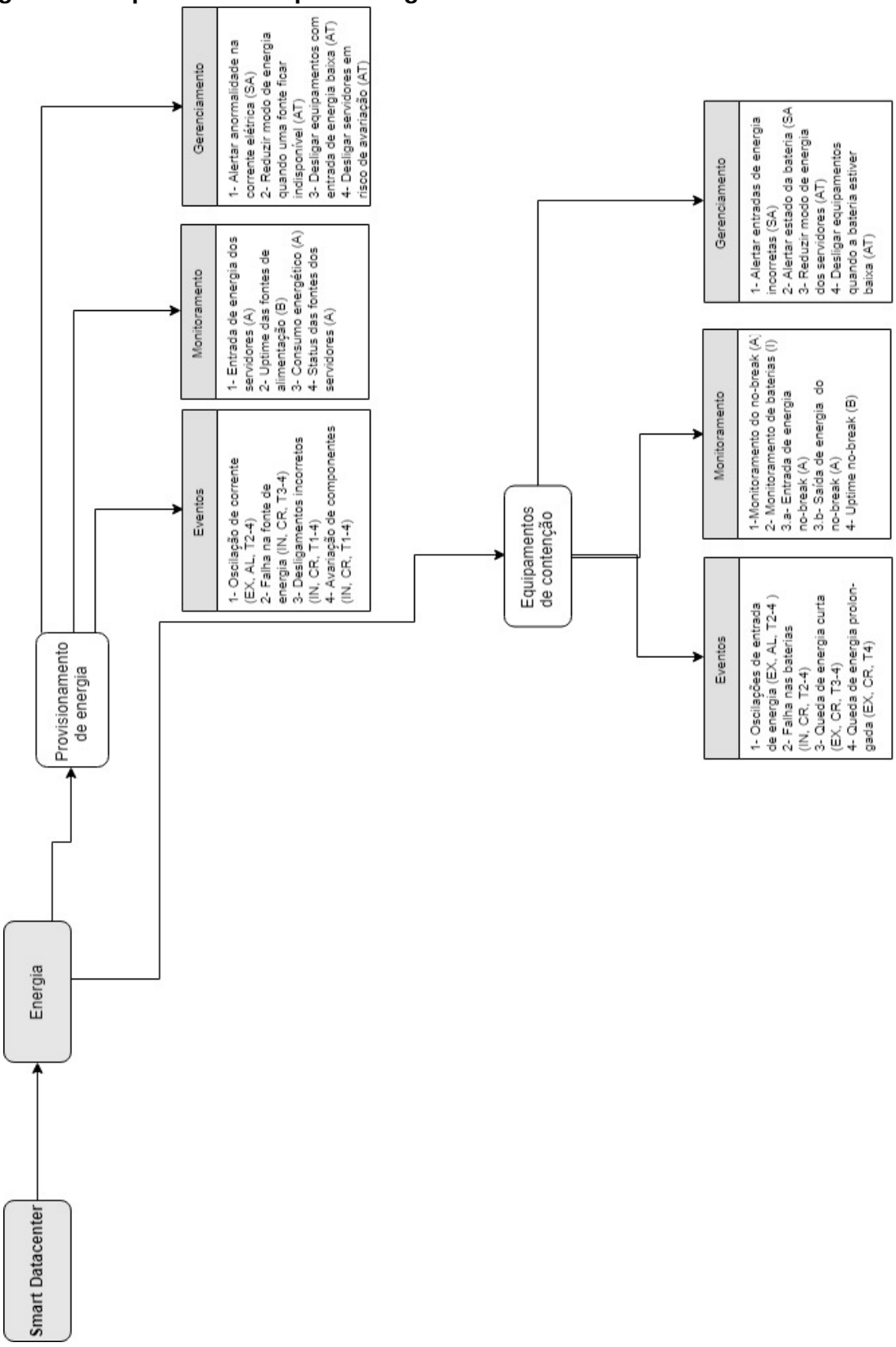
Reduzir o modo de energia dos servidores em caso dos equipamentos de TI é consiste em reagir a falhas decorrentes a entrada de energia e a *uptime* de alguma fonte de alimentação energética de um servidor reduzindo o modo de energia do equipamento para econômico reduz a quantidade de energia exigida tornando o sistema mais suportável a fonte única ou a redução nos níveis de energia recebidos. Esta ação está direcionada ao evento 2 mas também pode ser ativada no

evento 2 e foi classificada como (AT) autonômica visto que é executada reativamente para conter a ocorrência de um evento crítico.

Hibernar equipamentos com baixa entrada de energia consiste em enviar remotamente um comando para hibernar um servidor que estiver com baixa entrada de energia quando os níveis estiverem baixos a ponto da interrupção ser eminente. Esta ação está direcionada ao evento 3 e foi classificada como (AT) autonômica, já que é executada proativamente com objetivo de evitar desligamentos forçados e as consequências que vem com a ocorrência deste evento.

Desligar servidores em risco de avariação consiste em desligar servidores em risco eminente de desligamento forçado, isto é, quando os níveis de energia estiverem muito baixos, quando uma fonte de alimentação estiver apresentando mau funcionamento. Esta ação está direcionada ao evento 3 e foi classificada como (AT) autonômica pois é executada preventivamente de modo a conter e evitar avariações, e é ativada apenas em casos extremos.

Figura 23: Mapa Conceitual para Energia Samart Datacenter.



O monitoramento e gerenciamento inteligente para os equipamentos de contenção energética abordado no modelo conceitual proposto tem como objetivo

o melhor aproveitamento possível deste elemento, aumentando a duração do *uptime* dos principais serviços em caso de quedas de energia além da redução do consumo energético. Os eventos levantados para este elemento foram os seguintes:

1- Falha nas baterias ocorre quando alguma bateria de contenção energética utilizada no *datacenter*, apresentar falhas como indisponibilidade ou descarga rápida em uma ou mais unidades comprometendo a contenção de uma queda de energia. Este evento foi classificado como ((IN) tem origem interna já que as baterias fazem parte da infraestrutura mesmo sendo recomendado a alocação das mesmas em um sala separada, (CR) foi definido status critico pois se trata de um recurso de contenção, e quando ocorre falha toda queda ou oscilação de energia representa *downtime*, (T2-4) a categoria parte da Tier 2 onde a redundância do equipamento é básica até a 4 onde a infraestrutura está imune a esse tipo de evento).

2- Queda de energia curta ocorre quando há interrupção do recebimento de energia por devido a algum evento externo, no entanto com tempo de furação inferior a capacidade de autonomia obtida pelo uso das baterias, ou seja, uma queda que pode ser contida pelo no-break ou equipamento de contenção utilizado. Este evento foi classificado da seguinte forma((EX) tem origem externa pois sua ocorrência vem da falha no serviço contratado de uma concessionaria de energia ,(CR) tem status crítico pois raramente se sabe o tempo de duração deste evento e em caso de avançar para o evento 3 o *downtime* do *datacenter* é eminente, (T2-4) a categoria parte da Tier 2 com redundância básica e vai até a 4 onde há alta redundância e um tempo de autonomia maior)

3.6.5 Monitoramento e Gerenciamento de Segurança para Smart Datacenters

Os *datacenters* são ambientes de importância crítica normalmente com vasto armazenamento e trafego de dados muito sensíveis, além disso a maioria destas infraestruturas o *downtime* de serviços representa prejuízo para a organização. Deste modo manter a integridade, confidencialidade e privacidade no

ambiente tanto físico quanto computacional.

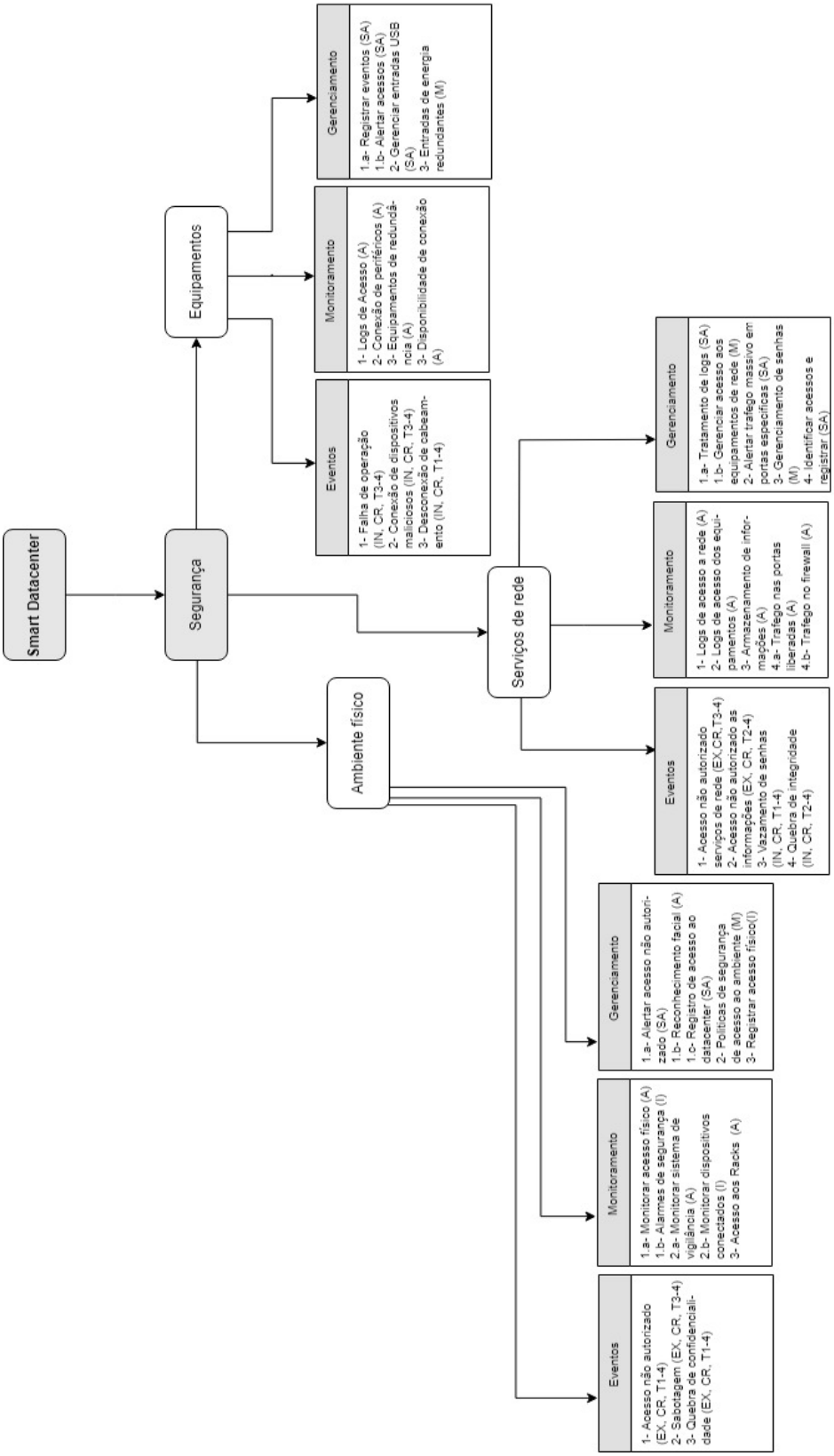
Quanto maior a categoria e a utilização de um *datacenter* mais complexo é o gerenciamento da sua segurança. A Figura 24 representa o diagrama de eventos levantados, quais elementos devam ser monitorados e quais ações devem ser implantadas e executadas sobre alguma condição. O diagrama foi dividido em ambiente físico, equipamentos e serviços de infraestrutura.

O monitoramento e gerenciamento de segurança do acesso físico em um *datacenter* se faz necessário segundo a norma de segurança da informação (ISO, 2013), e consiste em gerenciar a entrada de pessoas no ambiente computacional. Este tipo de controle é utilizado para evitar uma série de eventos, com má operação, sabotagem e até mesmo roubos ou furtos. Normalmente infraestruturas de grande porte contam com um sistema de vigilância (câmeras de segurança) para o monitoramento do acesso físico ao *datacenter*.

Em um *Smart datacenter*, uma função básica é o monitoramento e gerenciamento autonômico deste sistema de vigilância, tratando os dados coletados pelos dispositivos de segurança alertando e se possível reagindo a ameças. Foram levantados os seguintes eventos para segurança de acesso físico:

1- Acesso não autorizado ocorre quando indivíduos não autorizados tem acessam fisicamente a infraestrutura podendo interferir no funcionamento dos equipamentos de forma acidental ou intencional. Este evento foi classificado da seguinte forma((EX) tem origem externa pois sua ocorrência vem da falha no serviço contratado de uma concessionaria de energia ,(CR) tem status crítico pois acesso não autorizado representa um vulnerabilidade, (T2-4) a categoria parte da Tier 2 com redundância básica e vai até a 4 onde há alta redundância e um tempo de autonomia maior)

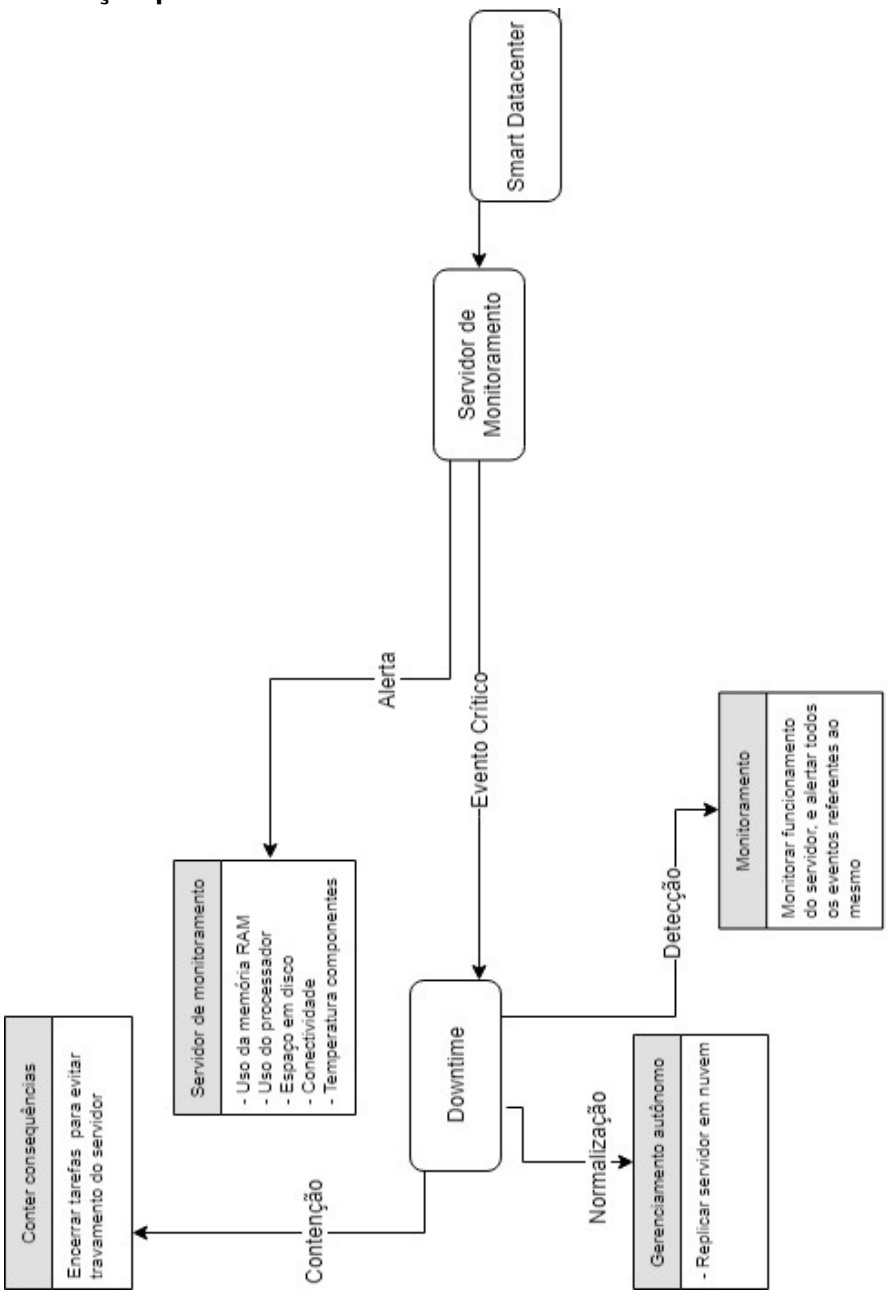
Figura 24: Mapa Conceitual para Segurança Smart Datacenter.



3.7 VALIDAÇÃO PARCIAL DO MODELO PROPOSTO

Para realizar a validação parcial do modelo e testar as melhorias vindas através da implantação do modelo conceitual proposto foi desenvolvido um diagrama conforme ilustrado na Figura 25 para ilustrar planejamento do serviço de monitoramento, isto é, ferramenta/servidor utilizados para este processo visando obter alta disponibilidade para os mesmos.

Figura 25: Alocação para de Servidor de Monitoramento.



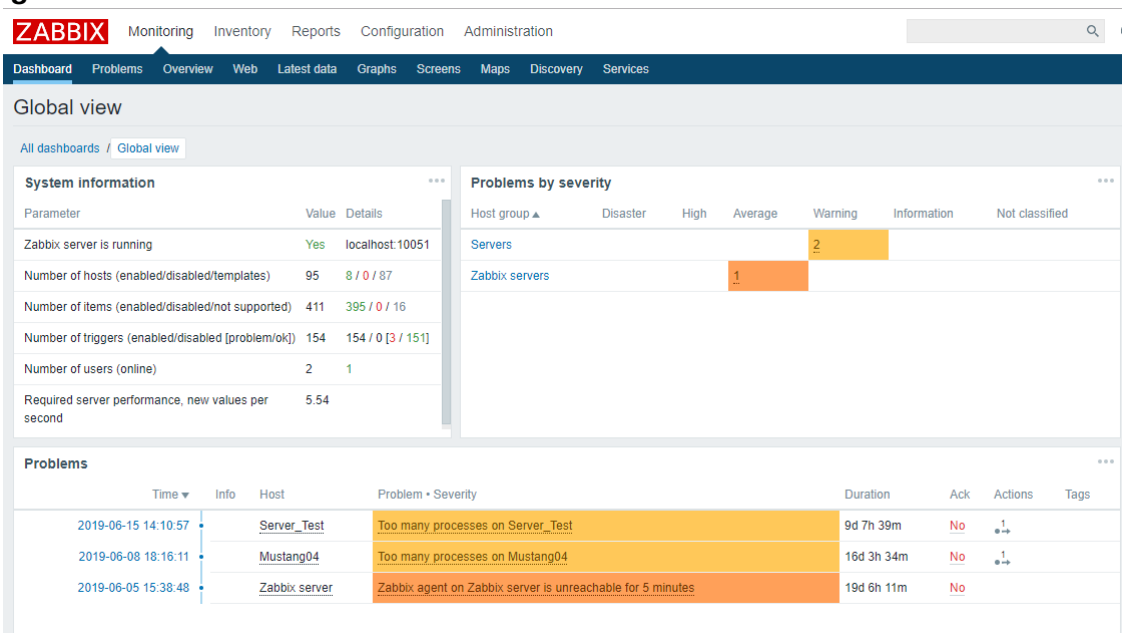
O principal problema gerado pelo mal funcionamento deste sistema é o

não recebimento das informações coletadas e eventos que possam vir a ocorrer no *datacenter*. Embora um servidor de monitoramento local seja funcional, ele esta suscetível a todos os eventos críticos que venham ocorrer na infraestrutura ou o mau funcionamento de algum componente do *hardware* do servidor.

Sem acesso às informações enviadas pelo servidor de monitoramento, um evento crítico como pode vir a desencadear um desastre maior. No modelo de monitoramento inteligente onde são elaboradas ações de gerenciamento para normalizar a infraestrutura, o equipamento destinado a esta função tem uma importância ainda maior portanto se faz necessário priorizar o *uptime* deste equipamento.

Para testar o modelo conceitual proposto no ambiente computacional do LARCC, optou-se pela ferramenta de monitoramento e gerenciamento *open source* Zabbix (DOCUMENTATION, 2008) que atualmente se encontra na sua versão 4.2. De acordo com a documentação da ferramenta, o Zabbix é um software que monitora vários parâmetros de uma rede e a integridade dos servidores.

Figura 26: Dashboard Zabbix LARCC.



Além de utilizar um mecanismo de notificação flexível que permite aos usuários configurar alertas para praticamente qualquer evento, ação que permite uma reação rápida aos problemas do servidor. O Zabbix oferece excelentes recursos de relatório e visualização de dados a figura mostra o *Dashboard* (painel de visualização) inicial da ferramenta que ilustra leituras e eventos recente coletadas

através do monitoramento.

No entanto o principal motivo da escolha desta ferramenta se deve aos recursos de ações e comandos remotos que integram a mesma. Deste modo o Zabbix pode ser utilizado para o monitoramento proativo e reativo, recursos que diferem um ambiente *Smart Datacenter* de uma infraestrutura com monitoramento estático.

3.7.1 Modelo de Monitoramento e Gerenciamento Inteligente de temperatura

O modelo conceitual de monitoramento e gerenciamento da temperatura dos equipamento de TI tem como principal objetivo a redução dos riscos, e a mitigação dos danos decorrentes do superaquecimento dos componentes, que é um evento crítico que pode afetar todos os dispositivos que compõe a infraestrutura de TI. Em um *smart datacenter* é necessária a execução de ações proativas e reativas com o propósito de reduzir os pontos de calor e conter o evento.

Foi desenvolvido um fluxograma com o objetivo de representar em alto nível a reação da ocorrência do evento crítico de superaquecimento dos componentes de TI em um *Smart Datacenter*. A Figura 27 ilustra o fluxo de verificações e decisões que devem ser tomadas quando identificado estado de risco a infraestrutura. Foram criados 4 gatilhos para disparar ações reativas no intuito de contenção de estado crítico, ou seja, são executadas para evitar os danos decorrentes da exposição a alta temperatura, portanto se detectado desastre eminente a integridade dos equipamentos será prioridade em ralação as aplicações. Segue a lista de gatilhos e ações:

- O gatilho 1 representado no diagrama como G1 é disparado sob a seguinte condição: quando a temperatura da CPU do host monitorado atinge o valor considerado alto pelo seu fabricante por exemplo sendo acima de 90 C e abaixo de 95 C o que representa um status de alerta e a temperatura não deve continuar aumentando.
- O gatilho 2 representado no diagrama como G2 é disparado sob a seguinte condição: quando a temperatura da CPU do host monitorado está acima do

valor considerado alto pelo seu fabricante por exemplo sendo acima de 90 C e abaixo de 95 C que representa ameaça a integridade da CPU.

- O gatilho 3 representado no diagrama como G3 é disparado sob a seguinte condição: quando a temperatura da CPU do host monitorado atinge a *redline* definida pelo seu fabricante o que representa grande ameaça a integridade do componente.

- O gatilho 4 representado no diagrama como G4 é disparado sob a seguinte condição: Uma vez que no *smart datacenter* a condição de para o disparo de um gatilho é verdadeira, uma ação é executada, desta forma o G4 serve para informar quando a ação de a atrelada a um dos gatilhos anteriores foi suficiente para reduzir o estado do componente a temperatura segura.

Também foram elaboradas ações que são executadas com intuito de contenção quando um gatilho é disparado, servido de condição para ativação de um comando remoto enviado ao host. As ações desenvolvidas para contençaõ do evento crítico superaquecimento foram:

- Ação 1 (A1) : reduzir a frequência do processador para média performance assumindo que a redução de carga contribua para a redução da temperatura do componente, esta é uma ação proativa com objetivo de evitar a ocorrência do evento superaquecimento.

- Ação 2 (A2) : reduzir a frequência do processador para média performance assumindo que a redução de carga contribua para a redução da temperatura do componente, esta ação é executada quando a redução para média performance não diminui a temperatura, fazendo com que a frequência do clock do processador seja alterada para baixa performance com objetivo de forçar a redução da temperatura.

- Ação 3 (A3) : executar comando remoto para hibernação do sistema operacional visto que os prejuízos de avariação tem alto potencial de se tornarem maiores que prejuízos de *downtime*.

- Ação 4 (A4) : alertar redução da temperatura e normalizar o processamento através da execução de um comando remoto de setar modo automático para a frequência do clock. Caso esse aumento eleve a temperatura para o nível de alerta o gatilho 1 é disparado repetindo a frequência de ação.

- Ação 5 (A5) : requer sistema de climatização gerenciável e consiste em enviar um comando remoto para redução da temperatura do equipamento de refrigeração fazendo com que a temperatura ambiente reduza quando as máquinas estiverem trabalhando próximo ao alerta de aquecimento.

O fluxograma ilustrado na Figura 27 representa a contenção ao evento crítico elaborada no modelo conceitual proposto. Este diagrama foi desenvolvido para alto nível afim de ilustrar o fluxo de tomada de decisões quando detectado risco de superaquecimento na infraestrutura:

Uma vez que em um host monitorado a temperatura da CPU apresenta um valor maior que 90 C, considerado alto pelos fabricantes de processadores o gatilho 1 (G1) é disparado, e com ele a ação de de reduzir a frequência do processador. Caso a execução de A1 reduza a temperatura para um valor igual ou menor ao que é considerado seguro para fabricantes, no caso 90 C o gatilho 4 (G4) é disparado, (A4) é executada, normalizando o processamento e caso o equipamento volte a aquecer (G1) é disparado novamente.

Se (A1) não for obter um resultado positivo e a temperatura continuar subindo o gatilho 2 (G2) é disparado e a ação 2 (A2) é executada reduzindo a frequência do processador para o nível baixo, com objetivo de obter redução da temperatura. Caso a execução de A2 reduza a temperatura para um valor igual ou menor ao que é considerado seguro para fabricantes, no caso 90 C o gatilho 4 (G4) é disparado e (A4) é executada, normalizando o processamento e caso esta ação volte a aumentar a ação o Gatilho é disparado novamente.

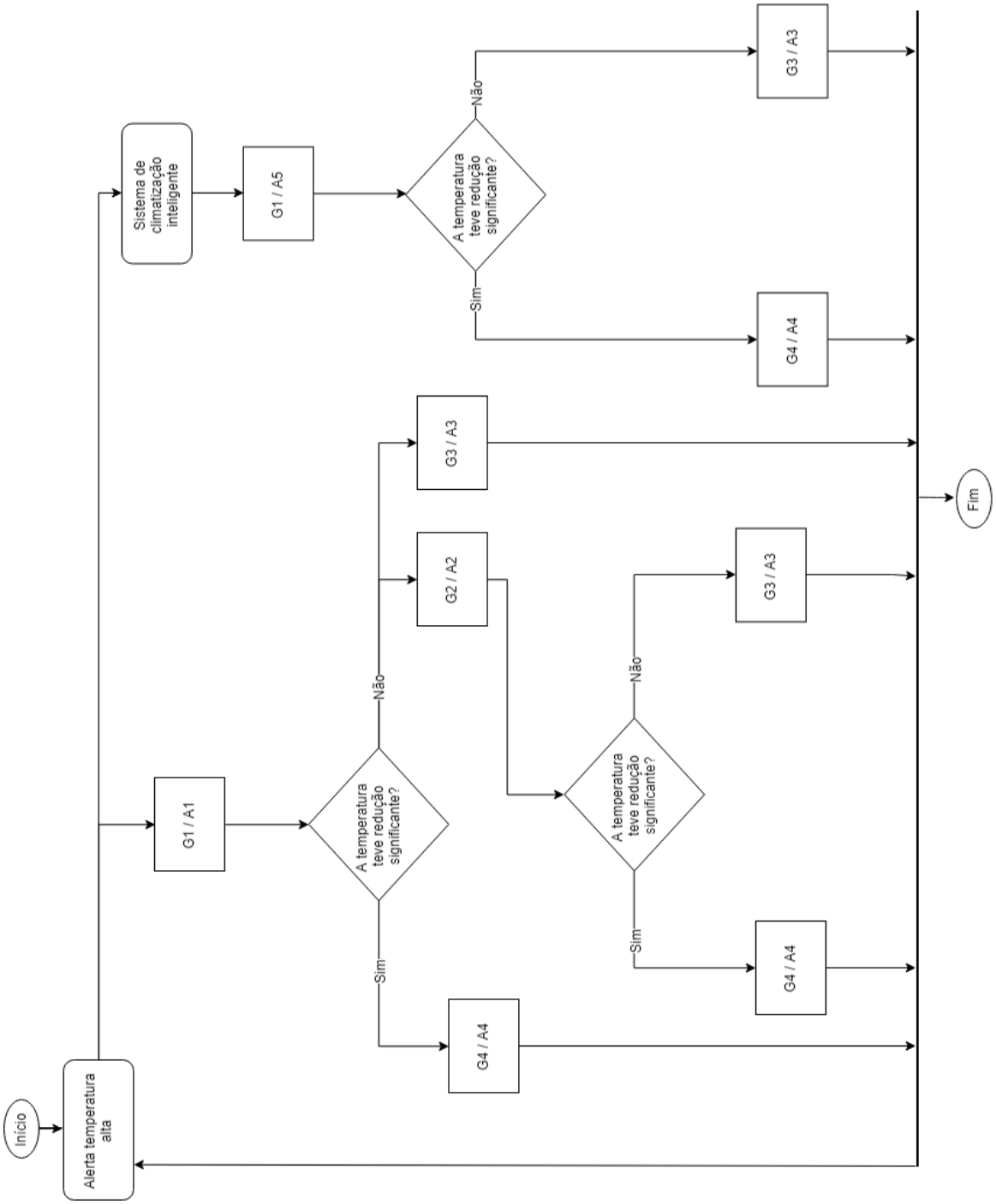
Se (A2) não obter resultado positivo e a temperatura subir para o nível crítico, O gatilho 3 (G3) é disparado e a ação 3 (A3) é executada fazendo com que o *host* seja hibernado através de um comando remoto, com o propósito de contenção dos danos decorrentes do superaquecimento, e a ferramenta de monitoramento e

gerenciamento envia uma mensagem de alerta para os administradores da infraestrutura por meio da ferramenta de monitoramento. Tendo em vista que (A3) afeta a disponibilidade do *host* foi criada uma segunda condição para sua execução, que só ocorre quando (G3) for verdadeiro em todos os *hosts* que possuam este gatilho.

Se a a infraestrutura contar com um sistema de climatização que suporte gerenciamento remoto então quando o gatilho 1 for disparado, seria executada uma (A5) reduzindo a temperatura para 18 C que segundo a norma ASHRAE de climatização de ambientes *datacenter* é suficiente para manter os equipamentos operando abaixo da *redline*, caso o resultado fosse positivo (A4) seria executada normalizando o processamento e informando resultado.

Os gatilhos e ações descritos na representação referente ao modelo de monitoramento e gerenciamento inteligente de temperatura, são adaptados e configurados na ferramenta utilizada para controle da infraestrutura, o Zabbix. E o dispara para execução de ações funciona como um loop qaundo a condição superaquecimento se torna verdadeira.

Figura 27: Representação em Alto nível de Gerenciamento de Superaquecimento para Smart Datacenter.



3.7.1.1 Implementação

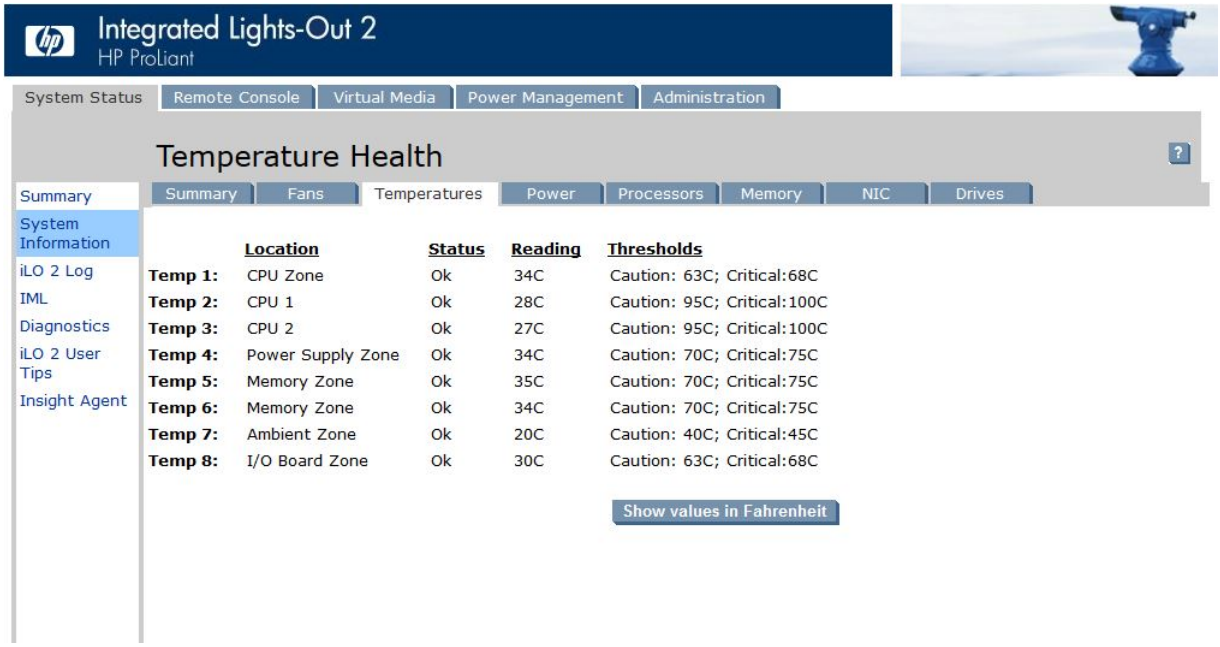
A aplicação parcial do modelo conceitual de monitoramento e gerenciamento de temperatura em um *Smart datacenter* tem como principal objetivo contenção de danos decorrentes da ocorrência do evento crítico superaquecimento. Primeiramente foram definidos os dados que serão monitorados e analisados nas

tomadas de decisões, e neste caso é preciso verificar as limitações de hardware e ambiente, já que quanto maior a quantidade de equipamentos gerenciáveis, maiores as possibilidade de ações autonômicas eficientes.

Uma vez que o laboratório de pesquisas utilizado neste estudo não possui equipamentos para monitoramento e gerenciamento da temperatura ambiente, não é possível determinar com exatidão a este valo. No entanto os servidores utilizados no experimento possuem sensores de temperatura nas principais áreas do seu *hardware*, portanto temperatura próxima do *redline* em todas estas áreas ocorrida em diversos servidores foi definido como falha no sistema de climatização e evento crítico.

A Figura 28 representa o monitoramento da temperatura feito através da placa de gerenciamento do servidor utilizado neste estudo. Os dados coleta de dados realizada por este dispositivo consistem no estado de calor de cada uma das principais zonas do hardware, ou seja, onde ficam seus principais componentes. O status ilustrado nesta na figura apresenta a temperatura das duas CPUs em relação a sua *redline* (CPU1 34C e CPU2 28 por exemplo), dados levados em conta para execução de ações pró-ativas.

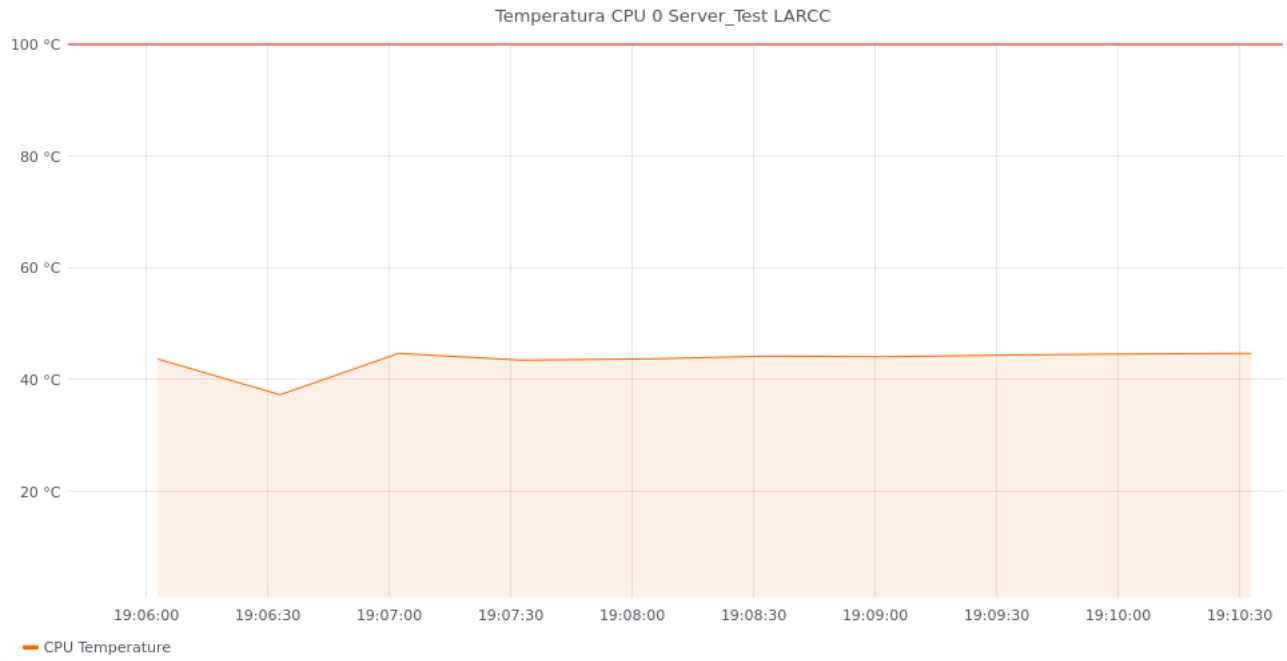
Figura 28: Interface de Monitoramento Servidor.



No monitoramento e gerenciamento de um *smart datacenter* não é recomendável utilizar um única fonte de dados, pois uma vez esta seja comprometida, este evento pode vir a prejudicar a tomada de decisões baseadas nesta coleta. Um exemplo disto seria monitorar a temperatura de uma CPU para decidir hibernar ou desligar um servidor, pois desta forma não seria possível identificar o que está sendo interrompido ou que pode estar gerando o calor elevado. A CPU pode ter sua temperatura elevada a partir de sobrecarga, ou de falha no sistema de climatização e um *smart datacenter* deve se aproximar ao máximo de fazer tal distinção.

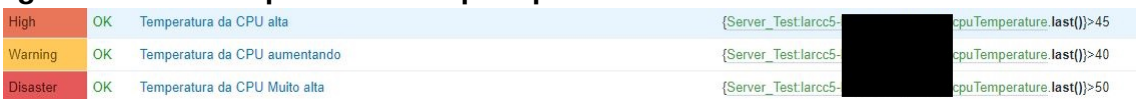
A principal ferramenta utilizada como fonte e coleta de dados é o Zabbix, definido como sistema de monitoramento da infraestrutura e utilizado para coletar informações da temperatura de cada *host* e enviar alertas quando for detectado que algum destes equipamentos atinjiu um valor próximo ao *redline*. A Figura 29 ilustra no gráfico de monitoramento do host utilizado para os experimentos operando com carga de trabalho habitual, que apresenta *Layout* diferente do *default* da ferramenta devida a implantação do Grafana utilizada no tratamento de gráficos. Esta coleta é feita através de sensores internos que compõe o *hardware* desta máquina.

Figura 29: Gráfico monitoramento da temperatura da CPU.



A leitura de dados da temperatura da CPU é utilizada para disparar os gatilhos utilizados como condições, como visto na Figura 27, que foram criados na ferramenta Zabbix. No entanto os valores setados para o disparo destes gatilhos foram modificados, com objetivo de realizar testes controlados de reação ao superaquecimento. O primeiro gatilho (G1) teve o valor de ativação alterado para 40 C, o segundo (G2) teve o valor de ativação alterado para maior que 45 C e o terceiro (G3), teve o valor alterado para 50 C, deste modo o equipamento testado não corre risco de superaquecimento real. A Figura 30 ilustra os gatilhos criados na ferramenta de monitoramento e seu nível de ameaça.

Figura 30: Gatilhos para Evitar Superaquecimento.



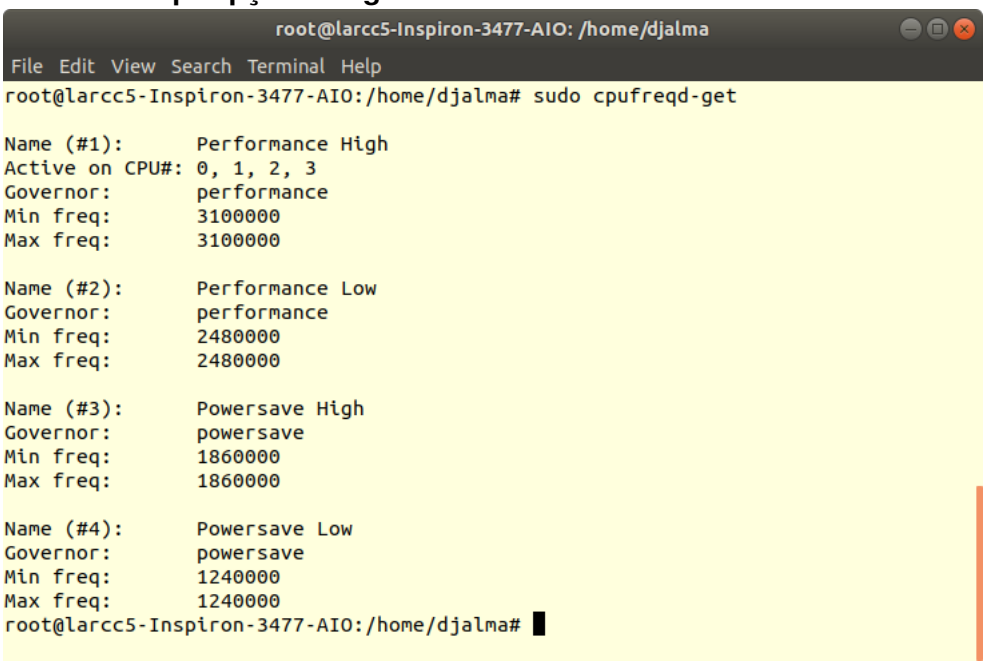
Ações automáticas foram criadas através da função comandos remotos que compõe as funções disponíveis no Zabbix 4.2, versão utilizada na implantação do modelo. No entanto este recurso vem desabilitado por default deste modo deve ser ativado em todos os *hosts* monitorados via *Zabbix Agent*, habilitando o parâmetro (EnableRemoteCommands=1) no arquivo de configuração alterando o valor 0 para 1. O segundo passo é conceder as permissões necessárias para que o usuário zabbix possa executar comandos no servidor, editando o arquivo sudo e adicionando o parâmetro (zabbix ALL=NOPASSWD: ALL). A ideia da implantação do modelo conceitual para temperatura de componentes é fazer com que a infraestrutura reaja a um estado que represente risco para a integridade do hardware, mas quando possível priorize o *uptime*.

Feito isto, uma vez que o Zabbix realize o monitoramento do *host* via agente, e este possua uma *trigger* atrelada para ser utilizada como condição, é possível executar comandos remotamente em sistema operacional. O modelo conceitual utiliza este recurso para diminuir a temperatura reduzindo a frequência do processador visto que este é o componente mais sensível ao aquecimento elevado, que pode vir a causar desligamentos forçados ou na pior hipótese avariação do componente.

Para o gerenciamento da frequência do processador foi utilizado o pacote

"cpufreqd", que possibilita definir um valor menor no intuito de reduzir a temperatura do componente através do parâmetro (sudo cpufreqd-set 4). As opções de gerenciamento dependem diretamente da quantidade e da frequência da CPU monitorada, a Figura 31 ilustra as opções disponíveis no hardware utilizado no estudo.

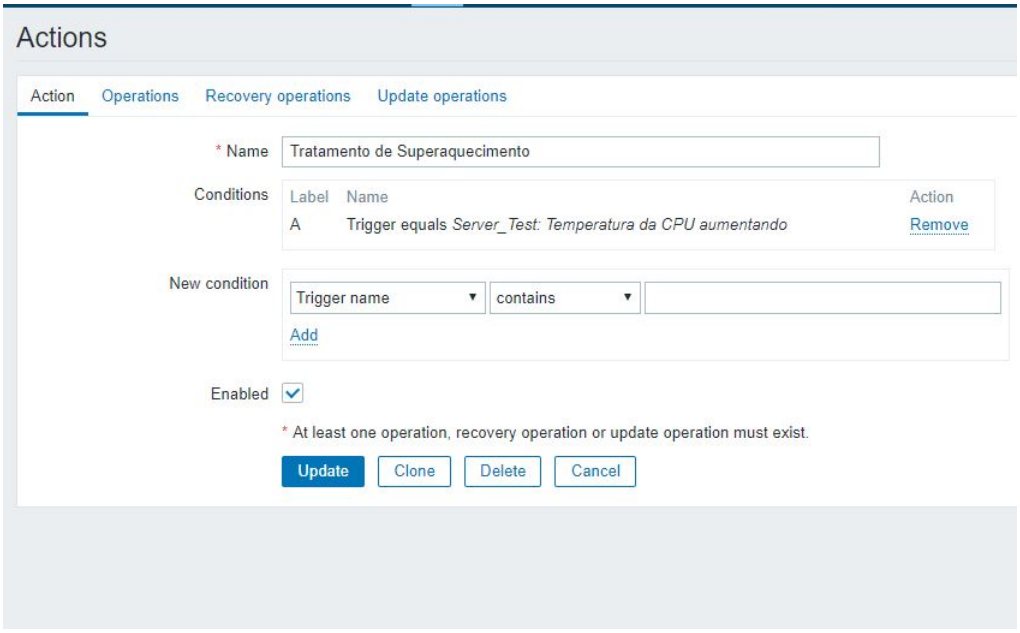
Figura 31: CPUfreqd Opções de gerenciamento.



Foi configurada a ação automática 1 que é executada quando a trigger de aumento de temperatura é disparada. Quando a temperatura da CPU for maior que 40 C no (valor definido para testar aquecimento sem por em risco a integridade do hardware) executar um comando remoto para reduzir a frequência da CPU. Uma vez que o *host* esteja com o "cpufreq"devidamente configurado e instalado, e os parâmetros forem testados localmente, a ação está pronta para ser configurada no Zabbix.

A Figura 32 ilustra a ação 1 configurada ferramenta de monitoramento utilizada neste estudo, o primeiro passo é definir uma condição de execução, neste caso o gatilho 1 (G1), que identifica anomalia na temperatura de um *host*, e quando tal condição for verdadeira o coamando remoto configurado deve ser executado.

Figura 32: Ação automática.



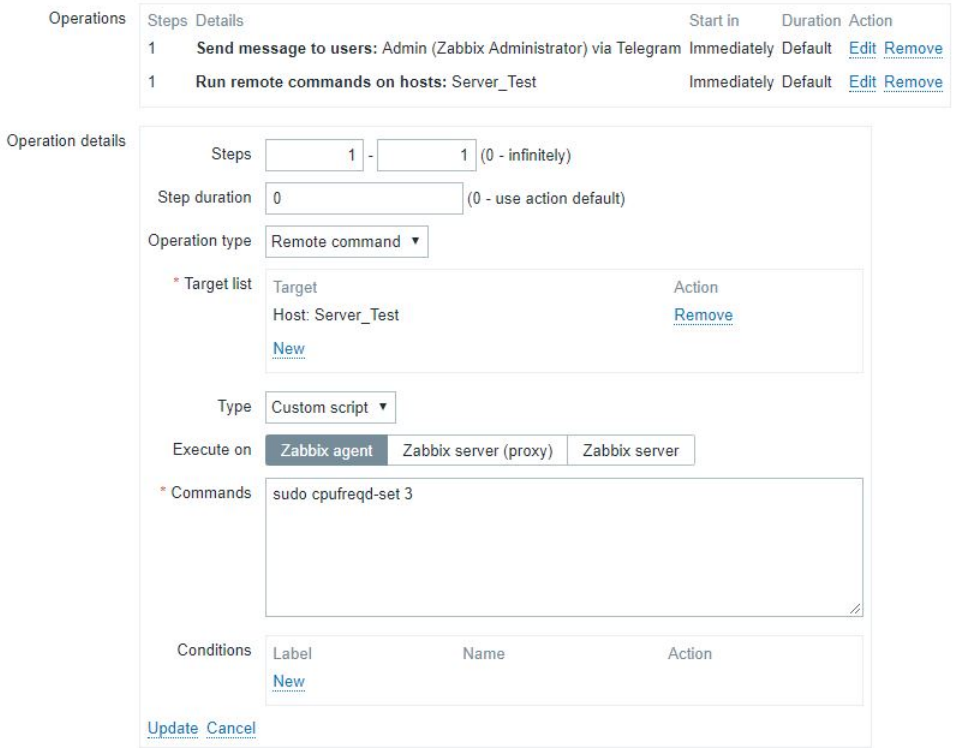
A Figura 33 ilustra a configuração de um comando remoto. A ação foi configurada da seguinte forma: definindo o tipo de operação como *Remote Command* o *host* no qual o comando será executado, o tipo de comando, que neste estudo foi definido como *custon script* e por fim o comando "sudo cpufreqd-set 3"que reduz a frequência do processador de 3.1 para 1.8 GHz, com objetivo de reduzir a temperatura do componente. Também foi configurada um segundo passo para esta ação, que é informar quando se a temperatura foi ou não reduzida.

Também foi configurada uma segunda ação que utiliza como condição o gatilho 2 (G2) disparado quando a temperatura da CPU alcança um valor superior a 45 C (valor definido com objetivo de não colocar em risco o *hardware* utilizado no experimento). Quando esta trigger é verdadeira é executado o comando remoto "sudo cpufreqd-set 4"que reduz a frequência do processador de 1.8 para 1.2 GHz com objetivo de reagir caso a primeira ação não for efetiva e a temperatura continuar a subir.

Foi configurada uma terceira ação a qual é ativada quando a temperatura chega ao nível "desastre"apresentando alto potencial para ultrapassar a *redline* estabelecida pelo fabricante do equipamento. A execução desta ação causa *downtime* dos servidores e aplicações só deve ser executada como ultimo recurso, e sob condições mais severas, por exemplo, quando for detectado potencial superaque-

cimento em todos os *hosts* de um grupo. Caso a condição de disparo deste gatilho for verdadeira, o zabbix executa o comando "sudo pm-suspend"suspendendo o sistema operacional do equipamento de modo a evitar avariações em componentes.

Figura 33: Configuração do comando remoto.



3.7.1.2 Validação

O principal objetivo desta implantação foi a contenção do evento crítico superaquecimento de modo que algumas ações possam interferir na performance de aplicações e no *uptime* dos equipamentos de TI presando a integridade do hardware. Isso se deve a algumas limitações de equipamento e itens de monitoramento, por exemplo, a ausência de um sistema de monitoramento da temperatura ambiente seja sistema de climatização gerenciável, redes de sensores ou mapa térmico, deste modo é possível distinguir com precisão se o evento foi disparado por uma falha de hardware, dissipação, ponto de calor ou falha geral no sistema de refrigeração.

O mapa térmico é gerado através do monitoramento por meio de uma câmera térmica, que gera imagens de todo o ambiente *datacenter*, contribuindo para a detecção de pontos de calor.

Uma rede de sensores externos trabalhando em conjunto com os sensores internos dos equipamentos, é um método muito eficiente para detectar com precisão a causa de um superaquecimento. O estudo de Qu e Li et al. (2013) propõe uma solução para determinar o melhor posicionamento dos sensores com base no sistema de climatização e o espaço físico disponível no *datacenter*. Desta forma com base na quantidade e posicionamento dos sensores que detectarem superaquecimento, é possível terminar se trata-se de um ponto de calor, problemas de dissipação de calor interno ou falha no aparelho de refrigeração do ambiente.

Sem um meio de coleta para estes dados o gerenciamento inteligente da temperatura do *datacenter* em status normal se torna uma tarefa difícil uma vez que o a temperatura elevada no componente é detectada mas não ha certeza absoluta da causa, não é viável interferir na qualidade do serviço ou *uptime* em um ambiente em funcionamento. Por esta razão, o modelo aplicado foi elaborado visando primeiramente contenção de eventos que tendem a gerar grandes prejuízos as organizações responsáveis por estas infraestruturas.

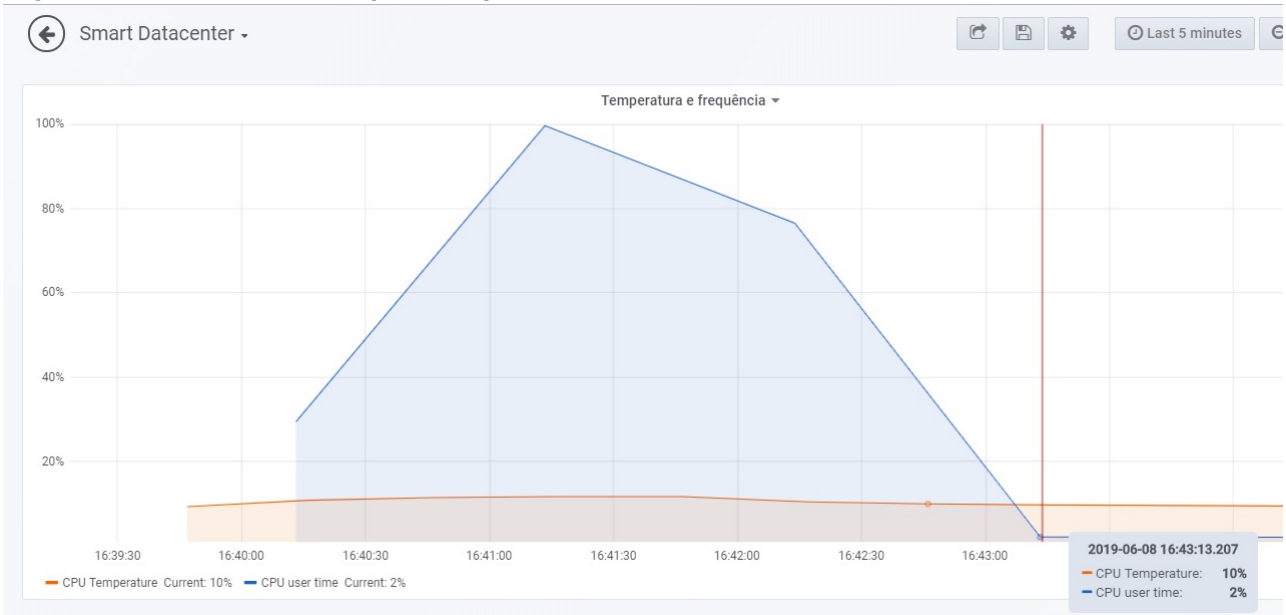
Para a realização deste teste a condição de disparo para a primeira *trigger* foi alterada para apenas 10 C, visto que é inviável desligar o sistema de climatização da infraestrutura para a execução de um teste, além disso esta temperatura não gera risco algum aos componentes.

Figura 34: Tratamento de Superaquecimento em *Smart Datacenter*.

A Figura 34 ilustra os resultados da aplicação do modelo na infraestrutura estudada. Os logs ilustrados são decorrentes da execução de um teste de *stress* executado na CPU do hardware monitorado, o teste faz com que a temperatura do processador amentar para um valor maior ou igual a 10 C, (temperatura baixa, mas utilizada garantir a integridade do componente) a *trigger* temperatura aumentando é disparada, e com ela o comando de reduzir a frequência do *clock* é executado remotamente.

Com isso a temperatura da CPU reduz, mas depois do período de 1 minuto estipulado tendo e vista a severidade da *trigger*, o processamento é normalizado, mas como o teste de stress continua em execução o loop acontece e a temperatura volta a subir, a trigger é disparada e o comando remoto executado, reduzindo a a frequência do processador, que devido a redução na atividade tem seu aquecimento reduzido novamente. Quando o teste chega ao fim o carga e a temperatura do processador são normalizadas e o administrador recebe um alerta, neste caso enviado via API do aplicativo Telegram.

Figura 35: Gráfico de Relação Temperatura Processamento *Smart Datacenter*.



A Figura 35 ilustra o gráfico de utilização do processador e temperatura da CPU do equipamento utilizado na realização deste teste. Quando a temperatura representada em laranja sobe ou valor determinado para que a *trigger* inicial seja

verdadeira o uma comando remoto de para reduzir a frequência do processador é executado e no intervalo entre 16:41H e 16:42H, ocorre uma redução na utilização do processador de 20% e a temperatura fica abaixo do 10 C definidos, quando o teste de *setress* é encerrado a o processamento reduz para 2% e é normalizado.

3.7.2 Modelo de Monitoramento e Gerenciamento Inteligente de Energia

O aplicação parcial do modelo conceitual de monitoramento e gerenciamento de energia em *smart datacenters* proposto neste trabalho tem como principal objetivo a preservação de energia quando detectado a interrupção do recebimento deste recurso. Quando tal evento é ocorrer devem ser executadas uma série de ações para reduzir o consumo energético, tentando aumentar o *uptime* das máquinas. Consequentemente, as ações propostas e implementadas tem como objetivo aumentar o tempo da duração das baterias do sistema utilizado para conter quedas de energia. Caso o desligamento forçado seja necessário, a prioridade é desligar corretamente os servidores para evitar futuras falhas em aplicações.

Foi desenvolvido um fluxograma para representar em alto nível o fluxo de ações executadas no intuído de preservar a carga das baterias no caso de ocorrência do evento crítico queda de energia. A Figura 36 ilustra o fluxo de verificações e decisões que devem ser tomadas quando identificado estado de risco a infraestrutura. Foram criados 4 gatilhos para disparar ações reativas no intuito de contenção de estado crítico, ou seja são executadas para evitar os danos decorrentes da exposição a alta temperatura, portanto se detectado desastre eminente, a integridade dos equipamentos será prioridade em ralação as aplicações.

Para um modelo inteligente de economia de bateria e contenção de queda de energia, é importante considerar a prioridade de *uptime* e desempenho de cada um dos *hosts* ligados a um sistema de contenção de interrupção energética como um no-break, por exemplo. Deste modo, quando o nível de bateria reduzir é possível programar qual o primeiro *host* que terá performance reduzida e no caso do evento se prolongar qual será desligado primeiro, e de modo autonômico manter ativo o maior tempo possível.

Outro fator a ser considerado é que exitem variáveis que podem afetar o

tempo necessário para execução de ações reativas para pongamento de carga de bateria. São eles a capacidade das baterias, o número de equipamentos ligados a elas, e a carga de trabalho e a demanda de energia destes componentes. A nível de infraestrutura, reduzindo poder computacional, o tempo de duração das baterias tende a aumentar.

Para tomada as configurações autonômicas de redução de consumo energético foram considerardes os seguintes estados de energia para o *host* monitorado: Modo performance alta, modo performance baixa, modo *powersave high* e modo *powersave low*. Estes modos de operação tem tendência a reduzir a performance do equipamento, no entanto quanto menor for o desempenho do hardware o consumo energético também tende a ser menor, no entanto a heterogeneidade de equipamentos de TI não permite definir esta informação como verdadeira. Segue a lista de gatilhos e ações:

- Gatilho 1 (G1) é disparado sob a seguinte condição: quando o nível de bateria for reduzido a 90%, o escolhido já que indica que a bateria que mantém o sistema operando está sendo consumida mas ainda não atingiu um estado de risco alto.

- Gatilho 2 (G2) é disparado sob a seguinte condição: quando o nível de bateria for reduzido a 50% , o que é considerado um estado de alerta uma vez que metade do recurso já foi consumido e *hosts* com prioridade menor podem ter seu modo de energia reduzido.

- Gatilho 3 (G3) é disparado sob a seguinte condição: quando o nível de bateria for reduzido a 10%, o que é considerado um estado cítico pois uma vez que o recurso esgotar todos os equipamentos serão desligados além disso este valor representa tempo hábil para o desligamento correto dos equipamentos.

Também foram elaboradas ações que são executadas com intuito de contenção, quando um gatilho é disparado e a condição para ativação de um comando remoto enviado ao *host* é verdadeira. As ações desenvolvidas para contenção do evento crítico superaquecimento foram:

- Ação 1 (A1): reduzir modo de energia do servidores de baixa prioridade, para econômico alto de modo a causar interferência mínima na execução das aplicações. Esta ação proativa com objetivo de aumentar a duração da bateria do no-break em caso de queda de energia.
- Ação 2 (A2): reduzir modo de energia dos servidores de baixa prioridade para econômico baixo, e dos servidores de maior prioridade para econômico alto. Esta ação tem como objetivo aumentar o tempo de duração da bateria quanto metade da carga já estiver sendo consumida.
- Ação 3 (A3): desligar servidores assumindo queda de energia longa, e desta forma evitar desligamento forçado. Esta ação reativa tem como objetivo desligar servidores corretamente sabendo que o desligamento forçado é eminente.
- Ação 4 (A4): normalizar processamento sempre que a condição de disparo de um dos gatilhos descritos acima for falsa: Esta é uma ação reativa quando executado quando a energia retornar.

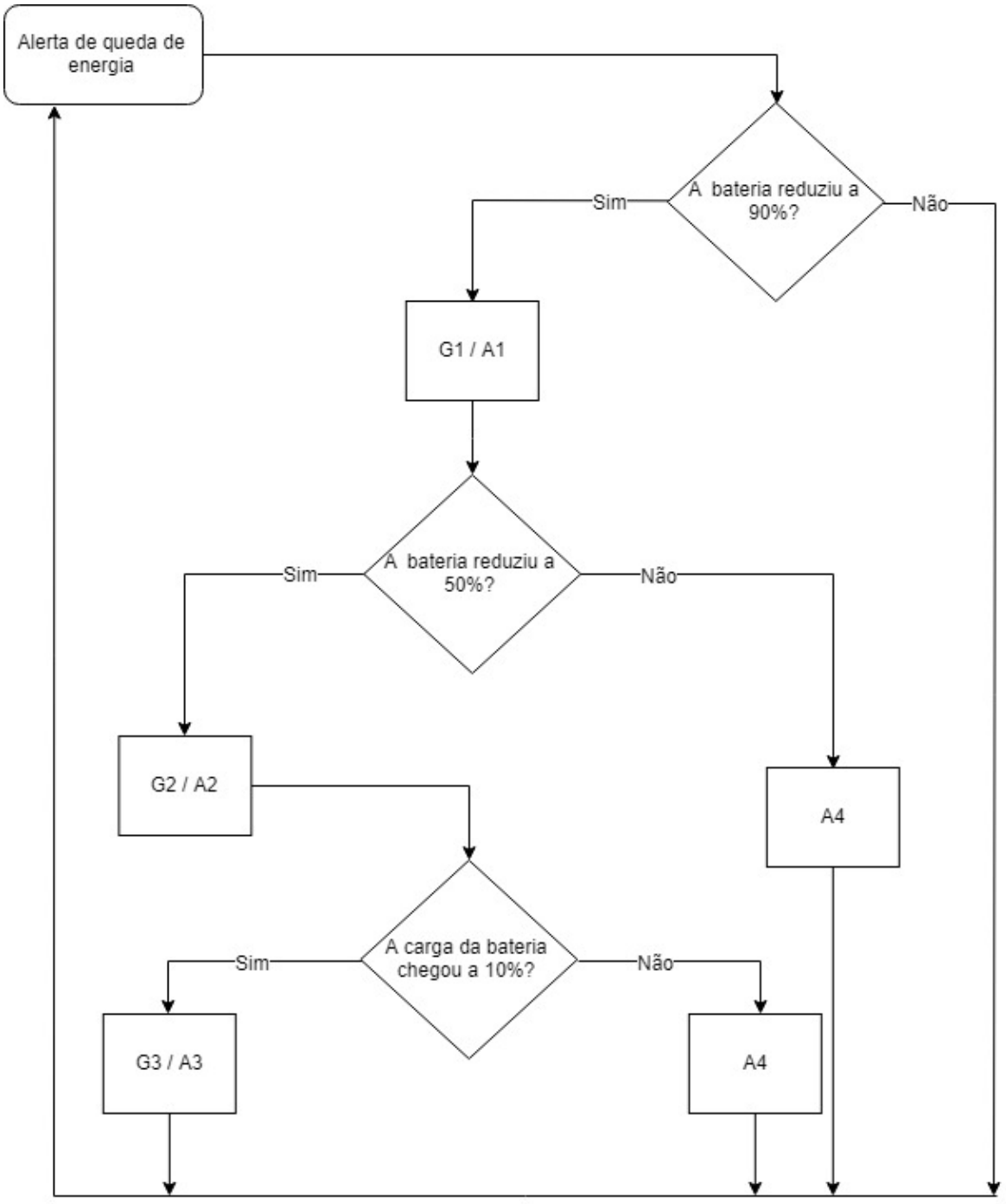
O fluxograma ilustrado na Figura 36 a contenção dos eventos queda de energia curta e longa em um *smart datacenter*, que utiliza um no-break gerenciável como dispositivo de contenção. Este diagrama foi desenvolvido em alto nível afim de ilustrar o fluxo de tomada de decisões quando detectado interrupção do serviço de energia.

Uma vez que a entrada de energia no no-break é igual a 0 o evento queda de energia curta é assumido. Se (G1) for falso o que significa que a energia retornou o evento é encerrado. Quando (G1) for disparado é assumido que houve consumo de baterias e (A1) é executada com objetivo de reduzir o consumo da bateria sem grandes interferências na aplicações.

Se (G2) for disparado significa que a bateria chegou a metade e a (A2) é executada reduzindo o modo de energia dos servidores que tiverem baixa prioridade para econômico baixo, e dos que tiverem alta prioridade para econômico alto, se ocorrer retorno de energia no intervalo entre (G1) e (G2) a (A4) é executada normalizando o processamento.

Se (G3) for dispara significa que o no-break esta com níveis de bateria baixos ou seja 10% e o intervalo entre este valor e 0% que significa bateria esgotada, deve ser utilizado para desligamento correto dos equipamentos e assumir a ocorrência do evento queda de energia prolongada. Se (G3) não for dispara e houver retorno de energia é executado (A4) e o processamento é normalizado.

Figura 36: Representação em Alto nível de Gerenciamento de Queda de Energia para Smart Datacenter.

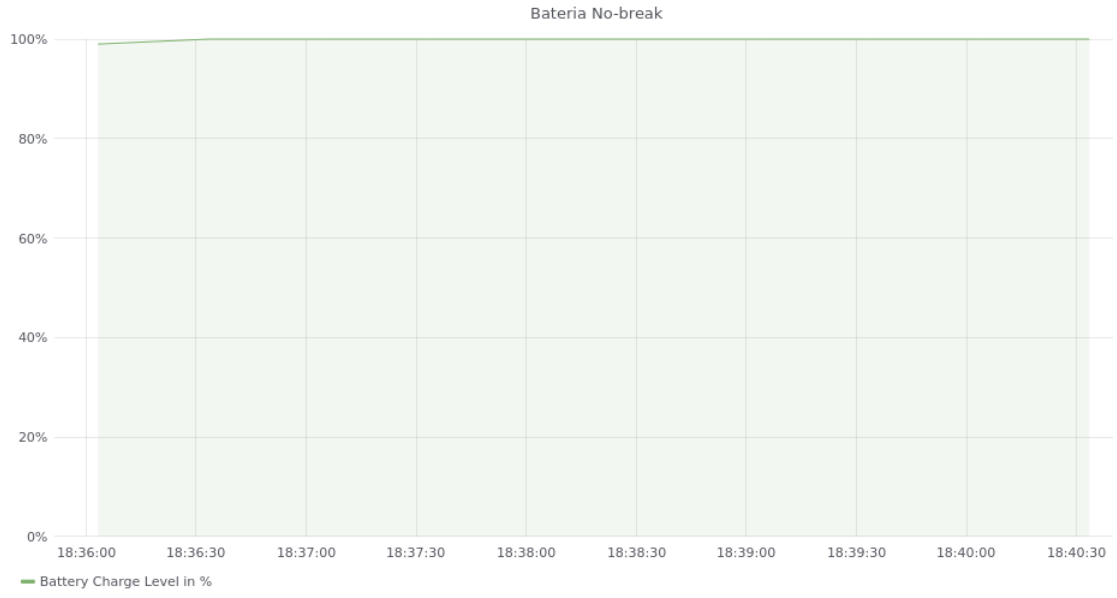


3.7.2.1 Implementação

O primeiro passo a implementação deste modelo foi a configuração do monitoramento do no-break gerenciável para coletar dados referentes a entrada e saída de energia, ou quais foram utilizados na configuração de gatilhos que serviram como condições para a execução de ações. O equipamento utilizado foi o no-break Delta UPS, linha Anplon, Série RT 1/2/3 kVA, que possui as seguintes especificações: Potência: ([RT-3k] 3kVA / 2,7KW), tipo de baterias: (12V 9Ah bateria selada), autonomia típica: (RT-2k/3k] : 7,5 min, tempo de recarga).

O monitoramento deste equipamento é feita através da placa de monitoramento e gerenciamento (Insigth power SNMP IPV4) que possui suporte ao protocolo SNMPv1. O a ferramenta Zabbix coleta as informações do equipamento através do protocolo SNMP. Para a aplicação deste foi realizada a coleta de dados dos seguintes itens. O nível de bateria disponível no no-break é o principal alvo da coleta de dados já que este modelo consiste em aumentar sua duração durante a ocorrência de um evento queda de energia.

Figura 37: Gráfico de Nível de Bateria no No-break.



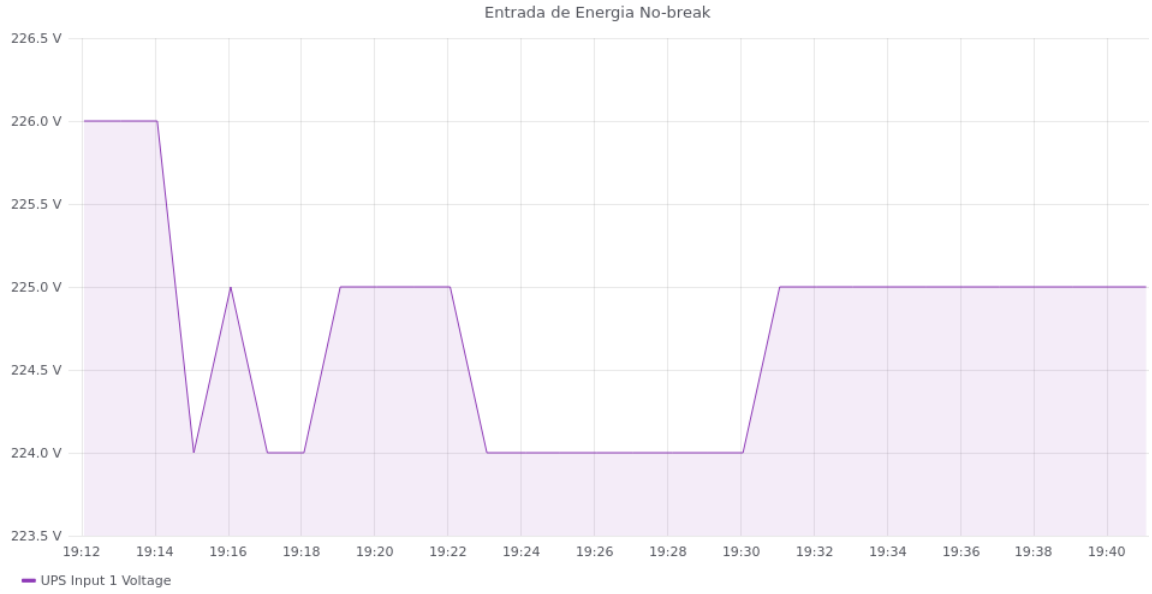
A Figura 37 ilustra o gráfico referente ao nível de bateria disponível no equipamento. Esta representação é linear e o intervalo de tempo que pode ser definido na ferramenta, esta é um representação gráfica dos dados coletados para a configuração do modelo de monitoramento e gerenciamento inteligente na ocorrência

de queda de energia.

Além do nível de bateria também foram realizados o monitoramento da entrada de energia do no-break. Esta coleta de dados foi configura com o objetivo de identificar o valor energético recebido pelo *no-break*, e para esse item foi configurado um gatilho que é disparado quando a este valor é igual a 0. Quando esta condição for verdadeira o *Smart Datacenter* interpreta queda de energia.

A Figura 38 é a representação gráfica dos valores coletados pelo ferramenta de monitoramento Zabbix, referente a voltagem de entrada do no-break utilizado no estudo. Se este valor chegar a 0 fluxo de ações representado na Figura 36 é iniciado caso este valor não se torne diferente de 0 antes que o equipamento chegue a 90% de carga de bateria.

Figura 38: Gráfico Entrada de energia no No-break.



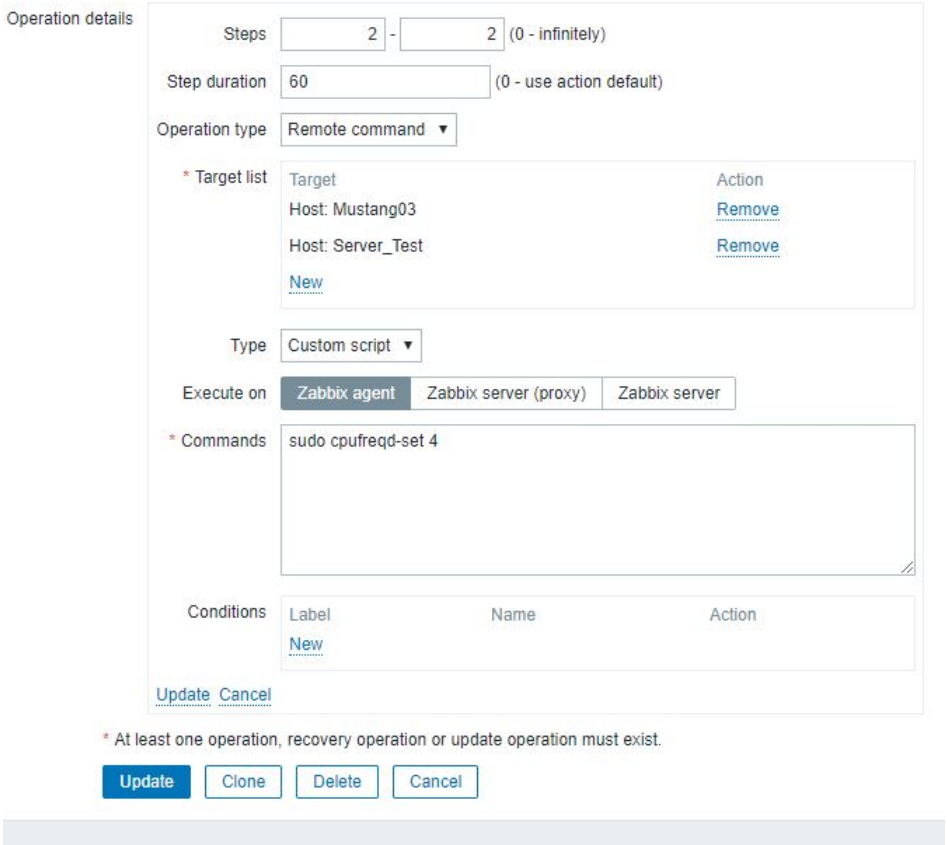
Também foi configurado o monitoramento da saída de energia do No-break, com o objetivo de medir o nível de energia que sai deste do equipamento e vai para os servidores. Esta coleta tem como objetivo detectar se a redução da capacidade de poder computacional é eficiente no objetivo de economia da bateria do no-break.

Os valores de ativação das *triggers* responsáveis por disparar as ações autonômicas deste modelo foram alteradas, com objetivo de tornar o experimento seguro para a infraestrutura no qual é testado. O primeiro gatilho disparado quando o nível de bateria for menor que 90% de bateria teve seu valor alterado para 98%

o segundo gatilho teve os valores alterados de 50% para 90%, e o terceiro de 10% para 85%. Desta forma o nível de bateria não tem uma redução suficiente para interferir na contenção de um incidente real.

Para a configurar as ações autonômicas executadas na ocorrência do evento, foi utilizada a função comandos remotos que compõe os recursos da ferramenta de monitoramento Zabbix. Primeiramente foi definida a *trigger* que serve de condição para a execução do comando remoto, depois foram configuradas as operações, parâmetros da execução destes comandos. A Figura 39 mostra um exemplo de configuração de comandos remoto no Zabbix, onde são definidas condições, intervalos, os *hosts* recebem o comando e o tipo de mensagem, nesse caso *custon script*.

Figura 39: Configuração de Comandos Remotos para Contenção de Queda de Energia.



A primeira ação foi configurada da seguinte forma: a *trigger* disparada quando o nível da bateria alcança um valor menor que a 98% (o valor real é 90%), o Zabbix envia um comando remoto para reduzir o nível de energia do dos *host*

atrelados a esta ação.

A segunda ação foi configurada da seguinte forma: quando a segunda trigger é disparada e a bateria do no-break chega a um valor igual ou menor que 90 (O valor real é 50%) é interpretado que a bateria já reduziu a metade de sua capacidade, portanto o usuário zabbix executa o comando de reduzir o nível de energia do servidor para baixo consumo em um intervalo 60 segundos envia um comando para reduzir o nível de energia dos servidores de alta prioridade para *powersave high*".

A terceira ação foi configurada da seguinte forma: quando a terceira *trigger* for disparada e o nível de bateria do no-break chegar a 85% (O valor real é 10%) os servidores ligados a este equipamento são desligados, e o modelo assume que o evento crítico é queda de energia longa.

A quarta ação foi configurada da seguinte forma: a quarta ação foi configurada como uma operação de *Recovery*, desta forma quando a entrada de energia no no-break for maior que 0, o significa que a energia retornou, uma vez disparada o modo de energia dos *hosts* é normalizado.

3.7.2.2 Validação

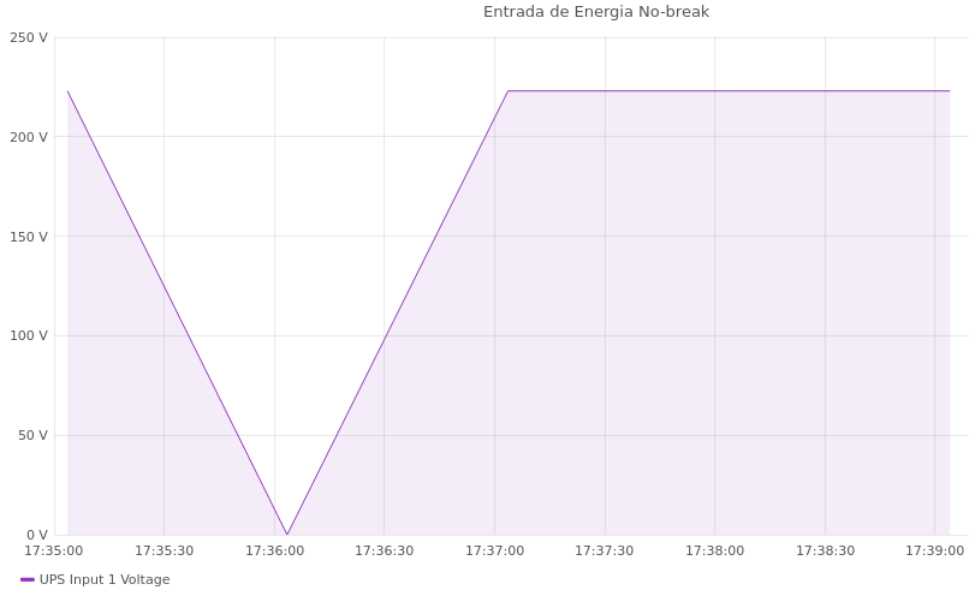
O monitoramento e gerenciamento de energia para *Smart Datacenters* a nível de infraestrutura tem os seguintes elementos como alvo. Primeiramente a otimização do uso da energia elétrica, reduzindo o consumo desnecessário sem interferência no desempenho ou disponibilidade das aplicação. Também o gerenciamento do equipamentos utilizados para contenção no caso de queda de energia utilizando recursos de forma mais moderada aumentando a duração da autonomia do sistema. E por fim a integridade dos componentes quando ocorrerem oscilações e quedas de energia que podem causar danos ao *datacenter*.

O objetivo deste estudo foi a utilização do modelo conceitual proposto para aplicar gerenciamento inteligente dos recursos em caso de queda de energia. Para testar a eficácia destas ações foi realizado um teste controlado interrompendo a alimentação do no-break para que o gatilho configurado como condição para que o sistema de monitoramento reaja a queda de energia fosse disparado. A Figura

40 ilustra o gráfico de entrada de energia no no-break indicando a ocorrência do evento queda de energia.

Este teste busca determinar os resultados da execução de ações autonômicas durante o intervalo em que a entrada de energia do no-break for menor que 0. Além de verificar se há redução nos níveis de saída de energia do no-break em consequência da redução de poder computacional.

Figura 40: Interrupção Controlada na Entrada de Energia.



Tendo em vista a capacidade de autonomia do no-break utilizado, foi setado como condição para disparo do gatilho inicial a seguinte condição, quando o nível de bateria chegar a 90%, porém para que este teste seja controlado o gatilho inicial é disparado com 98% de carga. Quando a *trigger* configurada foi disparada o objetivo era que o comando remoto fosse executado causando redução no nível de frequência do clock dos servidores, e que esta ação reduza a saída de energia do no-break quando a entrada for igual a 0.

Neste intervalo de tempo a saída de energia do no-break aumenta drasticamente chegando a um pico. A Figura 41 ilustra graficamente a saída de energia do No-break no momento em que o teste foi executado. O gráfico ilustra quando ocorre um aumento na demanda energética, no entanto o objetivo principal é reduzir o consumo para assim prolongar a duração das bateria do equipamento.

Como visto na Figura 41 durante a execução do teste as 17:38H até as

17:39H ocorre um declínio nos níveis de saída de energia, devido a execução da ação de redução de frequência de processamento. Além disso quando o nível de bateria é normalizado as 17:40H a saída de energia também é normalizada.

Figura 41: Saída de Energia durante o Evento.

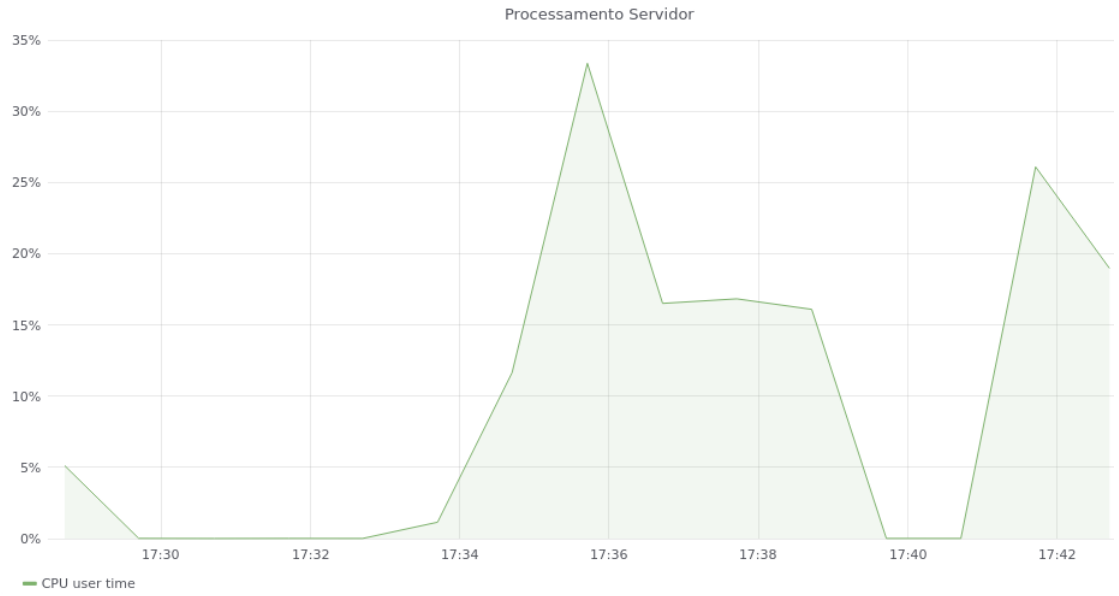
Na Figura 41 ilustra o gráfico referente a saída de energia, onde o seu valor começa a reduzir junto com o processamento mostrado no gráfico da Figura 41 no mesmo intervalo de tempo em que a entrada de energia do no-break é igual a 0, ou seja, o equipamento não esta recebendo energia. O teste foi executa as 17:36H, quando a alimentação do no-break foi interrompida e foi concluído as 17:38H onde a entrada de energia é restaurada, desta forma a redução na bateria não afeta possíveis eventos reais.

A Figura 42 ilustra o gráfico de processamento do servidor ligado ao no-break durante o evento, que está em 35% as 17:34H. Tal percentual vai reduzindo gradativamente conforme a queda de energia se prolonga, isso se dá devido a execução dos comandos remotos configurados na ferramenta de monitoramento *Zabbix*, que reduzem a frequência da CPU a medida que os níveis de bateria diminuem. Na Figura 42 é ilustrado gráfico onde pode-se acompanhar o comportamento do processamento do *host*.

Durante a ocorrência do evento a medida que os níveis de bateria diminuírem o processamento do servidor deve ser reduzido de modo a diminuir a saída de energia do no-break e prolongar a duração da bateria do mesmo. No entanto

quando a entrada de energia do no-break voltar a ser positiva, o processamento deve ser normalizado.

Figura 42: Processamento do servidor de teste durante o Evento.



Na Figura 42 ilustra a normalização da frequência do processado ao fim do intervalo de tempo no qual ocorre a realização do teste, onde o mesmo é aumentado para 25% como pode ser visto no gráfico representado na Figura 42. Deste modo quando a entrada de energia for maior que 0 o que significa retorno deste serviço, a frequência do *clock* é normalizada para que não haja interferência na execução de aplicações.

Com os resultados obtidos por meio da execução do teste de aplicação prática do modelo conceitual referente a energia, constatou-se que a redução na frequência de processamento dos servidores ligados ao no-break durante o teste ocasiona uma redução no consumo energético, capaz de prolongar a duração da bateria durante um evento crítico.

CONCLUSÃO

O presente trabalho teve como principal objetivo propor um modelo de monitoramento e gerenciamento para *Smart Datacenters*, e testar sua eficácia implantando-o parcialmente em uma infraestrutura computacional. Com os resultados obtidos no Capítulo 3 deste estudo foi possível obter os dados necessários para a montagem de um modelo que abranja as principais áreas de um *datacenter*.

Com a ausência de normas ou modelos para gestão de *Smart Datacenters*, o presente trabalho buscou através de uma pesquisa elaborar uma proposta de gerenciamento inteligente a nível de infraestrutura. Para isso foi realizada uma pesquisa para levantamento das atuais necessidades dos *datacenters*, e o nível de controle autonômico que já é utilizado em suas principais áreas da suas estruturas, divididas neste estudo em: climatização, redes, computação, energia e segurança.

O problema da pesquisa foi como realizar a validação prática do modelo conceitual de monitoramento e gerenciamento para *Smart Datacenters*, que foi aplicado para as áreas de energia e climatização. E desta forma analisar o nível de efetividade de uma abordagem de gerenciamento baseada em computação autônoma.

Foram levantadas duas hipóteses para esta pesquisa sendo que a primeira afirma: “A implantação do modelo conceitual permite gerenciar a temperatura dos servidores de forma autonômica e evitar superaquecimento de componentes". E a segunda afirma: “A implantação do modelo conceitual permite gerenciar os recursos dos servidores e forma autonômica para a redução do consumo energético".

Para testar a validação da primeira hipótese foi realizado o monitoramento da temperatura das CPUs dos servidores utilizados no teste, através de sensores internos que integram o *hardware* destes componentes. Por meio da utilização da leitura de dados coletados nestes sensores é possível detectar quando um componente está muito próximo, ou ultrapassa a *redline* estabelecida pelo seu fabricante.

Para testar o gerenciamento e a utilização de ações proativas e reativas a ocorrência de superaquecimento foram utilizadas as configurações de *triggers*, que são condições para execução de comandos remotos. Os gatilhos configurados são disparados proativamente em temperaturas de riscos, e reativamente em temperatura críticas. Nesse caso a execução do modelo funcionou da seguinte forma: foi determinado um valor de aquecimento baixo para disparar o gatilho inicial, a frequência do processador reduzida fazendo juntamente com a temperatura, esta é uma ação proativa.

Neste caso, considerando que o valor fosse acima da *redline* e a primeira ação não fosse efetiva, quando a temperatura crítica for atingida, no lugar da ação que reduz a frequência seria executado um comando que suspende a máquina. Para aumentar a eficácia da aplicação seria necessário um equipamento de climatização gerenciável ou uma rede de sensores de temperatura ambiente, uma vez que o gerenciamento tem a informação da causa do evento (falha no sistema de climatização, falha na dissipação de calor por exemplo) as ação reativas podem ser mais focadas na causa do evento.

Tendo analisado o desempenho da função de comandos remotos que compõe a ferramenta de monitoramento utilizada, pode-se afirmar que primeira hipótese que pressupõe que aplicação do modelo conceitual de monitoramento e gerenciamento para temperatura reduz o risco de superaquecimento foi corroborada, mas em cenários extremos, esta contenção afeta diretamente o *uptime*.

A segunda hipótese que pressupõe que a aplicação do modelo conceitual de monitoramento e gerenciamento de energia foi corroborada pois mesmo o modelo não sendo viável para redução do custo operacional energético, o consumo pode ser reduzido com propósito de prolongar a duração do nível de bateria do no-break, com a utilização de comandos remotos para reduzir a performance dos

equipamentos durante um evento crítico.

Portanto, o modelo inteligente de energia também foi ajustado para o nível de contenção de eventos, e utilizado com objetivo de prolongar o tempo de duração das bateria do no-break, quando detectado o evento queda de energia. Para a realização deste teste foi realizado um teste controlado interrompendo a bateria do no-break, e foram analisadas a saída de energia deste equipamento e a utilização do processador neste intervalo de tempo.

Com isso foi concluído que o modelo conceitual de monitoramento e gerenciamento para *smart datacenter* a nível de infraestrutura tem maior eficácia quando funciona de forma reativa a contenção de eventos críticos, reduzindo recursos quando necessário a fim de priorizar a integridade dos equipamentos de TI. Tendo em vista o crescente aumento nas infraestruturas de *datacenters* e a importância em manter o maior nível de disponibilidade e desempenho dos recursos, foram abordados os seguintes trabalhos futuros:

- Modelo de monitoramento e gerenciamento para *Smart Datacenter* a nível de aplicação.
- Análise de desempenho de aplicação do modelo em diferentes ferramenta de gerenciamento de redes.
- Modelo conceitual de monitoramento e gerenciamento inteligente para infraestruturas de rede.

O gerenciamento inteligente para infraestruturas de *datacenter* é uma área muito abrangente, e com o crescimento de tecnologias como computação em nuvem, e o aumento da demanda energética dos equipamentos de alto desempenho, existe uma necessidade crescente em utilizar abordagens que não requerem intervenção humana.

REFERÊNCIAS

ALMEIDA, R. M. A. de; MORAES, C. H. V. de; SERAPHIM, T. d. F. P. **Programação de Sistemas Embarcados: desenvolvendo software para microcontroladores em linguagem c**. Elsevier Brasil, 2017.

AVELAR, V.; AZEVEDO, D.; FRENCH, A.; POWER, E. N. PUE: a comprehensive examination of the metric. , v.49, 2012.

BOUHAÏ, N.; SALEH, I. **Internet of Things**: evolutions and innovations. John Wiley & Sons, 2017.

BROCKE, J. vom; ROSEMANN, M. **Manual de BPM: gestão de processos de negócio**. Bookman Editora, 2013.

BUYYA, R.; VECCHIOLA, C.; SELVI, S. T. **Mastering cloud computing foundations and applications programming**. Newnes, 2013.

CAUX, S.; ROSTIROLLA, G.; STOLF, P. Smart Datacenter Electrical Load Model for Renewable Sources Management. , 2018.

CHAVES, I. C.; PAULA, M. R. P. de; LEITE, L. G.; QUEIROZ, L. P.; GOMES, J. P. P.; MACHADO, J. C. Banhfap: a bayesian network based failure prediction approach for hard disk drives. , p.427–432, 2016.

DOCUMENTATION, Z. **ZABBIX Documentation, 2018**. Acesso em: 15 Fevereiro de 2019„ Disponível em: http://www.zabbix.com/downloads/ZABBIX Manual v1.

EBBERS, M.; ARCHIBALD, M.; FONSECA, C. F. F. da; GRIFFEL, M.; PARA, V.; SEARCY, M. et al. **Smarter Data Centers: achieving greater efficiency**. IBM Redbooks, 2011.

FAHRIANTO, F.; ANGGRAINI, N.; SUSENO, H. B.; SHABRINA, A.; REZA, A. Smart data centre monitoring system based on Internet of Things (IoT)(study case: pustipanda uin jakarta). In: INTERNATIONAL CONFERENCE ON CYBER AND IT SERVICE MANAGEMENT (CITSM), 2017., Denpasar, Indonesia. **Anais...** [S.l.: s.n.], 2017. p.1–9.

FIT, E. D. C. **Projeto De Sustentabilidade Energética aplicada a um ambiente data centers**. Bookman Editora, 2014.

GALSTAD, E. Nagios Version 3. x Documentation. **Nagios Group [viitattu 20.2. 2009]. Saatavissa: http://nagios.sourceforge.net/docs/nagios-3.pdf**, 2008.

GENG, H. **Data center handbook**. John Wiley & Sons, 2014.

GURGEL, P.; BRANCO, K.; TEIXEIRA, M. M. et al. **Redes de computadores**: da teoria a prática com netkit. Rio de Janeiro: Elsevier, 2014.

HIBA, S. H.; BELGUIDOUM, M. **Toward a meta-model for elasticity management in cloud applications**. [s.n.], 2017. 1–6p.

HUMBLE, J.; FARLEY, D. **Entrega contínua Como entregar software**. Bookman Editora, 2014.

ISO, I. 27002: 2013. **Information technology Security techniques-Code of practice for information security controls.**, [S.l.], 2013.

JAYASWAL, K. **Administering Data Centers, Servers, Storage, and Voice over IP**. John Wiley & Sons, 2005.

JOIA, A. A. L. A. **Gestão estratégica da tecnologia da informação**. Editora FGV, 2015.

KOOMEY, J. Growth in Data Center Electricity Use 2005 to 2010. **A report by Analytical Press, completed at the request of The New York Times**, v.9, 2011.

KUROSE, J. F.; ROSS, K. W.; ZUCCHI, W. L. **Redes de Computadores ea Internet**: uma abordagem top-down. Pearson Addison Wesley, 2013.

LAMB, F. **Automação Industrial na Prática-Série Tekne**. [S.l.]: AMGH Editora, 2015.

LEE, I.; LEE, K. The Internet of Things (IoT): applications, investments, and challenges for enterprises. **Business Horizons**, v.58, n.4, p.431–440, 2015.

LIMA, J. d. R. **Monitoramento de Redes com Zabbix, Monitore a saúde dos servidores e equipamentos de rede**. [s.n.], 2014.

LIU, Q.; DA SILVA, D.; THEODOROPOULOS, G. K.; LIU, E. S. Towards an agent-based symbiotic architecture for autonomic management of virtualized data centers. In: 2017 5TH . **Anais...** [S.l.: s.n.], 2012.

LOVATO, A. **Metodologia da Pesquisa SETREM**. Editora Setrem, 2013.

MARCONI, M. d. A.; LAKATOS, E. M. **Técnicas de pesquisa**. São Paulo: Atlas, 2017.

MARINESCU, D. C. Cloud infrastructure. **Cloud Computing: Theory and Practice**, p.67–98, 2013.

MARTIN, J. P.; KANDASAMY, A.; CHANDRASEKARAN, K. Toward Efficient Autonomic Management of Clouds: a cds-based hierarchical approach. In: **Advanced Computing and Systems for Security**. Springer, 2018. p.61–73.

MOUSAVI, A.; BEREZOVSKAYA, Y.; VYATKIN, V.; ZHANG, X. Energy efficient decision making in data centers with multiple cooling methods. , p.8785–8790, 2017.

MUKHERJEE, T.; BANERJEE, A.; VARSAMOPOULOS, G.; GUPTA, S. K. Model-driven coordinated management of data centers. **Computer Networks**, v.54, n.16, p.2869–2886, 2010.

MUNTEANU, I.; DEBUSSCHERE, V.; BERGEON, S.; BACHA, S. **Efficiency metrics for qualification of datacenters in terms of useful workload**. Grenoble, France: [s.n.], 2013.

NOROUZI, F.; BAUER, M. Autonomic Management for Energy Efficient Data Centers. **CLOUD COMPUTING 2015**, London, Canada, p.153, 2015.

OLIVEIRA, R. C. Q. **Segurança em redes de computadores**. Senac, 2018.

PARASHAR, M.; HARIRI, S. **Autonomic computing**: concepts, infrastructure, and applications. CRC press, 2006.

PORTOCARRERO, J. M.; DELICATO, F. C.; PIRES, P. F.; COSTA, B.; LI, W.; SI, W.; ZOMAYA, A. Y. **Ramses a new reference architecture for self-adaptive middleware in wireless sensor networks**. Elsevier, 2017. 3–27p. v.55.

QU, J.; LI, L.; LIU, L.; TIAN, Y.; CHEN, J. Smart temperature monitoring for data center energy efficiency. In: IEEE INTERNATIONAL CONFERENCE ON SERVICE OPERATIONS AND LOGISTICS, AND INFORMATICS, 2013., Dongguan, China. **Proceedings...** [S.l.: s.n.], 2013. p.360–365.

ROSSI, M.; RIZZON, L.; PASSERONE, R.; MINAKOV, I.; SARTORI, D.; BRUNELLI, D. Non-invasive cyber-physical system for data center management. **Sustainable Computing: Informatics and Systems**, v.16, p.66–75, 2017.

SCHULZ, G. **The green and virtual data center**. Auerbach Publications, 2016.

SENAI. **Microcontrolador 8051**. Brasilia, 2014.

SOKOLOWSKI, J. A.; BANKS, C. M. **Modeling and simulation fundamentals**: theoretical underpinnings and practical domains. John Wiley & Sons, 2010.

SOKOLOWSKI, J.; TURNITSA, C.; DIALLO, S. A conceptual modeling method for critical infrastructure modeling. In: SIMULATION SYMPOSIUM, 2008. ANSS 2008. 41ST ANNUAL, ˙Anais... [S.l.: s.n.], 2008. p.203–211.

SOMASUNDARAM, G.; SHRIVASTAVA, A. **Armazenamento e gerenciamento de informações como armazenar, gerenciar e proteger informações digitais**. Bookman Editora, 2009.

STEINDER, M.; WHALLEY, I.; CARRERA, D.; GAWEDA, I.; CHESS, D. **Server virtualization in autonomic management of heterogeneous workloads**. [s.n.], 2007. 139–148p.

TAURION, C. **Cloud computing-computação em nuvem**. Brasport, 2009.

TIA-942. **Tia-942 data center standards overview**. 2012.

TURBAN, E.; SHARDA, R.; ARONSON, J. E.; KING, D. **Business Intelligence: um enfoque gerencial para a inteligência do negócio**. Bookman Editora, 2009.

VASSOLER, G. L.; RIBEIRO, M. R. An intelligent and integrated architecture for data centers with distributed photonic switching. , p.1–5, 2017.

VERAS, M. **Cloud Computing nova arquitetura da TI**. Brasport, 2012.

VISWANATHAN, H.; LEE, E. K.; POMPILI, D. Self-organizing sensing infrastructure for autonomic management of green datacenters. **Ieee Network**, v.25, n.4, 2011.

VOGEL, A.; GRIEBLER, D.; MARON, C. A.; SCHEPKE, C.; FERNANDES, L. G. Private IaaS clouds: a comparative analysis of opennebula, cloudstack and openstack. , Heraklion, Greece, p.672–679, 2016.

WU, W.; LIN, W.; PENG, Z. An intelligent power consumption model for virtual machines under CPU-intensive workload in cloud environment. **Soft Computing**, v.21, n.19, p.5755–5764, 2017.

XU, J.; ZHAO, M.; FORTES, J.; CARPENTER, R.; YOUSIF, M. On the Use of Fuzzy Modeling in Virtualized Data Center Management. , June 2007.

YOGENDRA, J.; PRAMOD, K. **Energy efficient thermal management of data centers**. Springer Science & Business Media, 2012.