FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Rogério Carvalho Rosa

SEGURANÇA FÍSICA EM DATACENTERS: UM ESTUDO DE CASO

Americana, S.P.

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Rogério Carvalho Rosa

SEGURANÇA FÍSICA EM *DATACENTERS*: UM ESTUDO DE CASO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob a orientação do Prof. Dr. Pedro Domingos Antoniolli.

Área de concentração: Segurança da Informação.

Americana, S.P.

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

R694s ROSA, Rogério Carvalho
Segurança física em datacenters: um estudo de caso. / Rogério Carvalho Rosa. – Americana: 2016.
55f.

Monografia (Curso de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Dr. Pedro Domingos Antoniolli

1. Comunicação de dados 2. Segurança em sistemas de informação I. ANTONIOLLI, Pedro Domingos II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Rogério Carvalho Rosa

SEGURANÇA FÍSICA EM *DATACENTERS*: UM ESTUDO DE CASO

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 09 de dezembro de 2016.

Banca Examinadora:

Pedro Domingos Antoniolli (Presidente)
Doutor
Faculdade de Tecnologia de Americana

Eduardo Antonio Vicentini (Membro)
Mestre
Faculdade de Tecnologia de Americana

Rodrigo Nogueira Tofani (Membro)
Especialista
Faculdade de Tecnologia de Americana

DEDICATÓRIA

Dedico este trabalho especialmente ao meu pai Sr. Sebastião P. Rosa, pelo apoio e dedicação dado a mim, para seguir em busca da concretização dos meus sonhos, mesmo não podendo mais estar presente.

AGRADECIMENTOS

Agradeço primeiramente a Deus que me proporcionou o desenvolvimento deste trabalho e por estar presente em todos os momentos de minha vida.

Ao professor Dr. Pedro Domingos Antoniolli pela orientação, e incentivo dispensado ao desenvolvimento deste trabalho.

Agradeço também a minha família, meus amigos e minha namorada, pelo amor e paciência durante meu processo de conclusão do curso.

Aos companheiros de sala, pelas trocas de conhecimento realizadas ao decorrer do curso.

RESUMO

A tecnologia vem avançando constantemente, aumentando o fluxo de dados, fazendo com que as empresas invistam ainda mais na área de Tecnologia da informação (TI). Visando um maior nível de disponibilidade e proteção dos dados, tem-se a necessidade de aprimorar o local físico de armazenamento das informações. O Datacenter é projetado para abrigar servidores, equipamentos de rede, equipamento de armazenamento e equipamento de telecomunicação. Com o aumento da demanda da utilização de Datacenters, o risco de perder informações se tornou maior. Por outro lado, cada vem mais os recursos tecnológicos estão sendo aprimorados com o objetivo de aumentar o nível de segurança e disponibilidade. Devido a importância do Datacenter para as empresas, o tema escolhido para esse trabalho foi um estudo de caso de um Datacenter, demonstrando pontos de falhas e apresentando melhorias para a infraestrutura do Datacenter, baseado nas pesquisas realizadas. Um Datacenter baseado nas normas e requisitos mínimos de segurança, podem obter uma certificação e classificação TIER e consequentemente tendem a possuir um nível de disponibilidade maior, conforme será apresentado ao decorrer desse trabalho.

Palavras-chave: *Datacenter*; Classificação *TIER*; Segurança da Informação.

.

ABSTRACT

Technology is constantly advancing, increasing the flow of data, making companies invest even more in the area of Information Technology (IT). Aiming at a higher level of availability and data protection, there is a need to improve the physical location of information storage. The Datacenter is designed to house servers, network equipment, storage equipment, and telecommunication equipment. With the increasing demand for the use of Datacenters, the risk of losing information has become greater. On the other hand, every time more technological resources are being improved with the aim of increasing the level of security and availability. Due to the importance of the Datacenter for the companies, the theme chosen for this work was a case study of a Datacenter, showing points of failure and presenting improvements to the Datacenter infrastructure, based on the research done. A Datacenter based on the minimum security standards and requirements can obtain a TIER certification and classification and therefore tend to have a higher level of availability as it will be presented in the course of this work.

Keywords: *Datacenter; TIER Classification; Information Security*

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANSI	*American National Standards Institute*
AWG	*American Wire Gauge*
BICSI	*Bulding Industry Consulting Service International*
CERTBR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CFTV	Circuito de câmeras fechado de televisão
EIA	*Eletronic Indistries Alliance*
EPO	*Emergency Power Off*
ERP	*Enterprise Resource Planning*
IBGE	Instituto Brasileiro de Geografia e Estatística
MTM	*Main-tie-main*
NEC	*National Electrical Code*
NFPA	*National Fire Protection Association*
PDU	*Power Distribuition Unit*
PNAD	Pesquisa Nacional por Amostra de Domicilio
QDC	Quadro de energia do *Datacenter*
QDG	Quadro de energia geral
TI	Tecnologia da Informação
TIA	*Telecommunications Industry Association*
UPS	*Uninterruptible Power Supply*
USP	Universidade de São Paulo

SUMÁRIO

1. INTRODUÇÃO

A tecnologia da informação (TI) tem evoluído de forma significativa ao longo dos anos. O Instituto Brasileiro de Geografia e Estatista – IBGE (2014) divulga o resultado da Pesquisa Nacional por Amostra em Domicilio – PNAD, na qual consta que mais de 49,4% da população brasileira possui acesso à *internet*. Essa realidade se torna ainda mais impactante nos ambientes empresarias, que têm transformado o jeito com que as empresas lidam com seus negócios, independentemente de seu tamanho. O processo de informatização dos negócios é algo que as empresas buscam crescentemente, seja através da implementação de sistemas mais complexos, como ERPs (dentre estes o SAP R3, o mais utilizado em empresas de grande porte), ou mesmo através da implementação de *softwares* mais simples, como planilhas eletrônicas.

Devido a este fato, constata-se que as empresas estão cada vez mais dependentes da TI, e cresce a preocupação com a Segurança da Informação, seja no tráfego da informação, ou mesmo em seu armazenamento.

A forma com que as empresas armazenam suas informações é muito importante, uma vez que anteriormente todos os dados era armazenamento em arquivos, dentro de pastas e de armários protegidos com chaves e cadeados. No entanto, com a evolução da tecnologia, foram adquiridos novos recursos como computadores, que começaram a ser utilizados para armazenar tais informações.

De acordo com a pesquisa global de Segurança da Informação realizada pela empresa PWC (2014), ano após ano, a informação tem sido um dos ativos mais valiosos que a empresa possui, tanto pelo conhecimento que tal informação traz, como também pela pronta aplicação dessa informação para apoio ao processo de tomada de decisão (TURBAN e VOLONINO, 2013). Assim, o comprometimento desses dados pode gerar grande perda financeira, interferindo diretamente no crescimento da empresa, e até mesmo ameaçando sua sustentabilidade e existência.

Este trabalho tem por problemática a busca de melhorias de segurança da informação voltada para a segurança física de *datacenters* de empresas de médio porte.

2. SEGURANÇA DA INFORMAÇÃO

2.1 SEGURANÇA

De acordo com Aurélio (2001), segurança consiste no ato ou efeito de segurar, proteger algo ou alguém com um conjunto de ações e recursos, mantendo a qualidade do que é ou está seguro, diminuindo riscos e perigos.

Portanto, segurança é a condição ou estado que se estabelece em um ambiente, utilizando medidas adequadas, e assegurando a boa conduta das atividades em um determinado local.

2.2 INFORMAÇÃO

Para Sêmola (2003, p.45), a informação é definida como:

> *Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas as operações que envolvam, por exemplo, a transferência de valores monetários).*
> *A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvo de proteção de segurança da informação.*

Entende-se por informação também todo o dado ou conteúdo que tenha valor para a organização, tornando-a um bem que deve ser protegido de forma adequada.

2.3 SEGURANÇA DA INFORMAÇÃO

Segundo a norma ISO/IEC 27002 (2013), segurança da informação é a proteção da informação contra vários tipos de ameaças, para garantir a continuidade de negócio, minimizar o risco para este negócio, maximizar o retorno sobre os investimentos, bem como as oportunidades de negócio. Para tanto, a segurança da informação pode ser obtida a partir de um conjunto de controles adequados, incluindo políticas, processos, procedimentos e estruturas organizacionais.

2.3.1 PILARES DA INFORMAÇÃO

Com base em ISO/IEC 27002 (2013), a Segurança da Informação possui princípios básicos:

Confidencialidade: Proteger a informação para que a mesma não esteja indisponível ou revelada a indivíduos, entidades ou processos não autorizados;

Integridade: Garantir a exatidão da informação, mantendo a informação no mesmo estado em que foi disponibilizada, impossibilitando a alterações acidentais ou indevidas;

Disponibilidade: A informação deve estar acessível e disponível quando a mesma receber uma demanda para utilização.

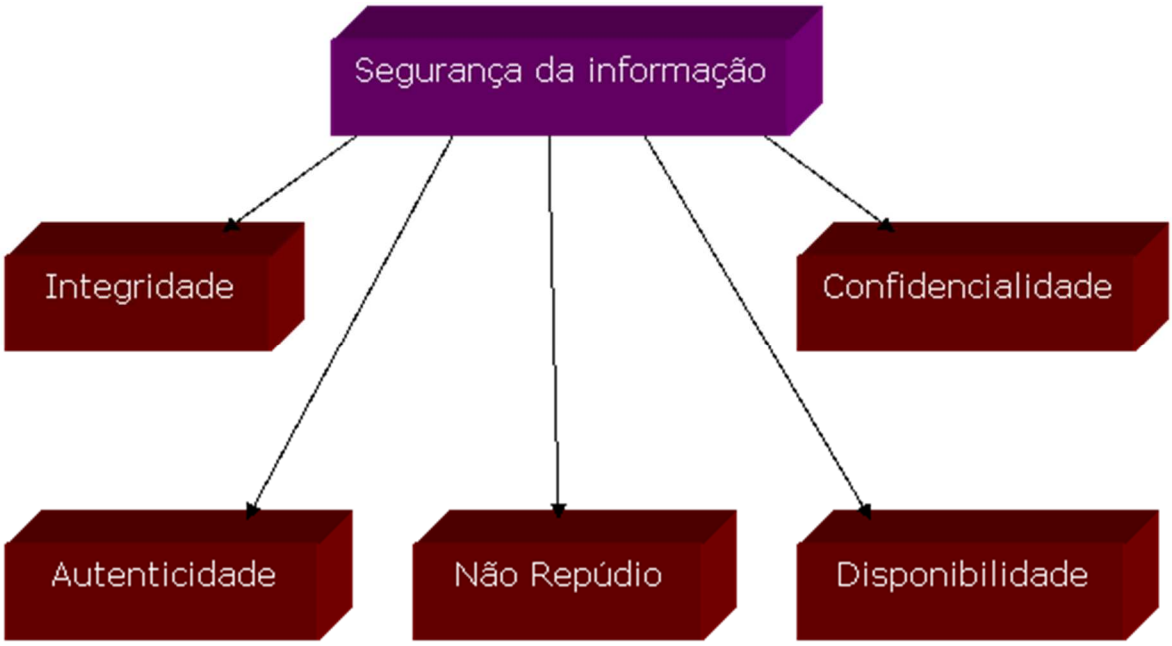
De acordo com a norma ISO/IEC 27001 (2013), a segurança possui outras propriedades importantes, tais como autenticidade e não repudio.

Autenticidade: Garante a identidade do usuário que produziu, modificou ou descartou a informação, assegurando que a informação é realmente da fonte que declara ser;

Não repúdio: Fornece provas para de que um determinado usuários realizou uma determina ação, garantindo que o usuário negue ter produzido, modificado ou descartado uma informação.

A Figura 1 apresenta as propriedades da Segurança da Informação, de acordo com ISO/IEC 27001 (2013).

Figura 1 – Pilares da Segurança da Informação



Fonte: Adaptado de ISO/IEC 27001 (2013)

Com base nos pilares da Segurança da Informação é possível definirmos a importância da informação dentro de uma organização, criando políticas de segurança para protege-las, no próximo capitulo será descrito os tipos de segurança existentes e qual melhor se adequa para cada empresa.

3. POLITICA DE SEGURANÇA

Uma política de segurança para a CERTBR (2003, p 6) é:

> *Um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade). A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham. Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem.*

Para Fraser (1997, p.7), política de segurança é:

> *Um documento formal que consiste em regras e procedimentos que descrevem como as pessoas que possuem acesso à informação, ou como os recursos tecnológicos, devem se comportar ao realizar uma determinada atividade.*

A segurança da informação tem como base a política de segurança, composta das normas regulamentadoras citadas acima (ISO), e que serão abordadas ao longo desse trabalho.

Campos (2006) afirma que a política de segurança não é um documento que irá informar tudo o que pode existir dentro de uma empresa relacionado à segurança da informação, nem mesmo regras gerais que se aplicam a qualquer aspecto de segurança da informação.

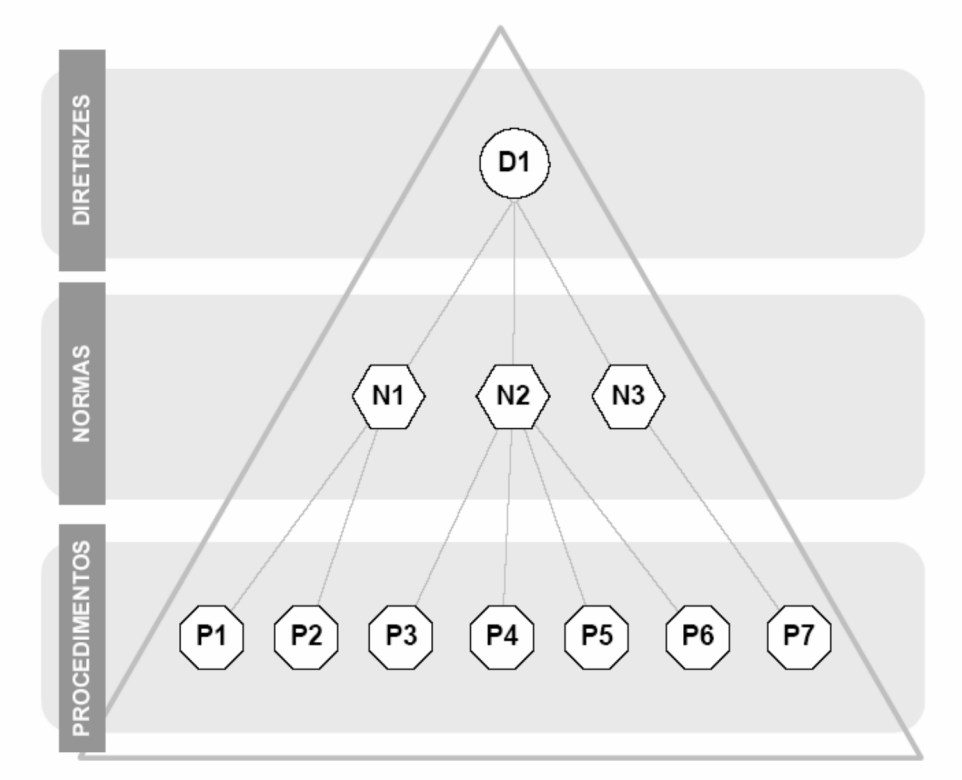
> *Mas afinal de contas o que significa a palavra política, que atualmente está sendo tão utilizada pelas corporações e instituições? Atualmente é comum ouvir frases do tipo "a política da nossa empresa é a qualidade total de nossos produtos", ou então "a política de recursos humanos não tolera funcionários que tenham registro policial". Esses são dois exemplos, mas que ajudam a entender o que significa a palavra política. A primeira frase é bastante abrangente e qualquer procedimento, ação ou decisão visando como objetivo a qualidade dos produtos fabricados, está de acordo com a política estabelecida pela empresa. Já a segunda frase é mais específica e deve ser considerada no processo de seleção e recrutamento de funcionários da empresa, conforme estabelecido na política de recursos humanos da empresa* (CAMPOS, 2006, p.100).

Referente à política de segurança, existe a mesma percepção, ou seja, ela deve conter um conjunto de regras para servir como primícias do comportamento das pessoas no tocante à segurança da informação, visando a proteção das informações e recurso tecnológicos da empresa.

A política de segurança deve prover o equilíbrio entre segurança e funcionalidade, definindo como a empresa irá monitorar, proteger e controlar suas informações e recursos. Segundo Dias (2000), é importante que na política sejam estabelecidas as responsabilidades e funções relacionadas à segurança, e que sejam discriminados os principais riscos, impactos e ameaças envolvidos. Dias (2000) reforça que uma política de segurança deve estar integrada às políticas institucionais da empresa, planejamento estratégico e metas.

Conforme a Figura 2, a política de segurança é um conjunto de diretrizes, compostas por normas/regras e seus procedimentos, que devem ser seguidas por seus utilizadores (CAMPOS, 2006).

Figura 2 - Estrutura de uma política de segurança da informação



Fonte: Campos (2006)

Os procedimentos (P) são instruções e coordenadas de como devem ser realizados determinadas atividades. Os procedimentos compõem as normas (N) que estabelecem os padrões de execução a serem seguidos, definindo as diretrizes (D) para uma política de segurança da informação (Campos, 2006).

3.1 TIPOS DE POLITICA DE SEGURANÇA

Para Ferreira (2003), existem três tipos de políticas de segurança, sendo elas a regulatória, a consultiva e a informativa.

- **Regulatória:** são consideradas como uma série de especificações legais, descrevendo com detalhes como executar determinada atividade, quem deve realizá-la, e fornecer algum tipo de parecer, informando porque tal ação é importante. Quando são impostas necessidades legais à organização, esse é o tipo de política utilizada;

- **Consultiva:** essa política auxilia os usuários na execução de uma determinada atividade, sugerindo métodos e ações que podem ser utilizados, provendo conhecimentos básicos relacionados às atividades dentro da organização, podendo evitar riscos na execução da mesma;

- **Informativa**: possui apenas caráter informativo, não tendo o mesmo rigor quanto à regulatória e consultiva, na qual não existem riscos se a mesma não for cumprida, porém pode contemplar advertências caso as informações contidas na política sejam ignoradas.

4. DATA CENTER

O *Datacenter* é uma estrutura física, sendo edifício ou parte de um edifício, projetado para abrigar uma variedade de recursos que fornecem armazenamento e gerenciamento de equipamentos de rede, servidores e telecomunicação.

Para Marin (2011), *Datacenters* são:

> *Ambientes que abrigam equipamentos responsáveis pelo processamento e armazenamento de informações cruciais para a continuidade de negócios nos mais variados tipos de organização, sejam empresas, instituições de ensino, indústrias, órgãos governamentais, hospitais, hotéis, entre outros (*MARIN, 2011*).*

E para a empresa Paloalto (2016), do ramo de Segurança da Informação, *Datacenter* é:

> *Uma instalação que centraliza as operações e o equipamento de TI de uma organização e onde ela armazena, gerencia e dissemina seus dados. Os datacenters abrigam os sistemas mais críticos de uma rede e são vitais para a continuidade das operações diárias. Consequentemente, a segurança e a confiabilidade dos datacenters e suas informações são uma prioridade para as organizações.*

4.1 NORMA ANSI/TIA-942

A *Telecommunications Industry Association* (TIA) é a principal associação comercial que representa a indústria da informação e da comunicação global de tecnologia, através do desenvolvimento de normas, iniciativas políticas, oportunidades de negócios, inteligência de mercado e eventos de rede (ANSI/TIA-942, 2005). Com o apoio de centenas de membros, a TIA melhora o ambiente de negócios para as empresas envolvidas em telecomunicações, *internet* banda larga, *internet* sem fio e móvel, tecnologia da informação, redes, cabeamento, satélites, comunicações unificadas, comunicações de emergência, e a ecologização da tecnologia. A TIA é credenciada pela *American National Standards Institute* (ANSI), uma instituição que supervisiona a criação, utilização e a publicação de diversas normas e diretrizes (ANSI/TIA-942, 2005).

De acordo com Veras (2009), a ANSI/TIA-942 é uma normal que especifica os requisitos mínimos para a infraestrutura de *Datacenters*, e os classifica em quatro níveis, de acordo com o nível de disponibilidade e redundância de sua infraestrutura. Esta norma destina-se a ser aplicável a qualquer *datacenter*, independente do seu tamanho.

Segundo a norma ANSI/TIA-942 (2005) existem quatro níveis de disponibilidade de infraestrutura do *datacenter*, sendo eles *TIER* I, *TIER* II, *TIER* III, *TIER* IV. Os níveis mais elevados não só correspondem à maior disponibilidade, mas também elevam os custos de construção e projetos desses *datacenters*. Em todos os casos, o *Datacenter* possui diferentes níveis de classificação para diferentes “partes” da sua infraestrutura. Por exemplo, um *datacenter* pode ser classificado como nível 3 para elétrica, mas como nível 2 em mecânica. No entanto, a classificação geral do *datacenter* será igual à classificação mais baixa entre todas as partes da infraestrutura. Assim, um *datacenter* que é avaliado como nível 4 para todas as camadas de infraestrutura, exceto para a elétrica, para o qual é classificado como nível 2, o mesmo, de forma geral, será classificado como nível 2 (*TIER* II), ou seja, a avaliação geral do *datacenter* é baseada em seu ponto mais fraco.

4.2 REDUNDÂNCIA

Os pontos únicos de falhas devem ser eliminados para que a redundância e a disponibilidade do *datacenter* aumentem (ANSI/TIA-942, 2005). A norma TIA-942 estabelece algumas nomenclaturas para as definições de redundância dos *datacenters*:

- **N:** Equipamento, caminho, serviço necessários e sem nenhuma redundância;

- **N+1:** Equipamento, caminho, serviço necessário mais um de redundância. Esse tipo de redundância não irá interromper a operação caso ocorrer a falha ou a manutenção em um único equipamento, caminho ou serviço.

  Ex.: Companhia de Energia Elétrica + *Nobreak*

- **N+2:** Equipamento, caminho, serviço necessário mais dois equipamentos, caminho, serviço de redundância. Esse tipo de redundância não irá interromper a

operação caso ocorra falha ou manutenção em algum dos equipamentos, caminhos e/ou serviços.

Ex.: Companhia de Energia Elétrica + *Nobreak* + Gerador

- **2N:** Dois equipamentos, caminho, serviço, se apenas um equipamento ocorrer falha ou manutenção, não ocasionará nenhum impacto na operação.

  Ex.: Companhia de Energia Elétrica A + Companhia de Energia Elétrica B

- **2(N+1):** Dois equipamentos, caminho, serviço, e mais redundância para cada um dos mesmos, tolerante a falha e nenhum impacto na operação.

  Ex.: Companhia de Energia Elétrica A + Companhia de Energia Elétrica B + *Nobreak* A+ *Nobreak* B + Gerador A + Gerador B.

  As instalações devem ser capazes de se manterem ativas, ou de serem testadas sem interromper a operação.

4.3. CLASSIFICAÇÃO DO DATA CENTER

De acordo com a norma ANSI/TIA-942 (2005) existem quatro níveis de classificação dos *Datacenters*, que variam de acordo com a sua infraestrutura e disponibilidade, conforme a Figura 3:

Figura 3 - Níveis de Datacenter

NÍVEIS DE *DATA CENTER* DE ACORDO COM A EIA/TIA-942

	Disponibilidade	***Downtime***	**Redundância, alimentação e resfriamento**	**Implementação**
Tier 1	99,671%	28,8 horas	Não possui	3 meses
Tier 2	99,741%	22 horas	Caminho único com componentes redundantes	3 a 6 meses
Tier 3	99,982%	1,6 hora	Múltiplos caminhos, mas só um ativo	15 a 20 meses
Tier 4	99,995%	0,4 hora	Múlitplos caminhos ativos	15 a 20 meses

Fonte: Zucchi (2013, p. 49).

4.3.1 DATA CENTER – *TIER* I (BÁSICO)

De acordo com a norma ANSI/TIA-942 (2005), o *Datacenter* classificado como *TIER* I está sujeito às interrupções em suas atividades, tanto planejadas quanto não planejadas. O mesmo possui quadro de distribuição de energia e refrigeração, mas pode ter ou não um piso elevado, *nobreak*, gerador (motor).

Se o *Datacenter* desse nível possuir um *nobreak* ou um equipamento de geração de energia, estes serão sistemas de módulos únicos, o que ocasionará muitos pontos de falhas. Para realizar a manutenção preventiva ou reparação dos equipamentos, os sistemas deverão ser desligados (ANSI/TIA-942, 2005).

Algumas situações de urgências, como erros de operação e falhas, podem contribuir para a paralização dos equipamentos, afetando diretamente a disponibilidade e funcionamento do *Datacenter.*

4.3.2 DATA CENTER – *TIER II* (COMPONENTES REDUNDANTES)

Com informações da norma ANSI/TIA-942 (2005), os *Datacenters TIER* II são um pouco menos suscetíveis às interrupções, tanto como atividades planejadas quanto não planejadas. Possuem piso elevado, *nobreaks* e geradores de motores, que possuem a estrutura de “Necessidade mais um” (N+1), porém em um único segmento. Quando se faz necessária a realização de uma manutenção, ocorre então o desligamento dos sistemas de energia do mesmo.

4.3.3 DATA CENTER – *TIER* III (PARALELAMENTE SUSTENTENTAVEL)

O *Datacenter TIER* III, possui equipamentos de refrigeração e alimentação de energia elétrica redundantes, porém com apenas um equipamento de cada segmento ligado, possibilitando atividades planejadas sem interromper a operação. O *TIER* III ainda está sujeito às falhas de operação e de componentes (ANSI/TIA-942, 2005).

Frequentemente os *datacenters* desse nível são preparados para serem atualizados para o nível acima, o *TIER* IV, caso o nível do negócio justifique o custo para essa atualização.

4.3.4 DATA CENTER – *TIER* IV (TOLERANTE A FALHAS)

O *Datacenter TIER* IV possui equipamentos de refrigeração e alimentação de energia elétrica redundantes e ativos, proporcionando uma tolerância a falhas (ANSI/TIA-942, 2005).

Todos os equipamentos presentes em um *TIER* IV devem possuir múltiplas entradas de energia, que devem funcionar normalmente com uma das entradas desligadas. Equipamentos que não são construídos com múltiplas entradas de energia devem utilizar uma chave de transferência automática para que não possua nenhum tipo de interrupção (ANSI/TIA-942, 2005).

O *TIER* IV possui capacidade de permitir qualquer tipo de atividade planejada sem nenhuma interrupção do *Datacenter*, pois os equipamentos de elétrica e refrigeração possuem redundância 2(N+1), o *TIER* IV terá tempo de inatividade apenas quando for acionado o alarme de incêndio, ou iniciado o desligamento de emergência (EPO), quando ocorrer algum desastre maior.

4.4 CLASSIFICAÇÃO DOS DATACENTERS POR ÁREA

De acordo com ANSI/TIA-942 (2005), as classificações dos *Datacenters* são formadas pela avaliação individual de quatro áreas, sendo elas Telecomunicações, Arquitetura, Elétrica e Mecânica. Cada uma dessas áreas possui também a classificação de quatro níveis *TIER* I, *TIER* II, *TIER* III e *TIER* IV, nos quais é baseada a classificação geral do *Datacenter*.

4.4.1 CLASSIFICAÇÃO NA ÁREA DE TELECOMUNICAÇÃO

Segundo a norma ANSI/TIA-942, a classificação da área de ***Telecomunicação*** para o *TIER* I possui um único caminho e uma sala de entrada, dedicada para os provedores de acessos (ANSI/TIA-942, 2005). A partir da sala de entrada, a distribuição dos serviços para a sala principal é realizada também por uma única via de comunicação com os demais equipamentos, sem nenhuma redundância física.

Todos os equipamentos devem ser identificados: cabeamento, tomadas, *racks*, com base na norma ANSI/TIA/EIA-606-A (2002).

Alguns pontos únicos de falhas de Telecomunicação *TIER* I são, de acordo com ANSI/TIA-942 (2005):

- Falhas nos sistemas ou equipamentos do provedor de acesso;
- Falha de manutenção no caminho e/ou sala dedicada aos provedores;
- Falha em equipamentos de rede, *switches* ou roteadores (caso não haja redundância);
- Um evento não planejado (catástrofe) pode ocorrer na sala de entrada ou na via de comunicação com a sala principal, interrompendo os serviços do Data Center.

Os requisitos para o *TIER* II da área de Telecomunicação são os mesmos do *TIER* I, mas os equipamentos críticos devem possuir redundância, como os equipamentos dos provedores, *switches*, roteadores incluindo fontes de alimentação e processadores redundantes. Redundâncias logicas podem ser configurados nos equipamentos de redes.

Segundo a norma ANSI/TIA-942 (2005), nesse nível é abordada a vulnerabilidade dos serviços de telecomunicações que entram no edifício. Adicionalmente, nesse nível é exigido um segundo caminho de entrada de serviços no qual os dois sejam interligados na sala de entrada. A recomendação da norma ANSI/TIA-942 é que esses dois caminhos estejam separados com uma distância mínima de 20 metros ao longo de toda a sua trajetória, e que cada caminho acesse a sala de entrada por um lado, mantendo a regra de distância mínima um do outro.

Alguns pontos únicos de falhas de Telecomunicação *TIER* II, de acordo com a normal ANSI/TIA-942 (2005), são:

- Os equipamentos dos provedores de acesso, ligados na mesma rede elétrica e apoiados por sistemas individuais de climatização, podem gerar indisponibilidade para os serviços do *Datacenter*, caso a energia elétrica venha a faltar ou o sistema de climatização falhar;

- Equipamentos dentro da sala principal ligados à mesma rede elétrica e apoiada por sistemas individuais de contingencia (*nobreak*), podem ocasionar problemas caso o nobreak e rede elétrica apresente alguma falhar;
- Um evento não planejado (catástrofe) pode ocorrer na sala de entrada ou na sala principal, ou no caminho de interligação das salas, e pode interromper os serviços do *Datacenter;*

Além dos requisitos dos níveis acima, o *TIER* III de infraestrutura de Telecomunicações deve ser servido por no mínimo dois provedores de acesso, os quais devem seguir a mesma regra de distância e de caminhos distintos (ANSI/TIA-942, 2005);

Este nível exige que o edifício possua duas salas de entradas, com a distância mínima de 20 metros uma da outra. Além disso, as salas não devem compartilhar os recursos de elétrica e climatização, e os equipamentos de ambas as salas devem estar preparados para continuar operando, mesmo que o equipamento da outra sala venha a falhar (ANSI/TIA-942, 2005).

Um outro ponto recomendado pela norma, e apontado pela empresa Furukawa (2016), é que todo o cabeamento e equipamentos, além de identificados, devem estar documentados, utilizando-se, por exemplo, planilhas.

Um dos pontos únicos de falha nesse nível, com base na norma ANSI/TIA-942 (2005), é que se um evento não planejado (catástrofe) ocorrer dentro da sala principal, pode interromper os serviços de todo o *Datacenter*.

A infraestrutura de Telecomunicações *TIER* IV deve, portanto, cumprir os requisitos do *TIER* III, além de possuir uma segunda sala principal, provisionando *backups* para os provedores de acesso e para os equipamentos críticos de rede, seguindo a mesma regra de, no mínimo, 20 metros de distância uma da outra. Além disso, com base na norma ANSI/TIA-942 (2005), as salas principais devem possuir sistemas de climatização, energia elétrica independentes, e serem tolerantes às falhas, não ocasionando impacto nos serviços do *Datacenter*.

Abaixo, na Tabela 1, os principais requisitos dos quatro níveis de classificação da infraestrutura de Telecomunicação (ANSI/TIA-942, 2005).

Tabela 1 – Requisitos da área de Telecomunicação por nível de classificação

TELECOMUNICAÇÃO	TIER 1	TIER 2	TIER 3	TIER 4
Cabeamento, racks, gabinetes e caminhos de acordo com as especificações	sim	Sim	sim	sim
Entradas Redundantes com uma separação mínima de 20 metros	não	Sim	sim	sim
Serviços de provedores de acesso redundantes	não	Não	sim	sim
Área de Distribuição Secundária	não	Não	não	opcional
Os roteadores e switches possuem fontes de alimentação e processadores redundantes	não	Sim	sim	sim
Múltiplos roteadores e switches para redundância	não	Não	sim	sim
Painéis de conexão, tomadas e cabos devem ser identificados de acordo com ANSI/TIA/EIA-606-A (2002)	sim	Sim	sim	sim
Patch cords devem ser identificados em ambas as extremidades	não	Sim	sim	sim
Documentação de interligação do cabeamento de acordo com a ANSI/TIA/EIA-606-A (2002)	não	Não	sim	sim

Fonte: Adaptado de ANSI/TIA-942 (2005)

4.4.2 CLASSIFICAÇÃO NA ÁREA DE ARQUITETURA

Marin (2011) afirma que para a área de **Arquitetura**, a estrutura deve ser construída de aço ou de concreto. Para a classificação *TIER* I de Arquitetura, sua estrutura não possui requisitos de proteção contra eventos físicos, eventos intencionais, acidentais, naturais ou falha humana. Além disso, a carga suportada em um *TIER* I deve ser de no mínimo 7,2 kPA, nas áreas dos equipamentos de acordo com a norma GR-63-CORE (ANSI/TIA-942, 2005).

Para o *TIER* II da área de Arquitetura, o *Datacenter* deverá possuir os mesmos requisitos do *TIER* I, e mais uma proteção mínima contra eventos físicos, eventos intencionais, acidentais, naturais ou falha humana (MARIN, 2011).

Ainda de acordo com o Marin (2011), as proteções mínimas são:

- Barreiras de vapor, nas paredes e tetos da sala principal dos equipamentos, para garantir o resultado dos equipamentos mecânicos que controlam o limite de umidificação do ar;
- Todas as portas devem ser de madeira maciça com armação de metal;
- Todas as paredes dever ser de altura total (do chão ao teto);
- Carga mínima suportada deve ser de no mínimo 8,4 kPA, nas áreas dos equipamentos de acordo com a norma GR-63-CORE.

O *TIER* III da área de Arquitetura deve cumprir todos os requisitos do *TIER* II (MARIN, 2011). Além disso, o *TIER* III possui um conjunto de proteções específicas contra eventos físicos, eventos intencionais, acidentais, naturais ou falha humana, sendo elas:

- Entradas redundantes no *Datacenter*;
- Acessos redundantes, com pontos de verificação para garantir o acesso separado de fornecedores e funcionários;
- Não devem possuir janelas no perímetro do *Datacenter*;
- A construção do *Datacenter* deve proporcionar proteção contra radiação eletromagnética. Construções de aço fornecem essa blindagem e, como solução alternativa, placas de alumínio podem ser embutidas nas paredes;
- Controle de acesso em todas as entradas, com acesso via *software* para monitorar e controlar o acesso à sala do *Datacenter*;
- A segurança dos *Datacenters*: devem ser protegidos por um sistema de detecção de intrusão (sensor de movimento e/ou infravermelho), e monitorado por circuitos de câmeras fechado de televisão (CFTV);
- Carga mínima suportada deve ser de no mínimo 12 kPA nas áreas dos equipamentos, de acordo com a norma GR-63-CORE;

Além dos requisitos do *TIER* III, o *TIER* IV da área de arquitetura deve possuir controle sobre todos os aspectos de suas instalações, incluindo um local externo ao prédio para uma unidade de gerador, e próximo ao mesmo deve existir uma área para armazenamento dos tanques de combustíveis utilizados pelo gerador (Marin,2011)).

As Tabelas 2, 3, 4 são destinadas às comparações dos quatro níveis de classificação da área de Arquitetura, com base na norma ANSI/TIA-942 (2005).

A tabela 2, possui comparações de níveis de classificação, baseadas no do local onde o datacenter se encontra (ANSI/TIA-942, 2005).

Tabela 2 - Requisitos da área de arquitetura (local) por nível de classificação

ARQUITETURA - LOCAL	TIER 1	TIER 2	TIER 3	TIER 4
Proximidade à área de perigo de inundação	sem exigência	Não dentro da área de perigo de inundação	Fora da área de risco de inundação de no mínimo 91até 100 metros da área de perigo	Fora da área de risco de inundação de no mínimo 100 metros da área de perigo
Proximidades de estradas e rodovias	sem exigência	sem exigência	Proximidade máxima de 91 a 100 metros	Distancia mínima de 0,8 km
Proximidade dos aeroportos	sem exigência	sem exigência	Proximidade máxima de 1,6 km	Distancia mínima de 8 km
Locais de estacionamento separados para visitantes e funcionários	sem exigência	sem exigência	Sim (fisicamente separados por cerca ou parede)	Sim (fisicamente separados por cerca ou parede)
Proximidade do estacionamento do visitante ao centro de dados paredes do edifício do perímetro	sem exigência	sem exigência	Proximidade máxima de 9,1 metros	Distancia mínima de 18,3 metros

Fonte: Adaptado de ANSI/TIA-942 (2005)

A tabela 3, possui comparações de níveis de classificação, baseadas na resistência da arquitetura datacenter contra incêndio (ANSI/TIA-942, 2005).

Tabela 3 - Requisitos da área de arquitetura (resistência ao fogo) por nível de classificação

ARQUITETURA – RESISTÊNCIA AO FOGO	TIER 1	TIER 2	TIER 3	TIER 4

Paredes de apoio externas com resistência ao fogo	sem exigência	sem exigência	1 hora mínima	4 horas mínimas
Paredes de apoio interiores com resistência ao fogo	sem exigência	sem exigência	1 hora mínima	2 horas mínimas
Pavimentos e tetos falsos com resistência ao fogo	sem exigência	sem exigência	1 hora mínima	2 horas mínimas
Cumprir os requisitos da NFPA 75	sem exigências	Sim	sim	sim
Componentes de construção				
Barreiras de vapor para paredes e teto da sala de computadores	sem exigência	Sim	sim	sim
Várias entradas de edifícios com pontos de verificação de segurança	sem exigência	sem exigência	sim	sim
Construção do *datacenter*	sem restrições	sem restrições	todo em aço	Todo em aço ou concreto
Altura do teto	2,6 metros no mínimo	2,7 metros no mínimo	3 metros no mínimo	3 metros no mínimo

Fonte: Adaptado de ANSI/TIA-942 (2005)

A tabela 4, possui comparações de níveis de classificação, baseadas na segurança da arquitetura datacenter contra incêndio (ANSI/TIA-942, 2005).

Tabela 4 - Requisitos da área de arquitetura (segurança) por nível de classificação

ARQUITETURA - SEGURANÇA	**TIER 1**	**TIER 2**	**TIER 3**	**TIER 4**

Tamanho da porta	mínimo de 1 metro de largura e 2,13 metros de altura	mínimo de 1 metro de largura e 2,13 metros de altura	mínimo de 1 metro de largura e 2,13 metros de altura, no *datacenter,* salas de eléctricas e mecânicas.	mínimo de 1,2 metro de largura e 2,13 metros de altura, no *datacenter,* salas de eléctricas e mecânicas.
Tipo da porta	sem exigência	Requisitos mínimos do norma	Preferencialmente madeira maciça com estrutura metálica	madeira maciça com estrutura metálica
Controle de acesso	sem exigência	Sim	Com sistema de relatórios	Com sistema de relatórios
Sem janelas exteriores no perímetro da sala de computadores	sem exigência	sem exigência	Sim	sim
Construção fornece proteção contra radiação eletromagnética	sem exigência	sem exigência	Sim	sim
Gravação do CFTV	sem exigência	sem exigência	Digital	digital

Fonte: Adaptado de ANSI/TIA-942 (2005)

4.4.3 CLASSIFICAÇÃO NA ÁREA DE ELÉTRICA

De acordo com a norma ANSI/TIA-942 (2005), a área de infraestrutura **Elétrica** de um *Datacenter* deve possuir uma distribuição primária pelas Companhias de elétrica. Os hospitais, durante uma interrupção, recebem alta prioridade, com o *Datacenter* não deve ser diferente. Preferencialmente, a alimentação deve ocorrer de modo subterrâneo, minimizando assim a exposição dos circuitos a raios, árvores, acidentes de transito, e vandalismo. Para o autor, o quadro de energia principal deve ser projetado visando crescimento, manutenção e redundância *main-tie-main* (MTM) (redundância automática para outro quadro, em caso de falha).

Para Veras (2009), a área de Elétrica inclui o sistema de geração de energia elétrica em *standby* (com redundância), que deve ser capar de fornecer energia elétrica de qualidade, e suprir toda a necessidade do *Datacenter* em caso de uma falha da Companhia de energia elétrica. Os geradores devem estar configurados para

fornecer a tensão e corrente de energia adequadas para os sistemas de fonte de alimentação ininterrupta (UPS), conhecidos como *nobreaks*.

No local onde os geradores ficarão instalados deverá ser fornecido equipamento para a refrigeração do ambiente, para que seja evitada a sobrecarga térmica e desligamento (VERAS, 2009).

Ainda de acordo com Veras (2009), o combustível utilizado nos geradores deverá ser o diesel, devido à sua combustão ser mais rápida do que gás natural. Controles do armazenamento devem ser tomados, e o reabastecimentos dos geradores deve ser monitorado para que não ocorram falhas, ocasionando a parada dos mesmos.

Referente ao sistema de UPS, o mesmo pode consistir em módulos individuais ou grupos de vários módulos paralelos. Sistemas de baterias podem ser fornecidos para cada modulo, ou para um grupo de módulos UPS (VERAS, 2009).

Quando um sistema de gerador é instalado, a principal função do sistema de UPS é suportar a operação do *Datacenter* até que os geradores entrem em operação. Teoricamente, a capacidade das baterias do sistema de UPS seria de segundos. No entanto, a norma ANSI/TIA-942 (2005) exige que a capacidade mínima seja de 5 a 30 minutos, devido a eventos imprevisíveis, que possam ocasionar falhas nos geradores. Assim, caso não haja geradores, a capacidade mínima do sistema de UPS deve ser de 30 minutos a 8 horas, tempo necessário para o desligamento ordenado dos equipamentos do *Datacenter*.

A estrutura de UPS deve possuir um sistema de monitoramento capaz de identificar a capacidade atual de armazenamento das baterias e gravar as tensões, impedância, ou resistência que passam para o sistema de UPS (ANSI/TIA-942, 2005).

Unidades de ar condicionado de precisão devem ser fornecidas para os sistemas de UPS, além das baterias. A expectativa de vida útil desses sistemas é afetada severamente pela temperatura (ANSI/TIA-942, 2005).

Sistema de Desligamento de Emergência (EPO) deve ser fornecido, conforme exigido pelo Código Elétrico Nacional (NEC). Sistema esse que possibilite o desligamento de todos os equipamentos, caso ocorra algum desastre, visando minimizar os dados causados aos mesmos. Adicionalmente, o sistema EPO deve estar ligado ao controle do alarme de incêndio, de acordo com a Associação Nacional de Proteção contra Incêndios (NFPA-70, 2002).

Referente ao sistema de aterramento e sistema de proteção contra raios, todos os equipamentos devem possuir, inclusive, a construção do edifico, de acordo com a guia de análise de riscos incluída na norma ANSI/TIA/EIA-J-STD-607-A (2002), que leva em conta a localização geográfica e construção civil.

A infraestrutura do *Datacenter* deve possuir os seguintes aterramentos, com base na normal ANSI/TIA/EIA-J-STD-607-A (2002):

- 1 AWG (unidade de medida Americana), ou condutor de capacidade maior para aterramento de acordo com a ANSI/TIA/EIA-J-STD-607-A (2002);
- 6 AWG, ou condutor de capacidade maior para equipamentos de climatização;
- 4 AWG, ou condutor de capacidade maior para cada coluna da sala de informática;
- 6 AWG, ou condutor de capacidade maior a cada escada cabo, bandeja de cabos, e sala de condutor de cabo entrar;
- 6 AWG, ou condutor de capacidade maior para cada conduta, tubulação de água, e sala de entrada do duto;
- 6 AWG, ou condutor de capacidade maior para cada computador ou telecomunicações armário, *rack* ou quadro. Não unir prateleiras, armários e quadros em série.

Abaixo, na Tabela 5, a conversão da unidade de medida AWG para milímetros (mm):

Tabela 5 - Unidades de medidas

Número AWG	Diâmetro				Seção	
	fio nu		esmaltado			

Fonte: Nexans (2013)

Esses requisitos da área de elétrica estão de acordo com o IEEE Standard 1100 (2005) – Práticas recomendas para aterramento de equipamentos eletrônicos e IEEE Standard 446 (1995) – Praticas recomendas para Sistema de emergência e de espera (*standby*), para aplicações industriais e comerciais.

Após esses requisitos, é possível definir o os *TIERs* da área de Elétrica. Para o *TIER* I fornecer o mínimo de distribuição de energia para atender os requisitos da carga elétrica do *Datacenter*, ele deve possui pouco ou nenhum tipo de redundância, ocasionando a paralisação dos serviços caso ocorra alguma falha (ANSI/TIA-942, 2005). No *TIER* I podem ser utilizados geradores e sistemas de UPS, porém estes são sistemas de módulos únicos, e sem redundância. Em relação ao aterramento, o mesmo não é necessário, mas pode ser desejável para atender aos requisitos dos fabricantes dos equipamentos, dentro do *Datacenter*.

O *TIER* II da área de Elétrica deve atender todos os requisitos do *TIER* I e possuir sistema de UPS N+1, e o sistema de gerador para suportar toda a operação (ANSI/TIA-942, 2005). Para o sistema de gerador não é necessária redundância. Nesse nível, devem ser contempladas duas unidades de distribuição de energia (PDU) para cada *rack* dentro do *Datacenter.* Cada *rack* deve possuir seu próprio circuito (um

de cada PDU). Em todos os *racks* devem estar identificados de qual circuito/PDU se origina a energia recebida. É necessário o aterramento para o *TIER* II, e o mesmo deve possuir sistema de desligamento de emergência (EPO).

Para o *TIER* III da área de Elétrica, de acordo com a norma ANSI/TIA-942 (2005), o mesmo deve atender todos os requisitos dos *TIER* II, além de possui redundância N+1 em todos os equipamentos de elétrica, incluindo geradores e sistemas de UPS e companhia de elétrica, utilizando o *main-to-main* (MTM) (conversão automática entre as companhias de elétrica). O armazenamento mínimo de combustível deve ser capaz de fornecer 72 horas de funcionamento para o sistema de UPS.

Adicionalmente, com base em Veras (2009), todos os equipamentos do *Datacenter* devem possuir fontes redundantes, e os que não possuem devem utilizar conversão automática, incluindo equipamentos que suportam a área de elétrica como equipamentos de refrigeração.

Veras (2009) argumenta que um sistema de monitoramento deve ser contemplado para monitorar os principais equipamentos elétricos, como os sistemas de geradores, UPS, companhias de energia elétrica e gerenciar o sistema mecânico, otimizando a eficiência e utilização dos mesmos gerando indicadores e alarmes de condições atuais.

Para o ultimo nível da área de Elétrica, o *TIER* IV exige, além dos requisitos do *TIER* III, que todos os equipamentos possuam redundância 2(N+1), fazendo com que qualquer falha que ocorra, automaticamente a carga seja migrada para o outro equipamento, não gerando nenhum impacto para a operação (ANSI/TIA-942, 2005).

A seguir, com base na normal ANSI/TIA-942 (2005), a tabela 6, comparativos entre os níveis de classificação da área de Elétrica:

Tabela 6 - Requisitos da área de elétrica (sistema de UPS e geradores) por nível de classificação

ELÉTRICA	TIER 1	NÍVEL 2	TIER 3	TIER 4

Caminho de entrada de energia elétrica	único	Único	redundante	redundante
Sala de elétrica	única	Única	redundante	redundante
Sistema permite a manutenção simultânea	não	Não	sim	sim
Capacidade gerador de combustível (a plena carga)	8 horas	24 horas	72 horas	96 horas
nível de redundância do sistema de UPS	N	N + 1	N + 1	2N
Monitoramento dos sistema de UPS via central de monitoramento	não	Não	sim	sim
Programa de Teste / Inspeção de Carga Total da Bateria	a cada dois anos	a cada dois anos	a cada dois anos	a cada dois anos ou anualmente
Tanques de combustível em salas externas	não	não	sim	sim
Dimensionamento do gerador	dimensionado para sistemas de computadores e telecomunicações somente elétricos e mecânicos	dimensionado para sistemas de computadores e telecomunicações somente elétricos e mecânicos	dimensionado para sistemas de computadores e telecomunicações somente elétricos e mecânicos com redundância	dimensionamento para todos os sistema da empresa com redundância
Sistema individual de aterramento no gerador	não	Sim	sim	sim
Teste de todo os sistema UPS e geradores	não	não	não	sim
Equipe de manutenção	no local em apenas manutenções ou alterações e de plantão nos demais momentos	no local em apenas manutenções ou alterações e de plantão nos demais momentos	24 horas por dia no local e plantão aos finais de semana	no local 24 horas por 7 dias da semana
Manutenção preventiva	não	Não	manutenção limitada	manutenção completa

Fonte: Adaptado de ANSI/TIA-942 (2005)

4.4.4 CLASSIFICAÇÃO NA ÁREA DE MECÂNICA

A última área que comtempla a classificação geral do *Datacenter* é a área de **Mecânica**. A área de sistemas mecânicos é composta por sistemas de climatização e sistemas de proteção contra incêndio (ANSI/TIA-942, 2005).

O controle da temperatura do *Datacenter* é de extrema importância, pois o calor compromete a eficiência dos equipamentos, além de diminuir a vida útil do mesmo (ANSI/TIA-942, 2005).

Segundo Vera (2009) O sistema mecânico deve ser capaz de atingir as temperaturas de 20° C a 25°C e a umidade relativa do ar dever ser controlada entre 45% e 55%. De forma geral, o controle de umidade e temperatura é realizado através de uma combinação de condicionadores de ar. O grande desafio é manter o ambiente nessas condições, visto que seu funcionamento é ininterrupto. Os sistemas de água gelada são mais adequados para centros de dados maiores. Unidades convencionais podem ser mais convenientes para os *Datacenters* menores, pois não requerem tubulações a serem instaladas.

O sistema de ar condicionado deve ser projetado para fornecer a temperatura e condições de humidade recomendadas pelos fabricantes dos servidores a serem instalados dentro do *Datacenter*, alguns equipamentos com altas cargas de calor podem exigir condutas de ar ou pisos de acesso para fornecer o resfriamento adequado (veras, 2009).

Para definir o sistema de proteção contra incêndio é preciso analisar os fatores de risco do *Datacenter* (ANSI/TIA-942, 2005). Essa analise pode ser dividida em quatro partes principais. A primeira é a questão da segurança de pessoas ou propriedades afetadas pela operação (ex.: sistemas de suporte de vida, telecomunicações, controles do sistema de transporte, controles de processo), a segunda é a ameaça de fogo para os ocupantes em áreas confinadas ou a ameaça à propriedade exposta (ex.: registros, armazenamento em disco), a terceira é a perda econômica do negócio devido ao tempo de inatividade e, por último, é a perda do valor do equipamento (ANSI/TIA-942, 2005).

Segundo Marin (2011) existem sistemas de detecção de alerta precoce, para evitar os danos e perdas que podem ocorrer durante os estágios iniciais de um incêndio. Um sistema de detecção de fumaça por aspiração fornece proteção para o Data Center, salas mecânicas e salas elétricas, este sistema possuem uma sensibilidade e capacidade de detecção muito além do que os detectores convencionais, o mecanismo de detecção convencional requer uma quantidade muito maior de fumaça antes mesmo de detectar um incêndio e essa diferença pode ser crucial para combater e interromper um incêndio em um Data Center.

Há, no entanto, vários sistemas de alerta precoce de acordo com a empresa Furukawa ([s.d]), sistemas de detecção de amostragem de ar que utilizam ionização convencional ou detectores fotoelétricos. Existem também detectores de fumaça à base de *laser* que não utilizam amostragem de ar e não fornecem um nível equivalente de detecção de alerta precoce para sistemas de detecção de amostragem de ar.

De acordo com Marin (2011), um sistema de extinção de incêndios de pré-ação fornece o próximo nível de proteção para o *Datacenter*, pois proporciona um nível mais elevado de confiabilidade e mitigação de riscos. O sistema de pré-ação com tubulação a água entrará em ação quando o sistema de detecção de fumaça indicar que há um evento em andamento. Uma vez que a água é liberada na tubulação, são ativados os *sprinklers* para combate ao incêndio.

Um sistema de supressão de incêndio de agente limpo fornece o mais alto nível de proteção para o *Datacenter*, salas elétricas e mecânicas (Marin, 2011). Este sistema seria instalado além dos sistemas de pré-ação e detecção de fumaça. O sistema de supressão de incêndio é projetado, após ativação, para que o gás de agente limpo inunde totalmente a sala. Este sistema é constituído por um gás não tóxico que é superior à proteção por aspersão de várias formas. Em primeiro lugar, o agente pode penetrar os equipamentos para extinguir incêndios, em segundo lugar, ao contrário dos *sprinklers*, não há resíduo do gás para ser removido após a ativação do sistema (ANSI/TIA-942).

Por fim, este agente permite que o fogo seja extinto sem prejudicar os outros equipamentos não envolvidos no incêndio. Portanto, usando a supressão gasosa o

Datacenter poderia retornar facilmente à operação após um evento com atraso mínimo e a perda seria limitada apenas aos itens afetados (Marin, 2011).

A *National Fire Protection Association* (NFPA) recomenda que o equipamento eletrônicos e de climatização sejam automaticamente desligados no caso de acionamento dos sistemas de supressão. Embora o raciocínio por trás disso seja diferente, os equipamentos eletrônicos podem muitas vezes serem recuperados após o contato com água, desde que tenham sido desenergizados antes do contato. O desligamento automático é recomendado principalmente para salvar o equipamento.

De acordo com a NFPA 75 (2003), é recomendável que o *Datacenter* possua também um extintor de incêndio de agente limpo, pois evita o pó químico dos extintores comuns, que podem afetar os equipamentos associados ao incêndio, de forma significativa.

A classificação da área de Mecânica, para o *TIER* I, inclui unidade de ar condicionado simples com a capacidade de resfriamento para manter a temperatura crítica do espaço e umidade relativa do ar, sem unidades redundantes. Como se trata de um único equipamento, uma falha ou manutenção causará interrupção parcial ou total no sistema de ar condicionado. Caso o *Datacenter* possua um gerador, todos os equipamentos de ar condicionado devem ser alimentados pelo gerador (ANSI/TIA-942, 2005).

No *TIER* II segundo a norma ANSI/TIA-942 (2005), além dos requisitos do *TIER* I, na área de mecânica o sistema de climatização deve possuir várias unidades de ar condicionado com a capacidade combinada de resfriamento para manter a temperatura crítica do espaço e a umidade relativa nas condições de projeto, com uma unidade redundante N+1.

Os sistemas de ar condicionado devem ser projetados para operação contínua 7 dias / 24 horas / 365 dias / por ano (ANSI/TIA-942, 2005).

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

alimentados através de circuitos dedicados e redundantes do UPS (ANSI/TIA-942, 2005).

Segundo Marin (2011), o sistema de climatização em um *TIER* III deve possuir os requisitos do *TIER* II, e incluir várias unidades de ar condicionado com a capacidade de resfriamento combinada para manter a temperatura crítica do espaço e a umidade relativa em condições de projeto, com unidades redundantes suficientes para permitir a falha ou o serviço de um quadro elétrico. Este nível de redundância pode ser obtido quando fornecidas duas fontes de energia para cada unidade de ar condicionado, dividindo-se o equipamento de ar condicionado entre várias fontes de energia (ANSI/TIA-942).

Para Veras (2009), os equipamentos de refrigeração do *Datacenter* devem possuir redundância N+2, para que o sistema não seja afetado com nenhum tipo de falha ou manutenção.

Com base na norma (ANSI/TIA-942, 2005), para o *TIER* IV da área de Mecânica, o mesmo deve possuir todos os requisitos do *TIER* III, porem com redundância 2(N+1).

Na tabela 7, as comparações entre os *TIER*s e seus respectivos requisitos da área de Mecânica:

Tabela 7 - Requisitos da área de elétrica (sistema de climatização e combate a incêndio) por nível de classificação

MECANICA	TIER 1	TIER 2	TIER 3	TIER 4

Tubulação próximo ao datacenter	permitido mas não recomendado	permitido mas não recomendado	não permitido	não permitido
Sistemas de climatização ligados aos gerador principal e reserva	sem exigência	Sim	sim	sim
Unidade de ar condicionados internos	sem redundância	uma unidade redundante por área critica	unidades de ar condicionado, suficientes para manter a área crítica durante a perda de uma fonte de energia elétrica	unidades de ar condicionado, suficientes para manter a área crítica durante a perda de uma fonte de energia elétrica
Controle de humidade relativa do ar	sim	Sim	sim	sim
Fonte de energia elétrica redundantes para o sistema de climatização	não	Não	sim	sim
Sistema de detecção de incêndio	não	Sim	sim	sim
Sistema de extintores de incêndios	quando solicitado	pré-ação (quando necessário)	pré-ação (quando necessário)	pré-ação (quando necessário)
Sistema de supressão gasosa	não	No	Agentes limpos listados na NFPA 2001	Agentes limpos listados na NFPA 2001
Sistema de Detecção de Fumaça de Aviso Precoce	não	Sim	sim	sim
Sistema de detecção de vazamentos de água	não	Sim	sim	sim

Fonte: Adaptado de ANSI/TIA-942 (2005)

5. QUEM CERTIFICA E CLASSIFICA UM DATACENTER?

A *Uptime Institute* é mundialmente reconhecida pela criação e administração dos rigorosos *TIER Standards & Certifications*, que permitem que *Datacenters* alcancem sua missão, enquanto atenuam o risco. É uma Organização que está atuando há mais de 20 anos no mercado (*UPTIME INSTITUTE*, 2016).

A *Uptime Institute* presta serviços de consultoria, ajudando as empresas a desenvolver, criar, lançar e gerenciar operações de *Datacenters*. Esta empresa é focada em aprimorar o desempenho, a eficiência e a confiabilidade da infraestrutura fundamental para os negócios que estão na base da economia da informação global. A consultoria serve todos os responsáveis pela disponibilidade de serviços de TI: operadores empresariais e de terceiros, proprietários, fabricantes, fornecedores e profissionais. No Brasil existe um diretor executivo responsável para prestar a consultoria e orquestrar a certificação de um *datacenter*.

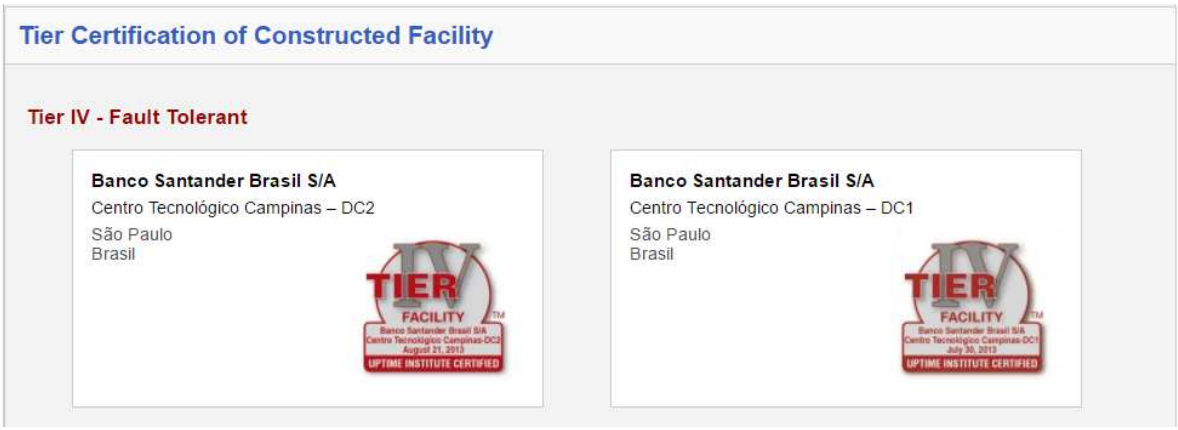
Abaixo, na Figura 4, um mapeamento de todos os países que possuem *Datacenters* certificados pela *Uptime Institute*:

Figura 4 - Mapa de países com Datacenters certificados pela Uptime Institute.

Fonte: Uptime Institute (2016)

No Brasil, há dois *Datacenters TIER* IV certificados pela *Uptime Intitute* conforme Figura 5:

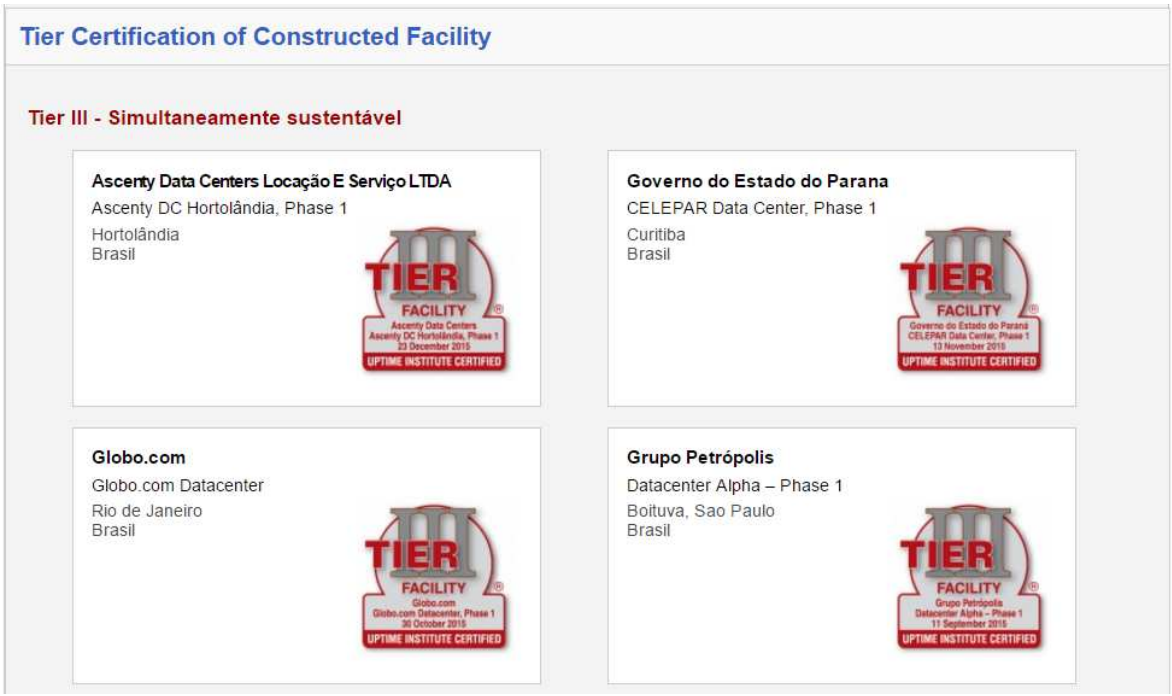
Figura 5 - Datacenters *TIER* IV no Brasil



Fonte: Uptime Institute (2016)

A Figuras 6 apresentam quatro *Datacenters TIER* III certificados pela *Uptime Institute* no Brasil.

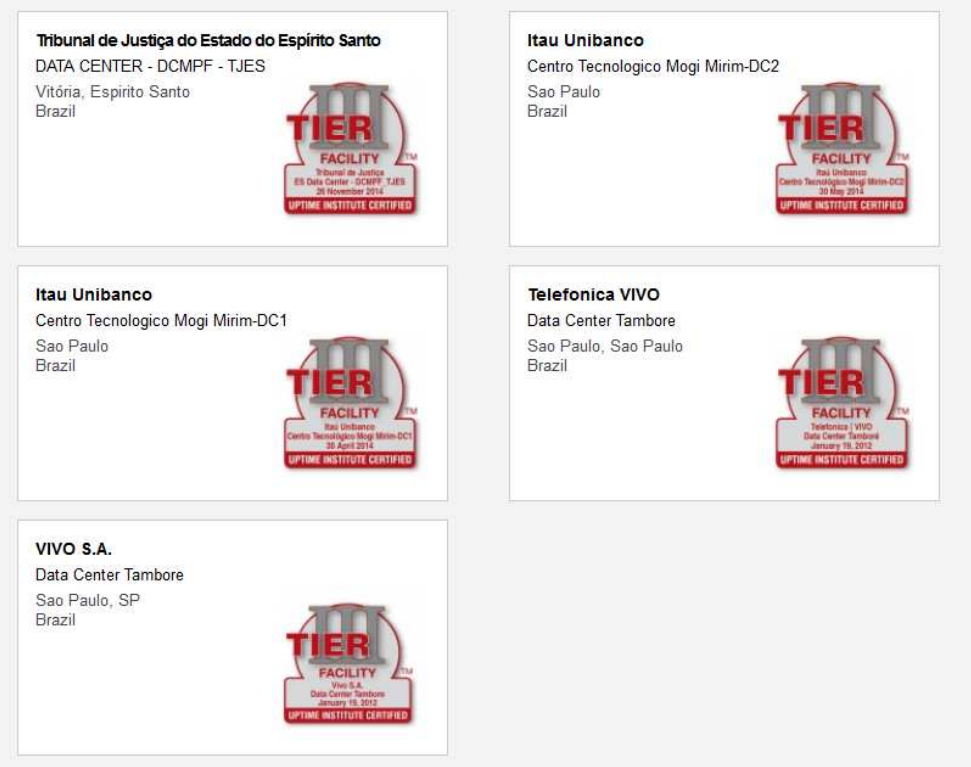
Figura 6 – Datacenters *TIER III* no Brasil



Fonte: Uptime Institute (2016)

A Figuras 7 apresenta outros *Datacenters TIER* III certificados pela *Uptime Institute* no Brasil.

Figura 7 - Outros Datacenters TIER III no Brasil



Fonte: Uptime Institute (2016)

Segundo Marin (2011), foi publicado em 2005 uma norma norte-americana ANSI que define as classificações de *Datacenters* em função da disponibilidade e redundância. A norma ANSI/BICSI-002 (Projeto de *Datacenter* e Melhores Práticas de Implementação), publicada em março de 2011, com cinco classificações de disponibilidade de *Datacenter*, F0 a F4, sendo a F0 a classe mais básica e a F4 a classe mais tolerante as falhas.

Porém segundo Marin (2011), a norma que se aplica para a infraestrutura de um *Datacenter*, de acordo com a sua disponibilidade e a sua redundância é a ANSI/TIA-942 (2005), a norma ANSI/TIA-942 (2005) é mais utilizada e é a única que aplica o conceito de *TIERs* (desenvolvido pelo *Uptime Institute*) para a classificação de *Datacenters*.

6. ESTUDO DE CASO

Com liderança no mercado em seu seguimento, a Organização a ser estudada nesse trabalho, denominada aqui como Empresa X, para ocultar sua identidade, iniciou suas atividades há mais de trinta anos, e hoje possui mais de 13 mil colaboradores no mundo.

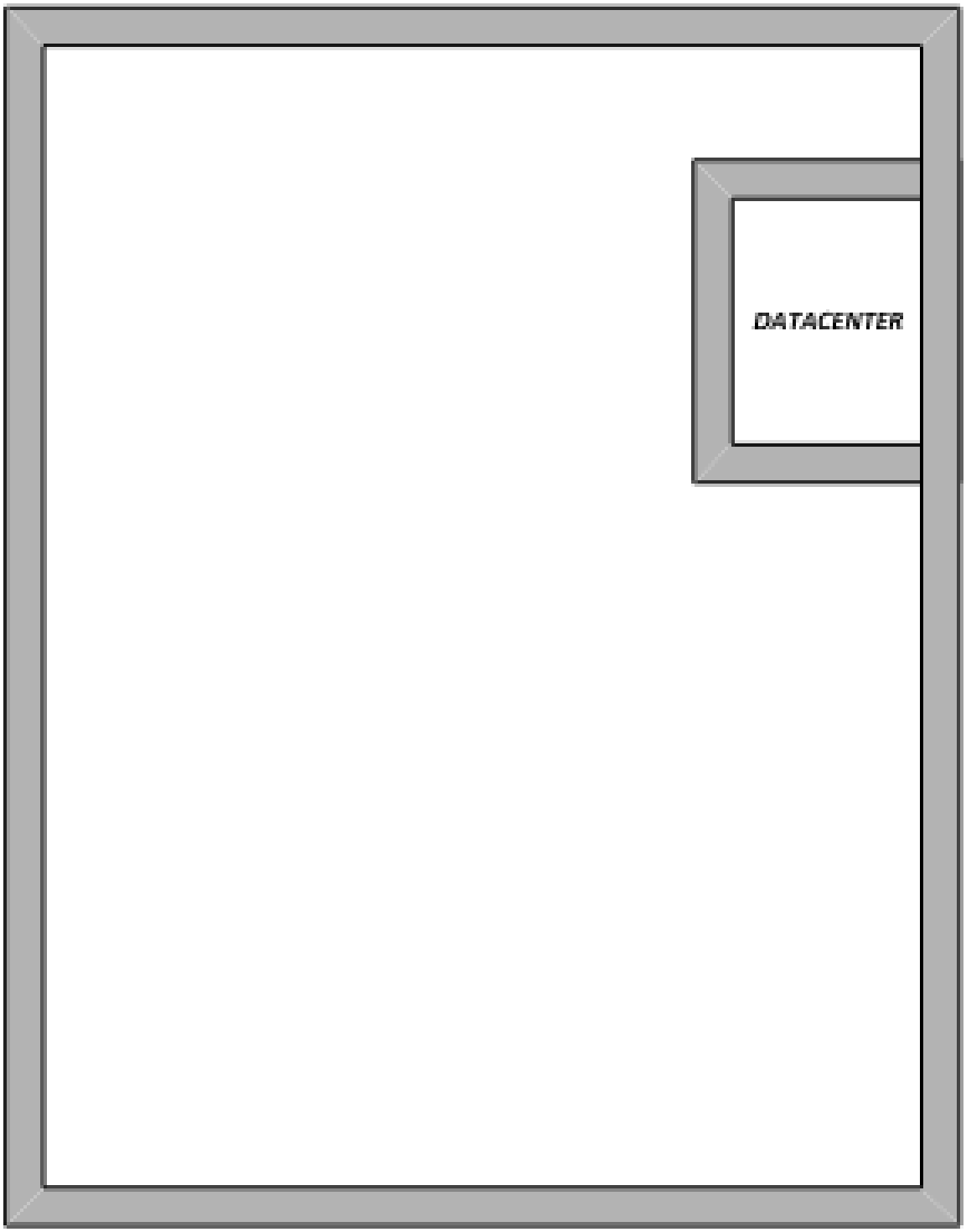
A empresa X está situada localizado em diversos estados do Brasil, oferecendo diversos produtos e soluções para seus clientes.

A área de TI da Empresa X é divido em três áreas, a primeira área de telecomunicações, responsável rede e telefonia de todas as unidades; a segunda área, a do Datacenter, responsável por todos os servidores da empresa e, por último, a área de operações, responsável pela manutenção e *backup* de toda a informação da empresa. Em todas as unidades há profissionais das três áreas, e todos os profissionais atuam em todas as unidades, eliminando qualquer dependência de um profissional.

Todas as áreas de TI possuem responsabilidades com a segurança da informação, que deve estar em *compliance* com as normas recebidas da matriz do Reino Unido. O estudo de caso é baseado na pesquisa bibliográfica realizada, no conhecimento adquirido e por conveniência, ou seja, com a participação do pesquisador como colaborador da Empresa X. Dessa forma, será analisado o cenário e toda a infraestrutura existente hoje na Empresa X, identificando os possíveis pontos de falhas.

Hoje o *Datacenter* da empresa está localizado no 1º andar do edifício, conforme apresentado na Figura 8, na qual pode-se visualizar sua localização no andar.

Figura 8 - Planta 1º Andar



Fonte: Adaptado da planta do 1º Andar da empresa

Baseado na pesquisa bibliográfica realizada, a primeira área de classificação de um *Datacenter* é a área de Telecomunicação. Esta área hoje, no *Datacenter* da

empresa, possui um único caminho para entrada de serviços. Os *links* de *internet* e de voz possuem redundância de operadoras (*Link* principal Operadora A + *Link* de redundância Operadora B). O caminho para esses *links* chegarem até a entrada da empresa é totalmente aéreo. A partir da entrada da empresa, o caminho se torna subterrâneo. Com essa infraestrutura atual existem riscos e pontos de falhas.

Os equipamentos dos provedores de serviços não possuem equipamentos de redundância e/ou fontes de alimentações redundantes. Todos os equipamentos considerados críticos e de responsabilidade da empresa, como *switches*, roteadores, possuem redundância física e logica, e todos possuem fontes de alimentação redundantes.

Hoje apenas o cabeamento atual dentro da *Datacenter* está identificado. Os demais equipamentos, tomadas, *racks*, quadros de energia, não estão identificados conforme informando pela norma TIA/EIA-606-A (2002).

Alguns pontos únicos de falhas na área de Telecomunicação do *Datacenter* da empresa são:

- Falha nos equipamentos dos provedores de serviços;
- Falha de manutenção no caminho de entrada dos serviços;
- Evento não planejado (catástrofe) pode ocorrer no caminho de entrada dos serviços;
- Cabeamento aéreo sujeito a acidentes e vandalismos;

Qualquer um dos eventos acima, se ocorrerem podem interromper os serviços do *Datacenter*.

Referente à segunda categoria de classificação, a área de Arquitetura do datacenter, é possível observar na Figura 9, e identificar que o *Datacenter* está localizado ao lado de um banheiro, um local onde possui tubulações de água.

Atualmente o *Datacenter* possui janelas externas, reduzindo o nível de proteção e aumentando a temperatura do ambiente, deixando de estar em conformidade com a norma ANSI/TIA-942.

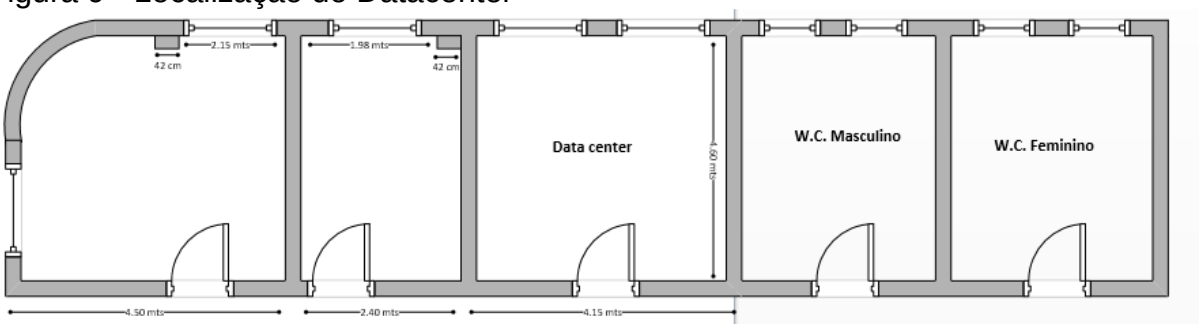
O acesso ao *Datacenter* é único, através de uma porta de vidro, e sem nenhum sistema de controle de acesso via *software*. O acesso ao *Datacenter* é monitorado por uma empresa terceira, através de circuitos de câmeras (CFTV).

Além dos itens citados acima, o *Datacenter* não possui piso elevado, dificultando a passagem de novos cabos, e organização dos mesmos.

Alguns pontos únicos de falhas na área de Arquitetura de *Datacenter* da empresa são:

- Caso alguma tubulação de água apresente falha (vazamentos), pode-se gerar riscos e danos aos equipamentos e a sala do Datacenter;
- Falha no circuito de câmeras, faz com que nenhum tipo de registro de quem acessou o Datacenter exista;
- Frágil proteção devido à existência de porta de vidro e janelas no Datacenter;

Figura 9 - Localização do Datacenter



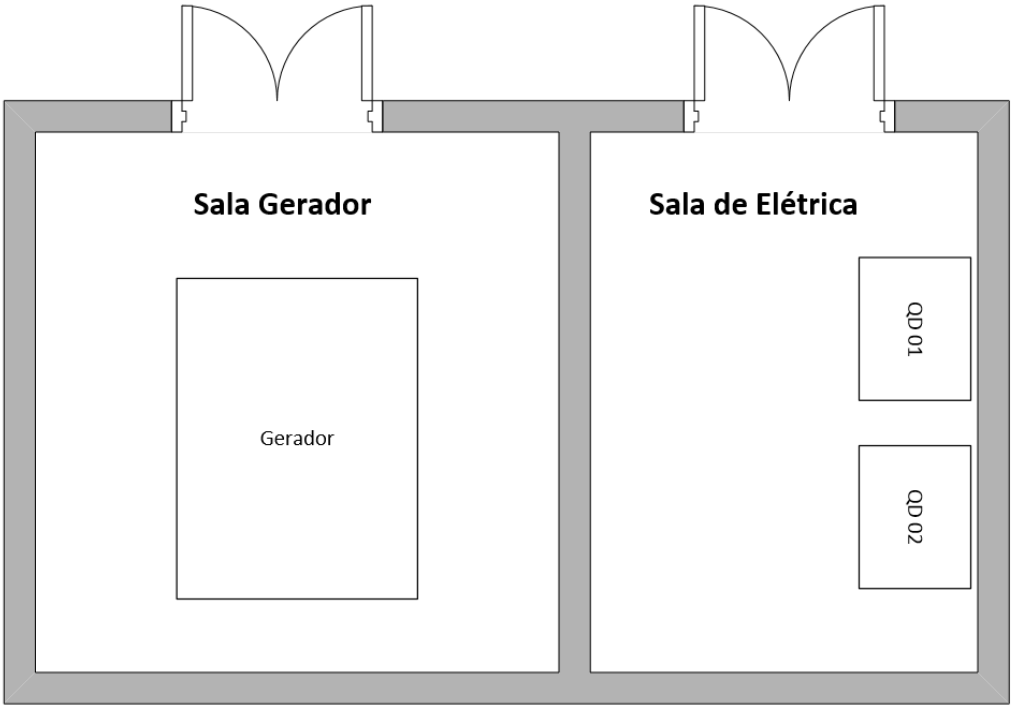
Fonte: Próprio Autor

A terceira categoria de classificação do *Datacenter*, a área de elétrica, hoje é composta pela Companhia de energia elétrica da cidade, e possui um modulo único gerador a óleo diesel, e um sistema único de UPS.

A Companhia fornece a energia através de cabeamento aéreo até a entrada única da empresa. A partir da entrada da empresa todo o cabeamento é subterrâneo até a sala de entrada de energia elétrica, localizada a 20 metros do prédio onde se encontra o *Datacenter*. A sala não possui nenhum equipamento para a climatização do ambiente onde estão os quadros de energia.

Conforme a Figura 10, o gerador se encontra ao lado da sala de entrada de energia elétrica. O gerador é abastecido por óleo diesel, e todo o combustível reserva está em uma sala dedicada, próxima ao gerador. O gerador é responsável por gerar energia para todo prédio, inclusive para o *Datacenter*, caso a Companhia de energia elétrica venha a falhar. A sala do gerador não possui nenhum tipo de climatização de ambiente.

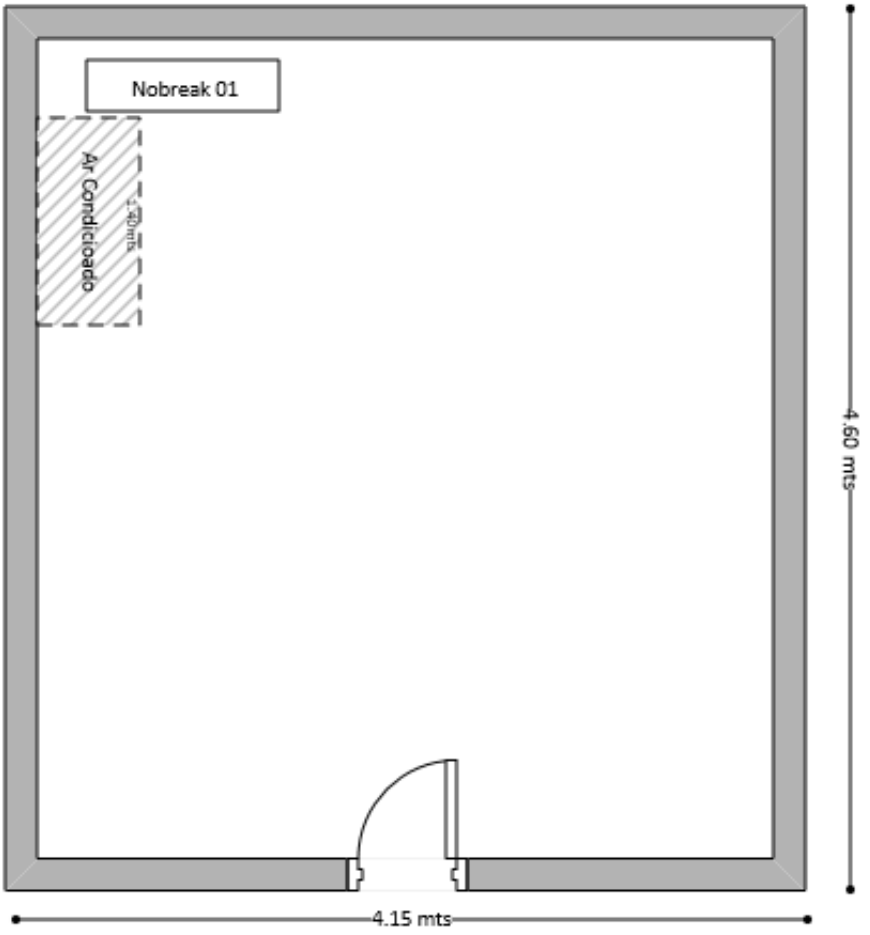
Figura 10 - Sala de entrada de energia elétrica e sala do gerador



Fonte: Próprio Autor

Dentro da sala do *Datacenter* existe um modulo de UPS, responsável por estabilizar a energia elétrica originada do PDU-01 (quadro de energia dedicado para a sala do *Datacenter*), conforme a Figura 11, e repassar energia para os equipamentos. Caso a Companhia de energia elétrica venha a falhar, o sistema de UPS é responsável em fornecer energia para todo o Datacenter, até que o gerador entre em modo de operação, e comece a fornecer energia para o *Datacenter* e para toda a empresa.

Figura 11 - Layout do Datacenter



Fonte: Próprio Autor

O sistema de UPS possui a capacidade atual de fornecer energia para o *Datacenter* durante quarenta minutos, tempo suficiente para desligar todos os equipamentos de forma correta, caso o gerador não entre em operação após uma falha da Companhia de energia elétrica. Essa informação de capacidade atual de carga é retirada do próprio *display* do equipamento de UPS, pois na infraestrutura atual do *Datacenter* não existe nenhum sistema de monitoramento da carga e condições da bateria.

Todos os *racks* e equipamentos dentro do *Datacenter* são aterrados.

Alguns pontos únicos de falhas na área de Elétrica do *Datacenter* da Empresa X são:

- Falha ou manutenção no *nobreak*;

- Falha ou manutenção do PDU-01 dentro do Datacenter;
- Falha ou manutenção nos quadros de elétrica, na sala de entrada de energia elétrica;
- Falha de manutenção no caminho de entrada do cabeamento elétrico;
- Evento não planejado (catástrofe) pode ocorrer no caminho de entrada do cabeamento elétrico;

Qualquer um dos eventos acima, se ocorrerem, podem interromper os serviços do *Datacenter*.

Para finalizar a analise, a última categoria de classificação de *Datacenter*, a área de Mecânica.

O *Datacenter* atual da empresa possui apenas um modulo convencional de ar condicionado, responsável pela refrigeração de todo o *Datacenter*. Caso o mesmo venha a falhar e/ou precise de uma manutenção, todo o ambiente o *Datacenter* sofrerá com o aumento da temperatura.

Atualmente não existe nenhum sistema de controle de umidade relativa do ar, e nenhum outro equipamento que monitore a temperatura do ambiente, caso o ar condicionado venha a falhar.

Referente aos sistemas de proteção contra incêndio, o *Datacenter* possui apenas extintores de pó químico para combater incêndio, ficando totalmente vulnerável a qualquer incêndio que ocorra, e que já esteja em um nível avançado.

Concluindo o estudo de caso, hoje se a Empresa X buscasse uma empresa para certificar o *Datacenter* com base nas normas de classificações citadas na pesquisa, em todas as áreas de classificação o *Datacenter* da Empresa X seria classificado como *TIER* I, e automaticamente obteria a classificação geral como *TIER* I, com disponibilidade de 99,671 % e *downtime* de 28,8 horas por ano.

7. PROPOSTA DE MELHORIA

Este capitulo tem como objetivo propor melhorias na infraestrutura do data center atual da empresa, colocando-o em condições mais elevadas de níveis de segurança exigida pelas normas técnica citadas nesse trabalho.

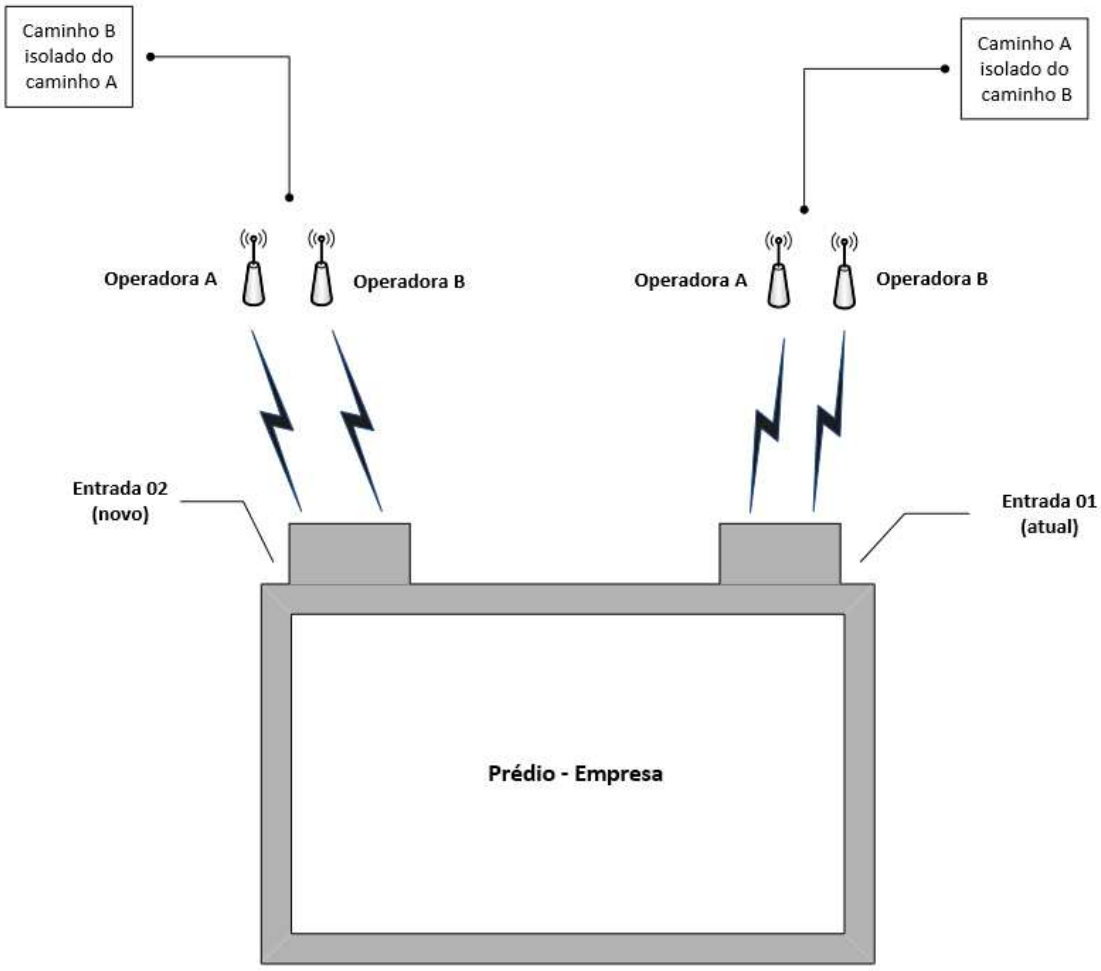
A primeira melhoria a ser implementada, é uma política de segurança do tipo regulatória para o *Datacenter*, descrevendo com detalhes, quem poderá acessar o datacenter, quais atividades devem ser realizas, como devem ser realizadas e quem deve realizar as atividades.

Na área de telecomunicação do datacenter as melhorias apresentadas são:

- Identificação de todos o cabeamento, *racks*, réguas de energia, tomadas e quadro de energia dentro do datacenter, facilitando qualquer manutenção/serviço dentro do datacenter;

- Criação de um novo caminho de entrada totalmente apartado do atual, para a entra de serviços de internet e de voz, para que as operadoras, possam providenciar uma dupla abordagem dos serviços utilizado hoje. Ou seja, cada operadora deverá entregar os seus serviços tanto pela entrada um como na entrada 02 e o ideal conforme a Figura 12 é que as operadoras não utilizem do mesmo meio físico utilizado hoje (cabeamento, fibra), caso haja essa possiblidade as operadoras deverão entregar seus serviços com uma estrutura totalmente separada da atual.

Figura 12 - Entrada de serviços de telecomunicação



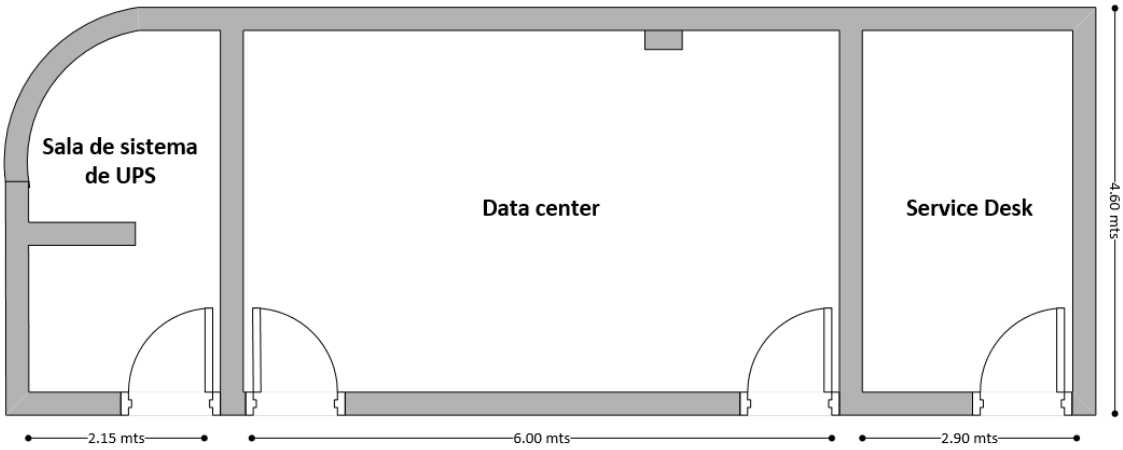
Fonte: Próprio autor

- Identificação de todos o cabeamento, *racks*, réguas de energia, tomadas e quadro de energia dentro do datacenter, facilitando qualquer manutenção/serviço dentro do datacenter;

Para a área de Arquitetura do datacenter, as melhorias apresentadas são:

- Alteração da localização do *datacenter*, conforme a Figura 13. Com essa alteração o datacenter deixará de correr risco de inundação caso ocorra vazamento por parte das tubulações de agua, dos banheiros localizados no andar.

Figura 13 - Alteração do layout



Fonte: Autor próprio

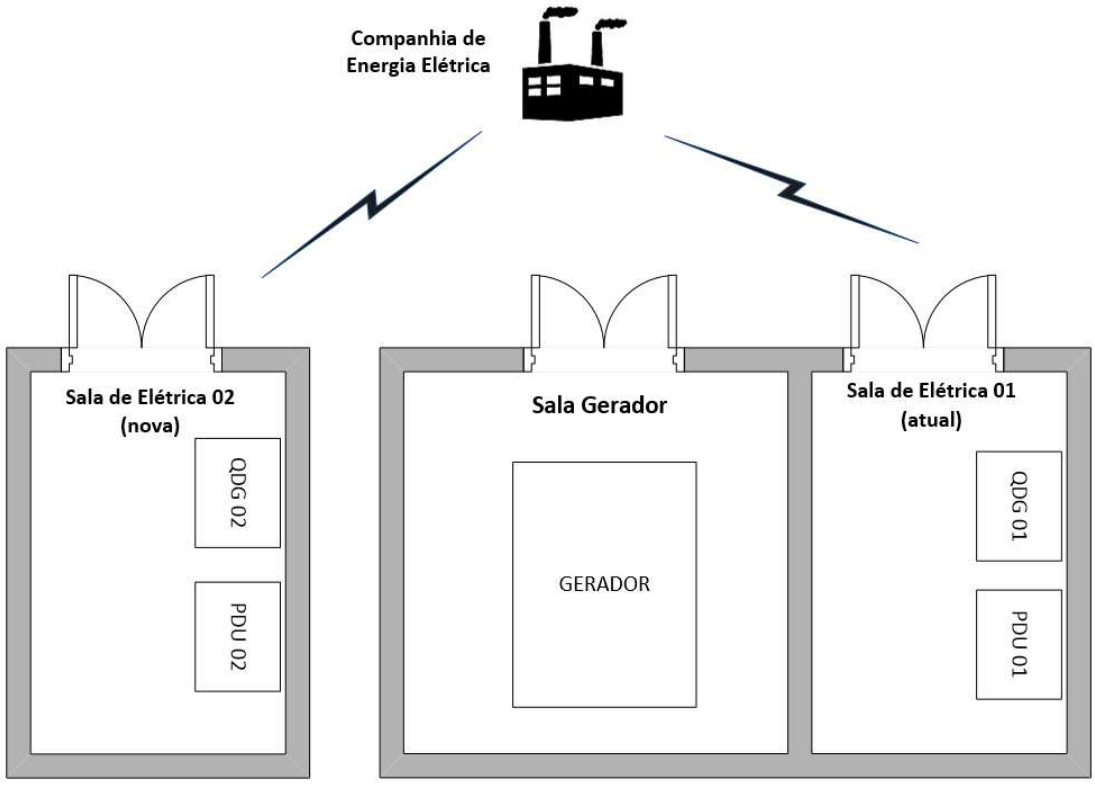
- Criação de uma sala dedicada para os equipamentos de UPS, conforme figura 13. Com a criação dessa sala, será possível disponibilizar mais espaço dentro do datacenter no qual o mesmo se encontra com espaço reduzido. O sistema de UPS receberá uma climatização dedicada aumentando a vida útil dos equipamentos e melhorando qualidade de energia fornecida pelos mesmos;
- Controle de acesso nas duas entradas do datacenter, com monitoramento via software possibilitando o identificar quem acessou o *Datacenter*;
- Remoção das janelas do perímetro do *Datacenter* e fechamento com alvenaria, aumentando a segurança do datacenter e diminuindo o aumento da temperatura;
- Substituição da porta de vidro, por portas de madeira maciça com estrutura metálica, fazendo com que aumente a segurança do *Datacenter*;
- Instalação de piso elevado em todo o *Datacenter*, possibilitando a melhor organização e manutenção do cabeamento;

Para a área de Elétrica do *Datacenter*, as melhorias sugeridas são:

- Criação de uma nova sala de entrada de elétrica, totalmente apartada da que existe hoje, conforme a figura 14, deixando de existir apenas um(a) caminho/entrada de energia elétrica na empresa;
- Solicitar que a operadora disponibilize dois circuitos de energia elétricas (se possíveis circuitos independentes e por caminhos diferentes), um para cada sala de elétrica conforme ilustrado na Figura 14;

- Solicitar que a operadora disponibilize dois circuitos de energia elétricas (se possíveis circuitos independentes e por caminhos diferentes), um para cada sala de elétrica conforme ilustrado na Figura 14;

Figura 14 - Entrada de energia elétrica



Fonte: Autor próprio

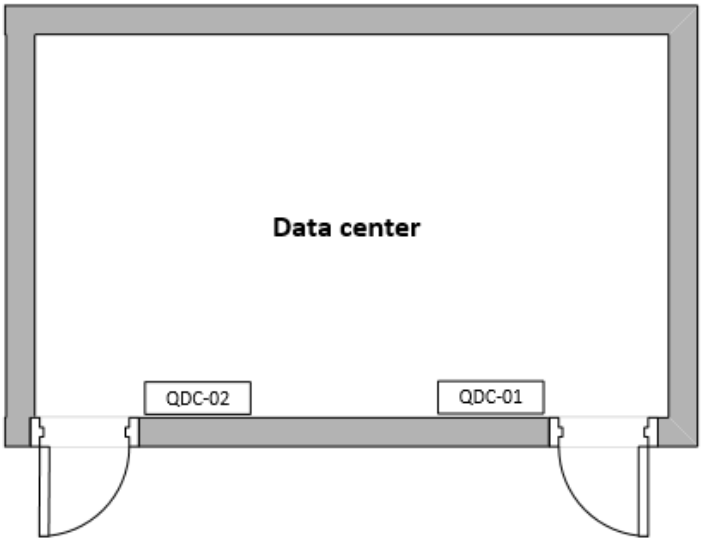
- Aquisição de um novo modulo de *nobreak*, para o uso do *Datacenter*, criando redundância do sistema de UPS, conforme figura 15;

Figura 15 - Sala do sistema de UPS

Fonte: Autor próprio

- Ampliação de mais um quadro no *Datacenter* (QDC), conforme a Figura 16, criando redundância e disponibilizando dois circuitos separados para cada *rack* dentro do *Datacenter.*

Figura 16 - Quadros de energia do Datacenter QDC-01 e QDC-02

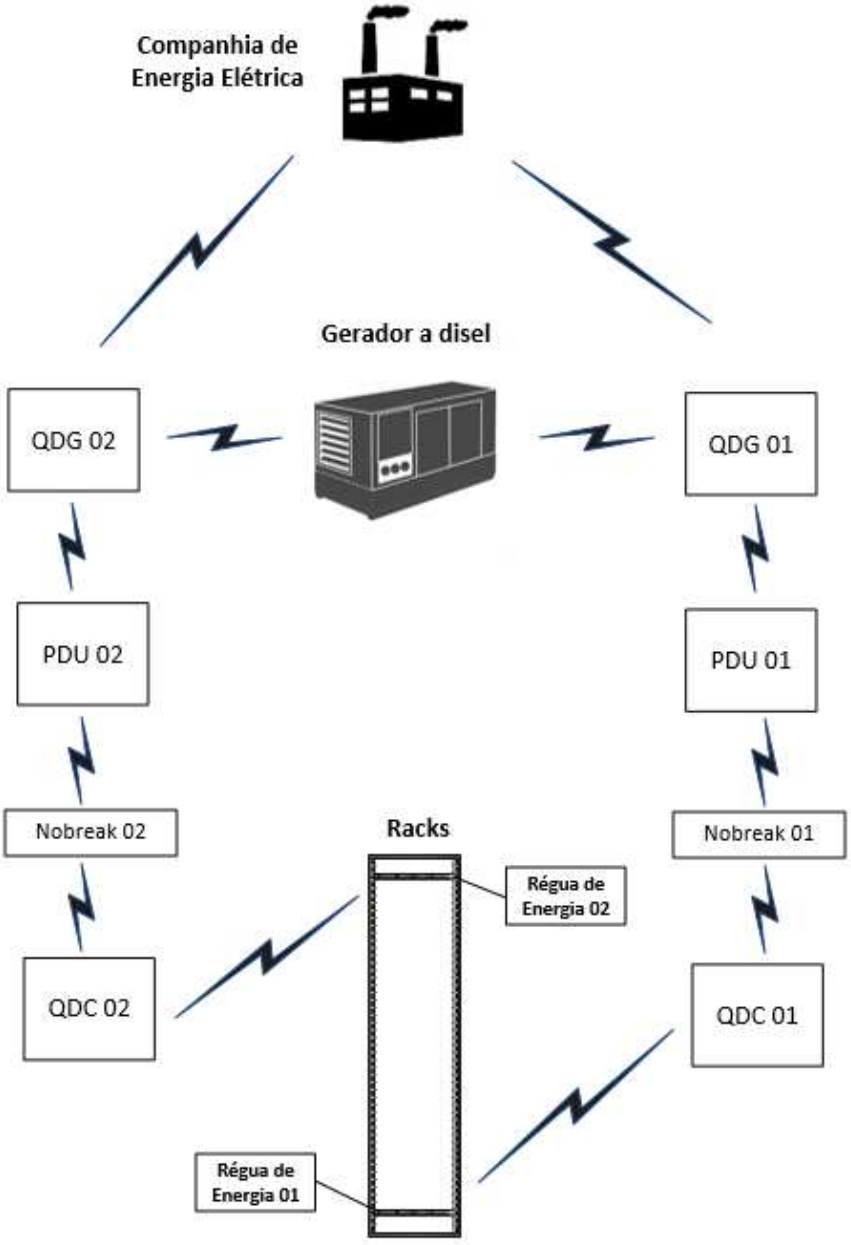


Fonte: Autor Próprio

Com todas as melhorias realizadas na área de Elétrica do *Datacenter,* a infraestrutura elétrica possuirá o cenário demonstrado pela Figura 17. A companhia

de energia elétrica disponibilizará dois circuitos de energia elétrica, uma para cada quadro geral (QDG). O gerador a *diesel* estará interligado também nos dois quadros gerais, pois caso a companhia de energia elétrica venha a falhar, o mesmo deve assumir a função de gerar energia elétrica para todo o prédio e *Datacenter*. Os PDU (pontos de distribuição de energia), receberão a energia elétrica dos quadros gerais, com a função de distribuir a energia para o prédio e para os *nobreaks* da sala de sistema UPS. Os *nobreaks* irão estabilizar a energia elétrica e repassar para os quadros do *Datacenter* (QDC). Quando ocorrer falha na companhia de energia elétrica, os *nobreaks* acumulam também a função de fornecer energia para os QDC's até o gerador entrar em operação. Cada QDC possui um disjuntor para cada rack, fazendo que cada rack receba dois circuitos de energia elétrica, um de cada QDC. No rack, cada régua de energia é ligada em um circuito de elétrico. Finalizando a redundância da área de Elétrica, todos os equipamentos possuem fontes redundantes. Uma fonte deve ser ligada a régua de energia um, e a outra fonte deve ser ligado a régua de energia dois.

Figura 17 - Cenário de Elétrica, após melhorias



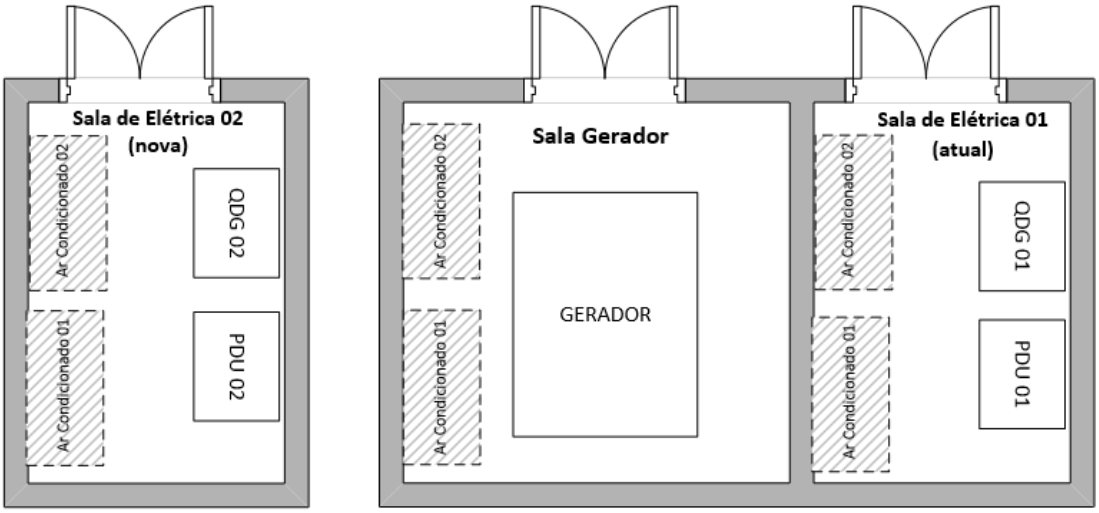
Fonte: Autor próprio

Para a área de Mecânica do *Datacenter*, as melhorias propostas foram divididas em duas partes, a primeira a parte de climatização, e a segunda a parte de sistema de controle e combate a incêndio.

As melhorias propostas para a parte de climatização são:

- Instalação de ar condicionado redundantes nas salas de elétrica e do gerador, conforme a Figura 18, controlando a temperatura e umidade relativa do ar dentro de cada sala, de acordo com especificação solicitada de cada equipamento.

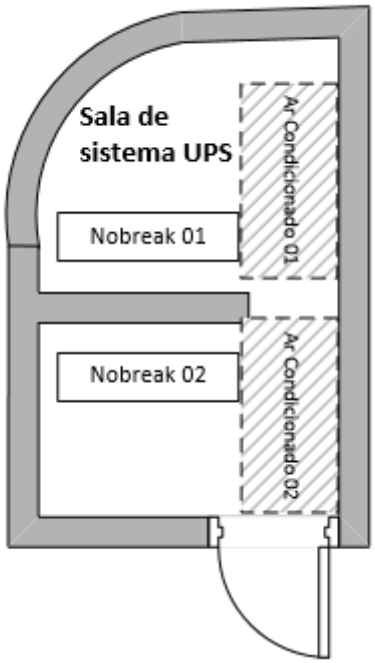
Figura 18 - Climatização das salas elétricas e sala do gerador



Fonte: Próprio Autor

- Instalação de ar condicionado redundantes na sala de sistemas de UPS, conforme a Figura 19, controlando a temperatura e umidade relativa do ar dentro da sala, de acordo com especificação solicitada de cada equipamento, aumentado a vida útil dos equipamentos.

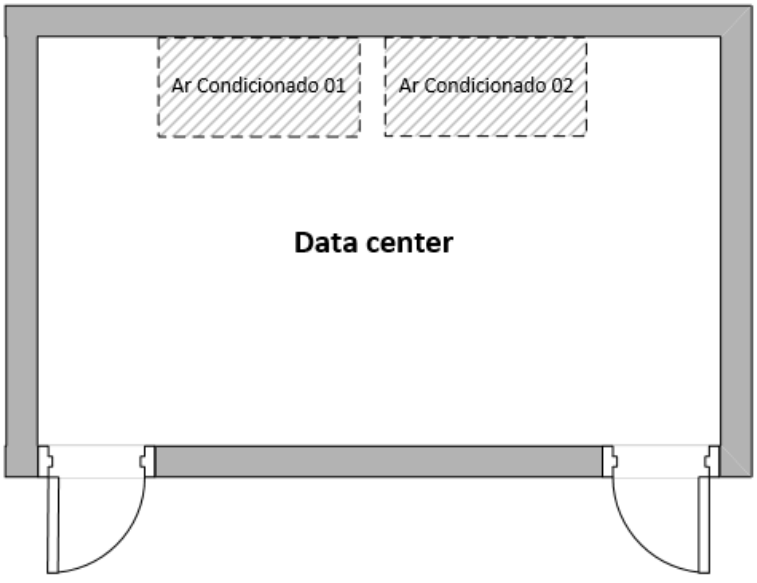
Figura 19 - Climatização da sala de sistema de UPS



Fonte: Próprio Autor

- Instalação de ar condicionado redundantes no *Datacenter*, conforme a Figura 20, controlando a temperatura e umidade relativa do ar dentro do *Datacenter*, aumentado o desempenho dos equipamentos.

Figura 20 - Climatização do Datacenter



Fonte: Próprio Autor

- Instalação em todas as salas de elétrica, gerador, sistema de UPS e *Datacenter*, um termostato inteligente, que permite, após a temperatura ultrapassar um ponto de alarme pré-determinado, sinalizar, enviar *email* ou mensagem para um celular indicando que existe um problema no sistema de climatização.

As melhorias para a segunda parte, a parte de controle e combate a incêndio são:

- Instalação de um sistema de detector de fumaça óptico nas salas de elétrica, gerador, sistema de UPS e *Datacenter*;
- Instalação de um sistema de supressão, esse sistema é um gerador de aerossol que utiliza o composto sólido e estável (SBK), não pirotécnico, à base de sais de potássio. Ao ser ativado pelo sistema de detecção de fumaça, o SBK sólido se transforma num aerossol com micropartículas coloidais 3D, que irão extinguir o fogo com grande rapidez e eficiência. A extinção do fogo é realizada através de reações químicas no nível molecular, que inibem os radicais livres existentes no fogo, os quais alimentam as chamas sem a redução do oxigênio no ambiente;
- Instalação de um sistema de aspiração nas salas de elétrica, gerador, sistema de UPS e *Datacenter*. Trata-se de um detector altamente sensível que permite identificar um foco de incêndio antes que um detector de fumaça possa fazê-lo. O sistema aspira continuamente o ar do ambiente, analisando-o e identificando partículas típicas de incêndio ainda numa fase prematura, como exemplo o superaquecimento de cabos. Esse sistema será utilizado como mecanismo de pré-alarme. Isto permitirá uma ação investigativa nos ambientes antes que os detectores de fumaça entrem em ação e acionem o sistema de supressão;
- Instalação e configuração de um sistema de desligamento de emergência, caso ocorra algum incêndio.

Com todas essas melhorias realizadas, todas as áreas de classificação do *Datacenter*, à área de Telecomunicação, Arquitetura, Elétrica e a área de Mecânica

receberiam a classificação *TIER* II. Automaticamente, a nota geral do *Datacenter* teria um upgrade para *TIER* II, passando a ter uma disponibilidade de 99,741 % e *downtime* de 22 horas por ano.

8. CONSIDERAÇÕES FINAIS

Todos os equipamentos alocados dentro de um *Datacenter* dependem diretamente da infraestrutura do *Datacenter* para que possam trabalhar com eficiência. Para que o *Datacenter* alcance um maior nível de disponibilidade e segurança da informação, o mesmo deve ser planejado e estruturado seguindo as normas e requisitos mínimos de segurança da informação.

Foi realizada uma pesquisa sobre a infraestrutura do *Datacenter*, seus requisitos e seus níveis de classificação. Para isso foram consultados livros, revistas, normas, e empresas especializadas em projetos de segurança da informação e *Datacenters*.

Com base no estudo realizado, foi apresentado o cenário atual do *Datacenter* da empresa X, com intuito de identificar quais os itens que estão fora de *compliance* com as normas, na qual possuem importância fundamental para um maior desempenho, evitando a perda de dados e paradas inesperadas. A classificação atual do *Datacenter* da empresa X baseou-se nos critérios identificados na literatura.

As melhorias propostas são alterações na infraestrutura física das áreas de classificações do *Datacenter.* Os benefícios com essas melhorias seriam o aumento da segurança da informação, e a redução de pontos de falhas, sendo elas por eventos não planejados ou manutenções, aumentando a eficácia do *Datacenter,* contribuindo assim para a continuidade do negócio. As implementações dessas melhorias variam de acordo com a disponibilidade de recursos e o orçamento da Empresa X, podendo ser realizadas em etapas.

Conclui-se ainda que o presente trabalho possibilitou o estudo e o entendimento de práticas e normas, agregando conhecimento técnicos para a formação profissional e acadêmica.

9. REFERÊNCIAS BIBLIOGRÁFICAS

ANSI/TIA/EIA-J-STD-607-A. ***Commercial building grounding (eartthing) and bonding requirements for telecommunications.*** Arlington, USA: TIA, 2002.

ANSI/TIA/EIA-606-A. ***Administration standard for commercial telecommunications infrastructure***. Arlington, USA: TIA, 2002.

ANSI/TIA-942. ***Telecomunicantios infrastructure standard for datacenters.*** Arlington, USA: TIA, 2005.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:** tecnologia da informação – sistemas de gestão de segurança da Informação - requisitos. ABNT,2013.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002-** tecnologia da informação - técnicas de segurança – código de prática para a gestão da segurança da informação. ABNT, 2013.

AURÉLIO, Buarque de Holanda Ferreira. **Dicionário da língua**. Brasília. Nova Fronteira, 2001.

BRITO, Mozar José. **Tecnologia da informação e mercado futuro**: o caso da BM&F. Tecnologia da informação e estratégia empresarial. São Paulo: FEA/USP, 1996.

CAMPOS, André. **Sistema de segurança da informação**: controlando os riscos. Florianópolis: Visual Books, 2006.

CERTBR. **Práticas de segurança para administradores de redes internet.** 2003. Disponível em: < http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.pdf>. Acesso em: 15 ago. 2016.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.

FERREIRA, Fernando Nicolau Freit, **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2003.

FRASER, Barbara. **GRFC 2196:** site security handbook. Pittsburgh.1997. Disponível em: < https://www.ietf.org/rfc/rfc2196.txt>. Acessado em: 16 ago. 2016.

FURUKAWA. **Guia de recomendação para *datacenter*.** [s.d]. Disponível em: <http://portal.furukawa.com.br/arquivos/i/itm/itmax/1184_GuiadeRecomendaAAao.pdf>. Acesso em: 5 jul. 2016.

IBGE. **Pesquisa nacional por amostra de domicílios.** 2014. Disponível em: http://www.ibge.gov.br/home/estatistica/populacao/trabalhoerendimento/pnad2014/default.shtm>. Acesso em: 3 jul. 2016.

IEEE Standard 446. ***Emergency and standby power systems for Industry and commercial applications working group.*** New York,USA: IEEE, 1995.

IEEE Standard 1100***. Powering and grounding eletronic equipment***. New York, USA: Emerald Book, 2005.

MARIN, Paulo S. ***Datacenters*****:** desvendando cada passo: conceitos, projetos, infraestrutura física e eficiência energética. 1. Ed. São Paulo: Érica, 2011.

NEXANS. 2013. Disponível em: < http://www.nexans.com.br/eservice/Brazil-pt_BR/fileLibrary/Download_540134436/Brazil/files/catalogo%20nus_maio%202013.pdf>. Acesso em: 02 ago. 2016 .

NFPA-70. ***National electrical code.*** Atlanta, GA: National Fire Protection Association, 2002.

NFPA-75. ***Standard of the protection of information technology equipment.*** Atlanta, GA: National Fire Protection Association, 2003.

PALOALTO. **O que é um *datacenter.*** [s.d]. Disponível em: < https:// www.paloaltonetworks.com.br/resources/learning-center/what-is-a-data-center.html>. Acesso em: 15 jul. 2016.

PWC. **Pesquisa global de segurança da informação.** 2014. Disponível em: <http://www.pwc.com.br/pt/publicacoes/servicos/consultoria-negocios/pesquisa-global-seguranca-informacao-14.html >. Acesso em: 25 mar. 2016.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SIEWERT, C.Vanderson, **Integração da política de segurança da informação com firewall. 2007. Disponível** em <http://artigocientifico.tebas.kinghost.net/uploads /artc_1202930234_72.pdf>. Acesso em: 07 de jul. 2016.

TURBAN, Efraim; VOLONINO, Linda. **Tecnologia da informação para gestão**. São Paulo: Bookman, 2013.

UPTIME INSTITUTE. Disponível em: <https://uptimeinstitute.com/*TIER*Certification/ constructed-facility-certifications.php?page=1&ipp=All&clientId=&countryName= Brazil &*TIER*Level=4 >. Acesso em: 27 de out. 2016.

VERAS, Manoel. ***Datacenter*****:** componente central da infraestrutura de TI. Rio de Janeiro. Brasport, 2009.

ZUCCHI, Wagner Luiz. Construindo um datacenter**. Revista USP.** São Paulo: USP,2013