

UNIVERSIDADE SÃO FRANCISCO

Engenharia de Computação

**FELIPE ROSSI**

OUTROS TRABALHOS EM:

[www.projetoederedes.com.br](http://www.projetoederedes.com.br)

**TÉCNICAS E PRÁTICAS PARA A CONSTRUÇÃO DE UM  
DATA CENTER SEGURO**

Itatiba  
2012

FELIPE ROSSI

R.A 002200500207

# **TÉCNICAS E PRÁTICAS PARA A CONSTRUÇÃO DE UM DATA CENTER SEGURO**

Monografia apresentada ao Curso de Engenharia de Computação da Universidade São Francisco, como requisito parcial para obtenção do título de Bacharel em Engenharia de Computação.

Orientador: Prof. Esp. Edval Piccolo de Matos.

Itatiba  
2012

Felipe Rossi

Técnicas e práticas para a construção de um Data Center seguro

Orientador: Prof. Esp. Edval Piccolo de Matos.

47 páginas

Palavras-chave: Construção Data Center, Segurança, TI, Normas.

**FELIPE ROSSI**

**TÉCNICAS E PRÁTICAS PARA A CONSTRUÇÃO DE UM DATA  
CENTER SEGURO**

Monografia aprovada pelo curso de  
Graduação em Engenharia de Computação  
da Universidade São Francisco, como  
requisito parcial para a obtenção do título de  
Bacharel Engenheiro de Computação.

**Data de aprovação:** \_\_\_\_/\_\_\_\_/\_\_\_\_

**Banca examinadora:**

---

Prof. Esp. Edval Piccolo de Matos (Orientador)  
Universidade São Francisco

---

Examinador um  
Universidade São Francisco

---

Examinador dois  
Universidade São Francisco

## **DEDICATÓRIA**

Dedico essa monografia primeiramente a Deus, principalmente ao meu pai e minha mãe, pois se não fosse por eles nada disso seria possível. À minha noiva, pela sua paciência e a ajuda que foram muito importantes. Em memória dos meus avós, a todos meus familiares e amigos que me acompanharam nessa jornada.

## **AGRADECIMENTOS**

Gostaria de agradecer primeiramente ao meu orientador, professor Edval Piccolo de Matos, pelos seus conselhos e por dividir sua sabedoria. Agradecer também aos professores por todos os ensinamentos e experiências. Aos meus amigos que me apoiaram e todos que estiveram do meu lado para que essa etapa da minha vida fosse concluída com sucesso.

*Procure ser um homem de valor,  
em vez de ser um homem de sucesso.  
(Albert Einstein)*

## RESUMO

A cada ano que passa a Tecnologia da informação (TI) evolui numa velocidade surpreendente. Em pouco tempo se tornou uma ferramenta de extrema importância para grandes, médias e pequenas empresas, sendo um diferencial competitivo no mercado e fazendo com que a demanda de produtividade seja atendida através de soluções com alto valor agregado. Para uma maior disponibilidade das aplicações da empresa são necessários que os servidores, links e equipamentos de rede, estejam em um local apropriado. O Data Center é o local mais apropriado para armazenar, processar dados e gerenciar aplicativos de forma segura. O desenvolvimento desse projeto tem como objetivo propor as melhores técnicas e práticas utilizadas na construção de Data Centers, baseando-se em normas e recomendações que atribuem maior disponibilidade e segurança. Serão descritas normas, que servirão de guias para definir o padrão que o projeto de construção deverá seguir. Após essa definição, serão propostas algumas técnicas que proporcionaram maior disponibilidade ao Data Center e são de total importância dentro de sua estrutura. Com a descrição das melhores práticas e técnicas utilizadas atualmente, será possível ter um instrumento de consulta para a construção de um Data Center seguro.

**Palavras-chaves:** Construção Data Center, Segurança, TI , Normas.



## **ABSTRACT**

With each passing year the Information Technology (IT) evolves with surprising speed. Soon it became a tool of extreme importance to large, medium and small businesses, with a competitive edge in the market and causing the demand is met through productivity solutions with high added value. For increased availability of enterprise applications that are necessary servers, network equipment and links, are in an appropriate location. The Data Center is the most appropriate place to store, process data and manage applications securely. The development of this project is to propose the best techniques and practices used in building data centers, based on standards and recommendations that assign greater availability and security. Standards are described, which serve as guides to set the standard that the construction project should follow. After this definition will be proposed some techniques that provided greater availability to the data center and are all important within its structure. With the description of best practices and techniques used today, you can have a consultation tool for building a secure Data Center.

**Keywords:** Data Center Construction, Security, IT, Standards.

## LISTA DE FIGURAS

FIGURA 1 – Diagrama básico de um Data Center.....	18
FIGURA 2 – Detalhe PMDC tudo em um.....	23
FIGURA 3 – Detalhe PMDC multiplos contêiners .....	24
FIGURA 4 – Detalhe do piso elevado. ....	25
FIGURA 5 – Detalhe da estrutura do projeto de piso elevado.....	26
FIGURA 6 – Detalhe do corredor quente e corredor frio, distribuição pelo piso elevado. ....	28
FIGURA 7 – Detalhe corredor quente e corredor frio, distribuição <i>overhead</i> .....	28
FIGURA 8 – Detalhe de um dos geradores da UOL .....	29
FIGURA 9 – Detalhe do aterramento no piso elevado. ....	30
FIGURA 10 – Detalhe <i>patch-panel</i> com os cabos sendo ligados na parte detrás. ....	32
FIGURA 11 – Detalhe de um <i>rack</i> com <i>patch-panel</i> .....	32
FIGURA 12 – Detalhe de bateria de cilindros FM-200. ....	37
FIGURA 13 – Detalhe sistema fixo de proteção contra incêndio.....	37
FIGURA 14 – Segurança em camadas.....	38

## LISTA DE TABELAS

TABELA 1 – Comparação do Tier.....	21
TABELA 2 – Especificações de temperatura e umidade relativa.....	27
TABELA 3 – Comparação das categorias de cabos de rede.....	33
TABELA 4 – Características multimodo .....	34
TABELA 5 – Distância aproximada em metros fibras multimodo .....	35
TABELA 6 – Luminosidade mínima para CFTV em Data Center. ....	41

## LISTA DE ABREVIATURAS E SIGLAS

ASHRAE – *American Society of Heating, Refrigerating and Air-Conditioning Engineers*

CAT – Categoria

CFTV – Circuito Fechado de TV

CO<sub>2</sub> – Dióxido de Carbono

EDA – *Equipment Distribution Area*

ER – *Entrance Room*

ESD – *Electrostatic Discharge*

Gb/s – Gigabit por segundo

HAD – *Horizontal Distribution Area*

HAVC – *Heating, ventilation, and air conditioning*

KPA – *Kilopascal*

KVM – *Keyboard, Video, Mouse*

LAN – *Local Area Network*

Mb/s – Megabit por segundo

MDA – *Main Distribution Area*

MHZ – Mega-Hertz

nm – nanómetro

PDU – Power Distribution Unit

PMDC – *Portable Modular Data Center*

SAN – *Storage Area Network*

TI – Tecnologia da Informação

UPS – *Uninterruptible Power Supply*

ZDA – *Zone Distribution Area*

## SUMÁRIO

1 INTRODUÇÃO.....	14
1.1 OBJETIVO .....	15
2 CLASSIFICAÇÕES E NORMAS DE DATA CENTERS.....	16
2.1 Classificação Segundo a TIA 942.....	16
2.1.1 Classificações de redundâncias.....	16
2.1.2 Topologia Segundo a TIA 942.....	17
2.1.3 Tier 1 – Básico.....	18
2.1.4 Tier 2 – Componentes Redundantes.....	19
2.1.5 Tier 3 – Sistema Auto Sustentado.....	19
2.1.6 Tier 4 – Alta Tolerância a Falhas .....	20
3 LOCALIZAÇÃO.....	22
3.1 Recomendações sobre localização geográfica.....	22
3.2 Data Center Portátil e Modular .....	23
4 PISO ELEVADO .....	25
4.1 Recomendações .....	26
5 REFRIGERAÇÃO E CONTROLE DE UMIDADE .....	27
5.1 Sistemas de Refrigeração .....	27
6 SISTEMA ININTERRUPTO DE ENERGIA ELÉTRICA .....	29
6.1 Sistemas Contra Descargas Elétricas .....	30
7 CABEAMENTO ESTRUTURADO.....	31
7.1 Topologia cabeamento estruturado .....	31
7.2 Cabeamento Metálico.....	33
7.3 Fibra óptica .....	34
8 COMBATE E PREVENÇÃO DE INCÊNDIOS.....	36
8.1 Gases inibidores de incêndio.....	36
8.2 Sistema fixo de proteção contra incêndio .....	37
9 SEGURANÇA E CONTROLE DE ACESSO.....	38
9.1 Segurança em Camadas.....	38
9.1.1 Métodos de identificação confiabilidade x custo.....	39
9.2 Biometria .....	40
9.3 Monitoramento CFTV .....	40
10 CONCLUSÃO .....	42
REFERÊNCIAS BIBLIOGRÁFICAS.....	44

# 1 INTRODUÇÃO

Com o avanço tecnológico e o grande fluxo de dados, as empresas estão investindo cada vez mais na área de Tecnologia da Informação (TI) [6]. Em busca de garantir a proteção dos dados e maior disponibilidade de recursos, houve a necessidade de melhorar ou construir Data Centers.

O Data Center é uma estrutura física sendo, sala ou edifício que foi projetado para abrigar uma variedade de recursos que fornecem armazenamento e gerenciamento de equipamentos de rede, servidores e telecomunicação [1].

A maneira de construí-lo e a forma de gerenciá-lo foram alteradas desde o surgimento do conceito em 1964 com o lançamento do IBM System 360, um mainframe<sup>1</sup> para centralizar todo o processamento de uma organização [3]. Desde então, empresas vem investindo cada vez mais neste quesito, devido à preocupação de manter suas informações sigilosas em um local apropriado dentro da empresa de uma forma segura. Como exemplo, podemos citar a empresa GOOGLE que investiu 951 milhões de dólares no último trimestre de 2011 [4], além da CPM Braxis Capgemini que investiu 14 milhões de reais em um Data Center próprio para atender a demanda de clientes [5].

Com este aumento de demanda pelos Data Centers, o risco de um desastre e a perda das informações ficou ainda maior. No entanto, as tecnologias e os conceitos para mitigar estes riscos estão sendo aprimorados cada vez mais, com o objetivo de alcançar maior segurança e disponibilidade.

Considerando a importância do Data Center para as empresas e a necessidade de uma maior disponibilidade dos seus recursos, foram coletadas as melhores práticas e técnicas para sua construção. A necessidade de aplicar estas técnicas e práticas foi o tema escolhido para a realização deste trabalho.

Um Data Center baseado nas melhores práticas tende a ter uma disponibilidade maior, assim podendo ser certificado com a classificação Tier, como veremos ao longo deste trabalho.

Por conter um grande número de equipamentos elétricos, o risco de curtos circuitos são eminentes, por este motivo, deve-se investir em sistemas de combate e prevenção de incêndio.

Para mitigar o risco de roubo de informação, as empresas estão implantando seguranças físicas nos próprios Data Centers, com monitoramento CFTV, Segurança em camadas, onde cada camada possui métodos de acesso diferentes.

---

<sup>1</sup> Mainframe - É um computador de grande porte, dedicado normalmente ao processamento de um volume grande de informações.

A localização é um fator de grande importância em um projeto de Data Center. Deve ser levada em consideração a infraestrutura do local onde será instalado. A localização geográfica deve ser estudada seguindo normas que determinam fatores de riscos e recomendações de melhores localidades.

Penando em flexibilidade, uma solução bastante interessante foi apresentada pela empresa IBM, o PMDC (*Portable Modular Data Center*) Data Center Portátil e Modular. O PMDC é construído a partir de um contêiner e foram projetados para suprir a necessidade de empresas que precisam de uma alocação temporária ou não possuam um local apropriado para a construção ou expansão [16]. Veremos mais detalhes ao longo deste trabalho.

## **1.1 OBJETIVO**

A elaboração deste trabalho tem como objetivo, apresentar as melhores práticas disponíveis no mercado atual para construção de Data Center. Abordaremos conceitos, tais como, refrigeração, controle de umidade, redundância energética, cabeamento estruturado, piso elevado, combate e prevenção contra incêndio como também a segurança de acesso. Com base nestes estudos, será apresentado um trabalho que possa servir como base de consulta para a comunidade científica, pessoas ou empresas interessadas no assunto.

## 2 CLASSIFICAÇÕES E NORMAS DE DATA CENTERS

Segundo Paulo Sérgio Marin [6] foi publicado em 2005 uma norma norte-americana ANSI que define as classificações de Data Center em função da disponibilidade e redundância.

Existe a norma ANSI/BICSI-002 (*Data Center Design and Implementation Best Practices*) Projeto de Data Center e Melhores Práticas de Implementação, publicada em março de 2011, com cinco classificações de disponibilidade de Data Center, F0 a F4 sendo a F0 a classe mais básica e a F4 a classe mais tolerante as falhas [6].

A norma que se aplica na infraestrutura de um Data Center, de acordo com a sua disponibilidade e a sua redundância é a ANSI/TIA 942 (*Telecommunications Infrastructure Standard for Data Center*) Infraestrutura de Telecomunicações para Data Centers que atualmente é a norma mais utilizada e é a única que aplica o conceito de Tiers (desenvolvido pelo *The Uptime Institute*) para a classificação de Data Centers.

### 2.1 Classificação Segundo a TIA 942

Segundo Manoel Veras [7], pela norma ANSI/TIA 942, existem regras aplicáveis para a classificação do Data Center em quatro níveis independentes de Tiers, são eles:

- Redundância
- Telecomunicação
- Arquitetura e estrutural
- Elétrica
- Mecânica

#### 2.1.1 Classificações de redundâncias

A norma ANSI/TIA-942 estabelece nomenclaturas para as definições da redundância dos Data Centers, utilizando como base a classificação Tier. As classificações são as seguintes [6]:

- Data Center “N”, sem nenhum tipo de redundância.
- Data Center “N+1”, existe pelo menos uma redundância, por exemplo: *nobreak*, gerador, *link* redundante, etc.
- Data Center “N+2”, existe uma redundância a mais, por exemplo: o Data Center será suprido na falta de energia por um *nobreak* e um gerador, sendo



assim duas redundâncias. Podendo se estender para os outros equipamentos, *links*, refrigeração, sistema de prevenção de incêndios, etc.

- Data Center “2N”, neste caso seria uma redundância completa, por exemplo: duas empresas de distribuição de energia (sendo que essas empresas devem vir de diferentes subestações) para alimentar o Data Center.
- Data Center “2(N+1)” existe uma redundância para cada equipamento, utilizando o exemplo anterior, seria necessário um *nobreak* ou gerador para cada uma das empresas de energia.

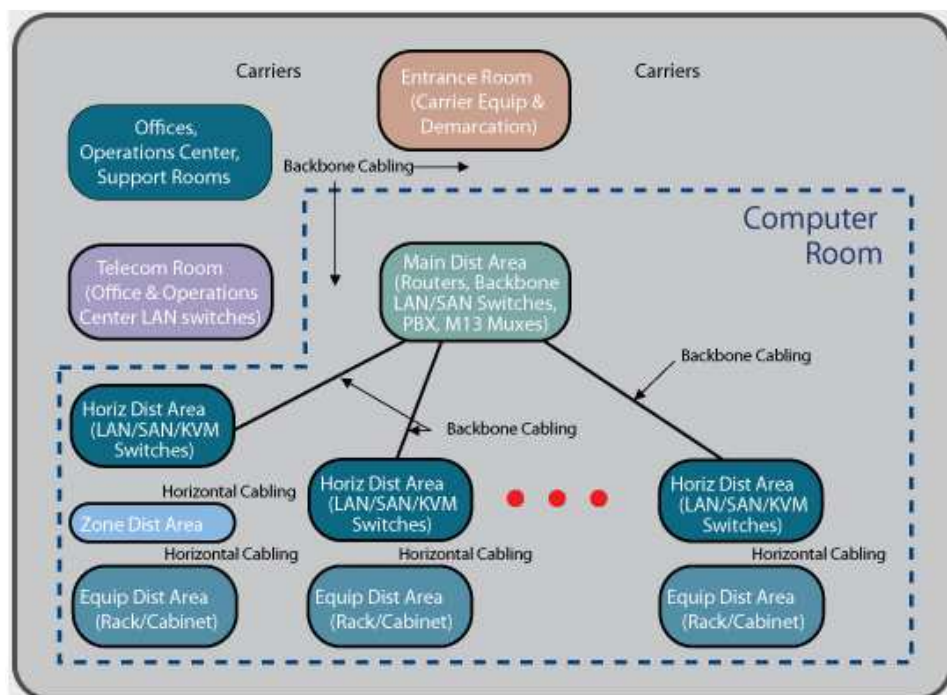
### 2.1.2 Topologia Segundo a TIA 942

De acordo com Manoel Veras [7], a topologia de um Data Center pode ser descrita de várias formas, pode-se basear na norma TIA 942 que é um padrão para este tipo de ambiente.

De acordo com informações obtidas do site da empresa Furukawa [8], as principais áreas presentes em um Data Center são:

- **Entrance Room (ER):** espaço de interconexão do cabeamento estruturado do Data Center e o cabeamento proveniente da telecomunicação.
- **Main Distribution Area (MDA):** local onde se encontra a conexão central do Data Center e de onde se distribui o cabeamento estruturado, incluindo roteadores e *backbone*.
- **Horizontal Distribution Area (HDA):** área utilizada para conexão com a área de equipamentos, incluindo o *cross connect* horizontal, equipamentos intermediários, LAN (*Local area network*), SAN (*Storage Area Networks*) e KVM (*Keyboard, Video, Mouse*) switches.
- **Zone Distribution Area (ZDA):** ponto de interconexão opcional do cabeamento horizontal. Fica entre HDA e o EDA, provê flexibilidade no Data Center.
- **Equipment Distribution Area (EDA):** área destinada para os equipamentos terminais (servidores, *storages*, unidades de fita), inclui também os *Racks*, gabinetes e equipamentos de comunicação de dados ou voz.

A figura 1 apresenta um diagrama básico com os espaços de um Data Center e como esses espaços são relacionados entre si.



Fonte: [http://portal.furukawa.com.br/arquivos/i/itm/itmax/1184\\_guiaderecomendaaaao.p](http://portal.furukawa.com.br/arquivos/i/itm/itmax/1184_guiaderecomendaaaao.pdf)

df

FIGURA 1 – Diagrama básico de um Data Center.

### 2.1.3 Tier 1 – Básico

Com informações da empresa Furukawa [8], no modelo básico da classificação -Tier 1 - não existe redundância nas rotas físicas e lógicas. Prevê um nível mínimo de distribuição de carga com pouca ou nenhuma redundância. Neste caso uma falha ou uma parada para manutenção pode ocasionar a interrupção parcial ou total da operação. Deve prever no projeto um sistema de condicionamento de ar simples ou múltiplo, com capacidade de resfriamento das principais áreas, porém sem redundância.

Segundo Manoel Veras [7], os potenciais pontos de falha dessa classificação são:

- Falta de energia da concessionária no Data Center ou mesmo na central operadora de telecomunicações.
- Falha nos equipamentos da operadora de telecomunicação.
- Falha nos roteadores, *switches* quando não forem redundantes.
  - Quaisquer eventos catastróficos na interligação ou nas áreas: ER, MDA, HDA, ZDA e EDA.

O Tier 1 possui uma disponibilidade de 99.671% e pode ter um *downtime*<sup>2</sup> de 28,8 horas/ano sem redundância energética ou refrigeração [9].

<sup>2</sup> *Downtime* – Tempo que o sistema não está operacional.

### 2.1.4 Tier 2 – Componentes Redundantes

De acordo com a Furukawa [8], no Tier 2 os equipamentos de telecomunicações do Data Center e também os equipamentos da operadora de telecomunicação, assim como os comutadores LAN-SAN, devem ter os seus módulos redundantes. O cabeamento do *backbone* principal LAN e SAN das áreas de distribuição para os comutadores devem ter cabeamento redundante, par metálico ou fibra.

Devem ter duas caixas de acesso de telecomunicação e dois caminhos de entrada até a ER com no mínimo 20 metros.

No Tier 2 é necessário prover módulos UPS (*Uninterruptible Power Supply*) redundantes para N+1 e também um sistema de gerador elétrico para suprir a carga, não é necessário redundância na entrada do serviço de distribuição de energia. O sistema de ar condicionado deve ser projetado para ter o funcionamento contínuo de 24x7x365, com no mínimo a redundância de N+1.

Segundo Manoel Veras [7], possíveis pontos de falha dessa classificação são:

- Falhas no sistema de refrigeração ou de energia podem ocasionar falhas nos outros componentes do Data Center.

O Tier 2 possui uma disponibilidade de 99.749%, pode ter um *downtime* de 22 horas/ano e redundância parcial em energia e refrigeração [9].

### 2.1.5 Tier 3 – Sistema Auto Sustentado

Para a Furukawa [8], um Data Center Tier 3 deve ser atendido por no mínimo duas empresas de telecomunicações, tendo como pré-requisito que os cabos venham por rotas distintas. Para uma melhor redundância é necessário ter duas ER com no mínimo 20 metros de separação, não podendo compartilhar equipamentos de telecomunicações e devem estar em zonas de proteção contra incêndios, sistemas de energia e ar condicionado distintos. Devem prover caminhos redundantes entre a ER, as salas MDA e as salas HDA. A conexão entre as salas devem ser feitas via fibra ou pares metálicos redundantes. Prover pelo menos a redundância elétrica N+1.

Segundo Manoel Veras [7], há somente um possível ponto de falha para essa classificação:

- Qualquer evento crítico ou catastrófico na MDA e HDA irá interromper os serviços do Data Center.

O Tier 3 possui uma disponibilidade de 99.982%, pode ter um *downtime* de 1.6 horas/ano e 72 horas de proteção contra interrupção de energia [9].

### 2.1.6 Tier 4 – Alta Tolerância a Falhas

Para um Data Center com alta tolerância a falhas, a Furukawa recomenda [8] no Tier 4, que todo o cabeamento do *backbone* seja redundante, além disso, devem ser protegidos por dutos fechados. Os equipamentos ativos, roteadores, modems da operadora e comutadores LAN/SAN devem ser redundantes. É recomendada a criação de uma MDA secundária, desde que fiquem em zonas contra incêndio separadas. Já o cabeamento da HDA deve ser feito por dois caminhos: um pela MDA principal e outro pela MDA secundária.

Deve-se prover uma disponibilidade elétrica de “2(N+1)”, sendo duas empresas públicas de energia a partir de diferentes subestações para redundância.

Segundo Manoel Veras [7], o potencial ponto de falha dessa classificação é:

- Caso não exista uma MDA e HDA secundária, pode vir a parar o sistema se a MDA ou HDA primária falhar.

O Tier 4 possui uma disponibilidade de 99.995%, pode ter um *downtime* de 0.4horas/ano e 96 horas de proteção contra interrupção de energia [9].

A tabela 1 mostra a comparação entre os quatro Tiers, podendo ressaltar alguns quesitos principais desta comparação, como por exemplo, o primeiro ano de implantação, o consumo de energia e a disponibilidade do Data Center [17].

TABELA 1 – Comparação do Tier.

	Tier I: Basic Components	Tier II: Redundant Maintainable	Tier III: Concurrently Tolerant	Tier IV: Fault Tolerant
Number of Delivery paths	Only 1	Only 1	1 Active, 1 Passive	2 Active
Redundant Components	N	N + 1	N + 1	2 (N + 1)
Support Space to Raised Floor Ratio	20%	30%	80-90%	100%
Initial Watts/m <sup>2</sup>	60-90	120-150	120-180	150-240
Ultimate Watts/m <sup>2</sup>	60-90	120-150	300-450	450 +
Raised Floor Height	30cm	45cm	80-90cm	80-90cm
Floor Loading Kilograms/m <sup>2</sup>	415	488	732	732 +
Utility Voltage	208, 480	208, 480	12-15kV	12-15kV
Months to Implement	3	3 to 6	15 to 20	15 to 20
Year First Deployed	1965	1970	1985	1995
Annual IT Downtime Due to Site	28.8 hrs	22.0 hrs	1.6 hrs	0.4 hrs
Site Availability	99.671%	99.749%	99.982%	99.995%

Fonte: <http://lautankencana.com/data-center-solutions>

### 3 LOCALIZAÇÃO

Muitos relatórios, estudos e especialistas expõem quais são os fatores mais importantes quando for decidir onde alocar um Data Center. A operação eficiente do mesmo e fatores de custo são o coração de qualquer decisão de negócios para onde construir e manter sua infraestrutura. Pequenas e grandes empresas têm igualmente uma série de critérios para escolher a fim de tomar a melhor decisão para a sua empresa de TI.

Os aspectos como a proximidade de redes de energia disponíveis, infraestrutura de telecomunicações, serviços de rede, linhas de transporte e serviços de emergência podem afetar os custos. Riscos, segurança e outros fatores também devem ser levados em consideração para o projeto de um Data Center [11].

#### 3.1 Recomendações sobre localização geográfica

São apresentadas, segundo as normas NBR 14565:2001, ANSI/BICSI-002 e ANSI/TIA-942, algumas recomendações para a escolha da localização que devem ser levadas em consideração.

Locais inadequados para construção [11]:

- Próximos a rios, lagos, oceanos e fundos de vale, pois estes locais têm riscos de inundações, enchentes, tsunamis, etc.
- Próximos a cabeceiras de pistas de aeroportos, pois existe o risco de acidente em potencial.
- Locais com riscos de desmoronamentos e perigo de incêndio.
- Locais propícios a abalos sísmicos e/ou tornados.
- Locais próximos a linhas de transmissões elétricas.
- Países ou locais com guerrilhas.

Locais recomendados para a construção:

- Próximos de acessos a estradas principais.
- Próximos a concessionárias de energia.
- Próximos a centros de serviços.
- Condomínios comerciais específicos para Data Centers.

Deve-se efetuar um estudo no início do projeto da construção do Data Center com as condições climáticas locais, para efetuar uma escolha adequada do sistema de resfriamento, fazendo um levantamento dos custos administrativos e fiscais [10].

### 3.2 Data Center Portátil e Modular

A IBM apresentou o PMDC (*Portable Modular Data Center*) Data Center Portátil e Modular, criado dentro de um contêiner, com as opções de contêineres de 3, 6, 12 e 16 metros quadrados [19].

Este Data Center contém um centro completo e compacto de alta densidade de infraestrutura de dados, também é composto por *hardwares*, *softwares*, sistema de manutenção, unidade de refrigeração e detecção de incêndio, sem a necessidade de infraestrutura predial.

O PMDC é considerado uma tecnologia sustentável, pois ocupa um espaço 50% menor com relação a um Data Center convencional e consome até 77% menos energia [19].

Pode-se observar na figura 2 a demonstração do PMDC *All-in-One* (Tudo em Um) de uma vista aérea. A infraestrutura, sistema de combate de incêndio e o sistema de refrigeração estão no mesmo contêiner [20].

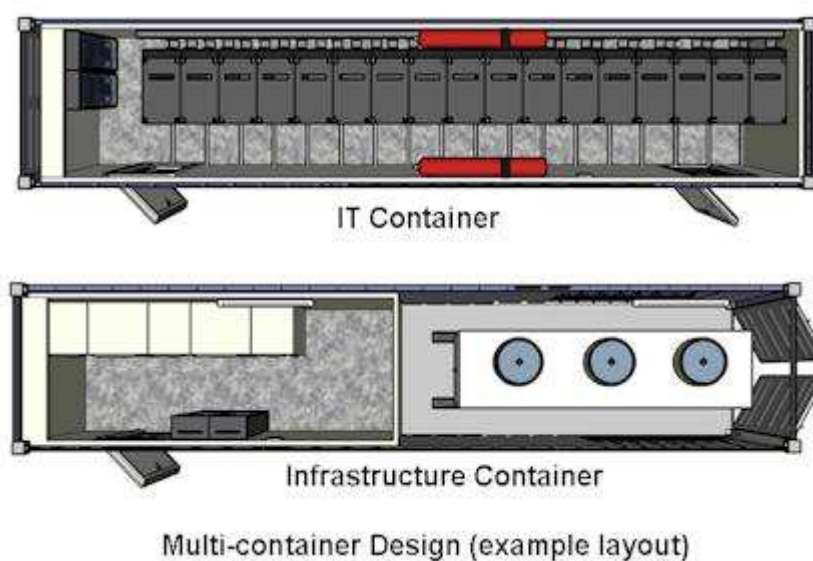


“All-in-One” Design (example layout)

Fonte: <http://www-03.ibm.com/press/br/pt/presskit/34498.wss>

FIGURA 2 – Detalhe PMDC tudo em um.

A figura 3 mostra o PMDC de múltiplos contêineres. No primeiro contêiner estão os servidores e o sistema de combate e prevenção de incêndio. No segundo contêiner, a infraestrutura e sistema de refrigeração [20].



Fonte: <http://www-03.ibm.com/press/br/pt/presskit/34498.wss>

FIGURA 3 – Detalhe PMDC múltiplos contêiners

Este tipo de Data Center pode ser utilizado por empresas que tenham a necessidade de expansão do Data Center, porém sem modificação predial, para uma utilização temporária ou móvel [20].



## 4 PISO ELEVADO

Para projetar um espaço padronizado, modular, expansível para TI, muita atenção deve ser dada para acomodar corretamente o fornecimento de energia, comunicação e o ar refrigerado sob o piso elevado.

O piso elevado é um piso que eleva o ambiente em alguns centímetros, criando um espaço para a instalação de cabos de comunicação, elétricos, ar refrigerado e/ou as tubulações de água gelada para refrigeração [12].

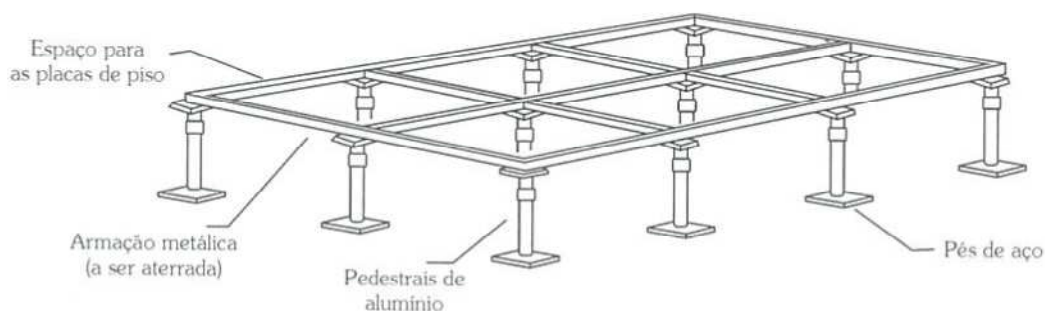
Na figura 4 podemos observar o detalhe dos cabos de dados passando sob o piso elevado [15].



Fonte: [http://www.formica.com.br/produtos/pro\\_formipisodissi.htm](http://www.formica.com.br/produtos/pro_formipisodissi.htm)

FIGURA 4 – Detalhe do piso elevado.

A figura 5 apresenta os detalhes da estrutura do piso elevado, os espaços para colocar as placas 60x60 cm e a armação do piso a ser aterrada [6].



Fonte: Paulo Sérgio Marin (2011)

FIGURA 5 – Detalhe da estrutura do projeto de piso elevado.

## 4.1 Recomendações

A recomendação para a altura do piso elevado é de no mínimo 150 mm para cabos de comunicação e de energia, porém se for utilizar ar refrigerado sob o piso é necessário uma altura mínima de 300 mm. Em geral, baseado em uma dimensão de 600 x 600 mm pisos com um revestimento anti-estático [12].

Para uma maior segurança, de acordo com Paulo Sergio Marin [6] é necessário que a estrutura do piso esteja aterrada para evitar o acúmulo de carga estática, tanto nos equipamentos e *racks*, quanto no piso, podendo ocasionar instabilidade ou a queima do equipamento.

Segundo especificações na norma TIA 942 é necessário que a altura mínima do Data Center, medida a partir do piso acabado até qualquer obstáculo (forro ou teto) seja de 2600 mm [18].

De acordo com Paulo Sérgio Marin [6], o local em que o piso elevado será instalado deve suportar uma carga mínima de 732,36 kgf/m<sup>2</sup> (7,2KPA quilopascal), porém se o Data Center for de alta densidade, terá que suportar uma carga mínima de 1.220,6036 kgf/m<sup>2</sup> (12 KPA).

Para uma melhor organização do Data Center, recomenda-se a instalação do piso elevado, para conseguir ter um melhor aproveitamento do espaço, organização e estética, mesmo se não for possível fazer o resfriamento pelo piso elevado.

## 5 REFRIGERAÇÃO E CONTROLE DE UMIDADE

O sistema HVAC (*Heating, Ventilation, and Air Conditioning*, Aquecimento, Ventilação e Ar Condicionado), inclui múltiplas unidades de ar condicionado com capacidade de manter a temperatura e umidade, com unidades redundantes, podendo efetuar manutenções sem parar o sistema de HVAC.

A Classe 1 da ASHRAE (*American Society of Heating, Refrigerating and Air-Conditioning Engineers*, Sociedade Americana de Engenheiros de Climatização), uma entidade norte-americana internacional na área de padronização para climatização, demonstra na tabela 2 as informações permitidas e recomendadas de temperatura para a entrada de ar nos equipamentos e também a umidade relativa [30].

TABELA 2 – Especificações de temperatura e umidade relativa.

Especificações do ambiente				
Classe	Temperatura (°C) permitida	Temperatura (°C) recomendada	% umidade relativa permitida	% umidade relativa recomendada
1	15 até 32.2	20 até 25	20 - 80	40 -55

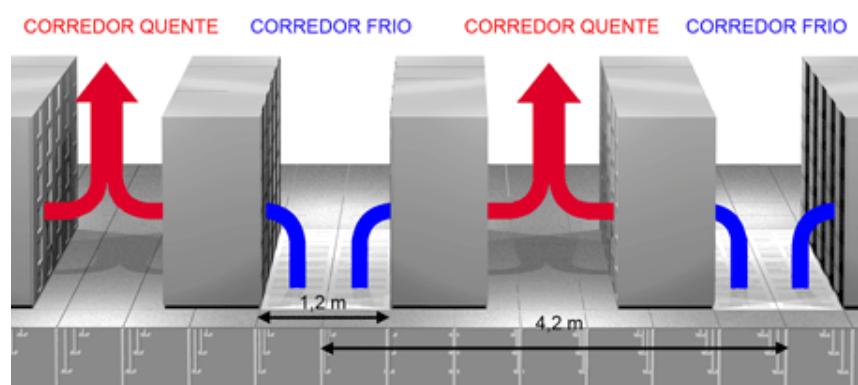
Fonte: <http://searchdatacenter.techtarget.com/tip/Using-ASHRAE-specs-for-data-center-metrics>

De acordo com Paulo Sérgio Marin, aproximadamente cem por cento de toda energia elétrica consumida no Data Center é convertida em calor, que precisa ser retirada do ambiente. Existem várias técnicas disponíveis para remover o calor de forma eficiente [6].

### 5.1 Sistemas de Refrigeração

Segundo Manoel Veras, uma alternativa para melhorar a refrigeração do Data Center é utilizar fileiras de *racks* de frente para outra fileira. O ar frio será fornecido pela frente do *rack* através de aberturas no piso elevado. O corredor ventilado é conhecido como corredor frio. O ar frio é atraído através dos *racks* pelas ventoinhas dos servidores e expulso de volta para o corredor quente. O ar quente ascendente a partir deste corredor encontra o seu caminho de volta para a unidade de ar condicionado a ser refrigerado e, em seguida, repetir o ciclo [7].

Problemas ou indisponibilidades em sistemas de ar condicionado são responsáveis por algumas das falhas de *hardware*. Adotando o sistema corredor quente e corredor frio além do insuflamento sob piso elevado, como demonstrado na figura 6, é o primeiro passo para se ter um maior controle do fluxo de ar no Data Center e eliminar pontos quentes [7].

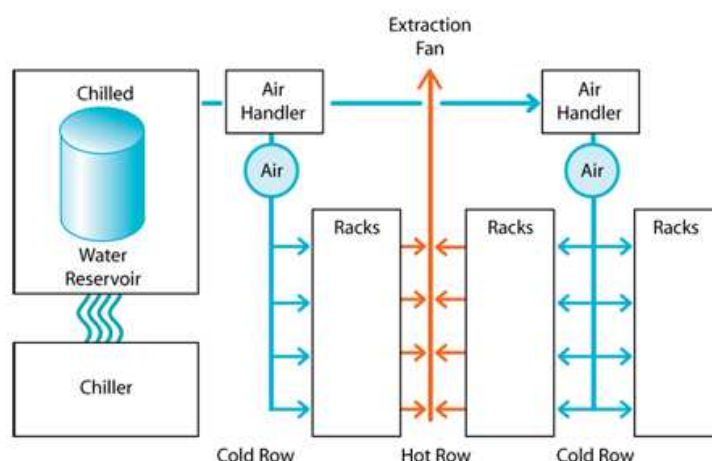


Fonte: [www.tcsolutions.com.br/](http://www.tcsolutions.com.br/)

FIGURA 6 – Detalhe do corredor quente e corredor frio, distribuição pelo piso elevado.

A distribuição de ar pelo teto (*overhead*) deve ser dimensionada para o ar frio ser diretamente distribuído no corredor frio pela parte superior do corredor. O ar quente resultante do resfriamento dos equipamentos irá formar também corredores quentes, que deverão ser posicionados exaustores para a retirada do ar quente [6].

A figura 7 demonstra o ar frio sendo distribuído pela parte superior e o corredor quente utilizando um exaustor para retirada do ar quente [31].



Fonte: <http://www.netriver.net/seattle-data-center/data-center-hvac>

FIGURA 7 – Detalhe corredor quente e corredor frio, distribuição *overhead*.

Existe o sistema autocontidos ou confinados, que podem ser usados para isolar o corredor frio. Este método fecha a parte superior do corredor e instalam-se portas para o acesso. É bastante utilizado em áreas críticas no Data Center e não é necessária a instalação em todo os corredores [6].

## 6 SISTEMA ININTERRUPTO DE ENERGIA ELÉTRICA

O sistema elétrico de um Data Center é constituído pelo Sistema Ininterrupto de Energia UPS (*Uninterruptible Power Supply*). Tem a função de fornecer energia para todos os equipamentos de um Data Center, incluindo equipamentos de detecção, alarme de incêndio e segurança. É composto por conjuntos de *nobreaks* e contém baterias, inversores e retificadores [22].

Os *nobreaks* redundantes, ligados em paralelo, irão assegurar o suprimento contínuo de energia, mesmo em caso de falha de transformadores ou a falta de energia elétrica [22].

As baterias são dimensionadas para garantir uma autonomia por um período mínimo de 15 minutos. Este tempo é suficiente para partida e conexão dos geradores a diesel em caso de falta de energia elétrica da concessionária [23].

O sistema de energia de emergência, consiste de um grupo de geradores a diesel que entrarão em funcionamento e se conectarão ao sistema elétrico do Data Center automaticamente.

Os geradores precisam ser dimensionados para suportar todas as cargas necessárias ao funcionamento dos equipamentos do Data Center durante uma possível falta de energia da concessionária.

A figura 8 traz o detalhe de um dos geradores do site da UOL. De acordo com a empresa, os geradores têm autonomia de 72 horas sem o reabastecimento e são acionados uma vez por semana como uma forma de manutenção [24].



Fonte: <http://tecnologia.uol.com.br/ultimas-noticias/redacao/2010/04/27/com-capacidade-para-30-mil-servidores-novo-data-center-do-uol-coloca-computacao-verde-em-pratica.jhtm>.

FIGURA 8 – Detalhe de um dos geradores da UOL

## 6.1 Sistemas Contra Descargas Elétricas

A utilização de equipamentos de informática em um Data Center se torna muito importante, a ponto de ter um projeto de sistema de aterramento bastante confiável, para evitar danos irreparáveis em equipamentos que possuem alto custo e são de vital importância para os sistemas de rede de comunicações, telecom, entre outros.

Para a construção de um prédio com aterramento é necessário seguir normas como a NBR-5419 e NBR-5410.

A norma NBR-5419 fixa as condições exigíveis ao projeto de instalações e manutenções de sistema de proteção contra descargas atmosféricas de estruturas. Aplica-se às estruturas comuns, utilizadas para fins comerciais, industriais, administrativos ou residenciais [25].

A norma NBR-5410 estabelece as condições a que devem satisfazer as instalações elétricas de baixa tensão, aplica-se principalmente às instalações elétricas de edificações, qualquer que seja seu uso, residencial, comercial, público ou industrial [26].

Recomenda-se construir um sistema de aterramento isolado com destino ao para-raios e outro sistema de aterramento separado para o Data Center, eletrocalhas, *racks* e piso elevado [27].

A figura 9 apresenta um detalhe do aterramento na estrutura do piso elevado para eliminar o acúmulo de carga estática, conseqüentemente, evitar o efeito da descarga eletrostática ESD (*Electrostatic Discharge*) e o conseqüente dano aos equipamentos do Data Center [6].



Fonte: [http://www.infraengenharia.com.br/#/flog/album/data-center-salas-cofres\\$c=1353862274034](http://www.infraengenharia.com.br/#/flog/album/data-center-salas-cofres$c=1353862274034)

FIGURA 9 – Detalhe do aterramento no piso elevado.

## 7 CABEAMENTO ESTRUTURADO

Cabeamento estruturado é uma maneira padronizada de cabear um tipo de rede, não dependendo do seu tipo, minimizando custos e maximizando possíveis expansibilidades futuras. Todos os tipos de dados como voz (telefonia) e multimídia (vídeo), podem ser transmitidos através do mesmo cabo na mesma infraestrutura (painéis, tomadas, conectores) [36].

O sistema de cabeamento estruturado em uma possível reestruturação de rede, evita que seja perdido tempo de trabalho. Este sistema possui um tempo de vida longo, assim requerendo uma maior consideração. Tendo um planejamento criterioso, previne-se um congestionamento na rede, o que poderia diminuir o seu desempenho [36].

### 7.1 Topologia cabeamento estruturado

De acordo com informações de Paulo Sérgio Marin [6], o sistema de cabeamento estruturado se define em quatro elementos principais:

- Sala de comunicação
- Área de trabalho
- Cabeamento horizontal
- Cabeamento do *backbone*

A sala de comunicação é o local ou espaço físico onde são armazenados todos os equipamentos de rede (roteadores, *switchs*) em *racks*. Nesses *racks* são instalados também os *patch-panels*, que são painéis onde ficam ligados os cabos vindos de uma estação. As conexões dos *patch-panels* para os *switchs* são feitas através de um *patch-cord*<sup>3</sup> [6].

Através do manuseio dos cabos de rede podemos alterar o *layout* lógico da rede, desconectando uma das extremidades do *patch-cord*, de uma porta do *switch* e conectando-a em outra porta de outro *switch* [6].

Pode-se observar na figura 10 o detalhe dos cabos sendo ligados na parte detrás do *patch-panel*. Esses cabos vêm da área de trabalho.

---

<sup>3</sup> *Patch-cord* – Peça de cabo flexível com um conector RJ45 em cada extremidade.





Fonte: <http://in.rsdelivers.com/product/krone/7022-1-056-24/24-way-cat6-utp-modular-patch-panel/5123057.aspx>

FIGURA 10 – Detalhe *patch-panel* com os cabos sendo ligados na parte detrás.

A figura 11 mostra em detalhes a organização dos *patch-cords* ligados nos *patch-panels* no *rack*. Possui *patch-panel* em formato de “V” e os tradicionais.



Fonte: [http://www.electralink.com/content/includes/gallery/Rack-GSPanelTerminations\\_Systimax\\_BIG.jpg](http://www.electralink.com/content/includes/gallery/Rack-GSPanelTerminations_Systimax_BIG.jpg)

FIGURA 11 – Detalhe de um *rack* com *patch-panel*.

O cabeamento horizontal é um *link* entre o *patch-panel* e à tomada da área de trabalho. Uma vez instalado, não pode mais ser alterado. Todas as modificações devem ser feitas na sala de comunicação alterando o *patch-cord* [6]. A área de trabalho é o espaço delimitado para a instalação da rede que permita a sua utilização por um usuário. É



necessário esboçar o *layout* das disposições dos setores e a quantidade de estações de trabalho, para assim definir uma malha de cabos que os atenda, lembrando que não se devem ultrapassar os 90 metros [6].

O cabeamento *backbone* consiste em cabos para a ligação de salas de comunicação. Estas salas podem estar no mesmo andar ou em distâncias maiores. A limitação do cabo metálico é de 100 metros, se ultrapassada essa distância será necessária à utilização de fibra óptica [6].

## 7.2 Cabeamento Metálico

Os cabos metálicos são agrupados em categorias nomeadas de “cat”, com base em algumas especificações. Algumas categorias foram atualizadas com mais esclarecimentos ou padrões de teste (por exemplo, 5e, 6-a). Essas categorias servem para identificar facilmente que tipo de cabo será necessário para uma aplicação específica. Os fabricantes são obrigados a aderir aos padrões [37].

As diferenças nas especificações do cabo não são tão fáceis de ver como mudanças físicas. Por isso, analisaremos o que cada categoria suporta. Abaixo está a tabela 3 para referência das características dos cabos [37].

TABELA 3 – Comparação das categorias de cabos de rede.

	Distância (metros)	Velocidade			Mhz
		100Mb/s	1Gb/s	10Gb/s	
Cat-5	100	x			100
Cat-5e	100	x	x		100
Cat-6	100 55 para 10Gb/s	x	x	x	250
Cat-6a	100	x	x	x	500

Fonte: <http://www.howtogeek.com/70494/what-kind-of-ethernet-cat-5e6a-cable-should-i-use/>

À medida que o número da categoria aumenta, o mesmo acontece com a velocidade (Mb/s<sup>4</sup> e Gb/s<sup>5</sup>) e Mhz (mega-hertz) do fio. Isso não é uma coincidência, porque cada categoria traz métodos mais rigorosos para eliminar *crosstalk*<sup>6</sup> e adicionar isolamento entre os fios.

<sup>4</sup> Mb/s – Megabit por segundo

<sup>5</sup> Gb/s – Gigabit por segundo

<sup>6</sup> *Crosstalk* – Interferência devido a um processo chamado de indução entre um cabo e outro.

## 7.3 Fibra óptica

A fibra óptica é um material isolante elétrico feito de um filamento extremamente fino e flexível, de vidro ultrapuro ou plástico (materiais com alta resistência ao fluxo de corrente elétrica). Possui uma estrutura simples, composta por capa protetora, interface e núcleo. Está sendo muito utilizada nas telecomunicações e exames médicos, como endoscopias e cirurgias corretivas de problemas visuais, entre outras aplicações possíveis [38].

São dois tipos mais comuns, variando o tipo de fonte luminosa usada e a quantidade de sinais que podem ser emitidos dentro da fibra:

- Monomodo
- Multimodo

No tipo monomodo, a propagação da luz é feita por um único modo, pois a fibra tem um núcleo pequeno. A largura da banda utilizada é maior e existe uma menor dispersão da luz laser emitida, tendo a transmissão de sinais a grandes distâncias. Apesar da qualidade da fibra monomodo ser superior, a fabricação é mais cara e o manuseio é difícil [38].

No tipo multimodo além do laser, pode-se utilizar como fonte o LED<sup>7</sup>. Possuem um diâmetro maior, assim podendo transmitir mais de um sinal por filamento [38].

De acordo com a Meridian Technologies, existem dois tipos diferentes de fibra multimodo: de 50/125µm e 62.5/125µm. Cada uma possui as fibras com características padrão e as melhoradas que são chamadas de laser otimizado [39]. A tabela 4 demonstra as características das fibras multimodo.

TABELA 4 – Características multimodo

Fibra tipo multimodo	Comprimento da onda	Padrão (62.5/125µm)	Laser otimizado (62.5/125µm)	Padrão (50/125µm)	Laser otimizado (50/125µm)
Largura da banda (MHz-km)	850nm	160	200-500	500	1000-2000
	1300nm	500	500	600-1000	500

Fonte: [http://www.meridian-tech.com/downloads/Articles/Fiber%20Bandwidth%20\(MM%20vs.%20SM\).pdf](http://www.meridian-tech.com/downloads/Articles/Fiber%20Bandwidth%20(MM%20vs.%20SM).pdf)

A tabela 5 demonstra as distâncias aproximadas em metros em relação ao comprimento de onda [39].

<sup>7</sup> LED - Diodo emissor de luz.

TABELA 5 – Distância aproximada em metros fibras multimodo

<b>Tipo de fibra</b>	<b>Comprimento de onda</b>	<b>Distância de transmissão aprox. (Metros)</b>
<b>Padrão (62.5/125µm)</b>	<b>850nm</b>	<b>200</b>
	<b>1300nm</b>	<b>660</b>
<b>Padrão (50/125µm)</b>	<b>850nm</b>	<b>660</b>
	<b>1300nm</b>	<b>1000</b>
<b>Laser otimizado (50/125µm)</b>	<b>850nm</b>	<b>2500</b>
	<b>1300nm</b>	<b>660</b>

Fonte: <http://www.meridian->

[tech.com/downloads/Articles/Fiber%20Bandwidth%20\(MM%20vs.%20SM\).pdf](http://tech.com/downloads/Articles/Fiber%20Bandwidth%20(MM%20vs.%20SM).pdf)

## 8 COMBATE E PREVENÇÃO DE INCÊNDIOS

O sistema de combate e prevenção contra incêndios pode ser composto por procedimentos de brigadas de incêndio, de sistema de detecção de fumaça, gases inibidores e extintores. Além de atender as normas exigidas pelo corpo de bombeiros local, o sistema de combate de incêndio não poderá causar danos nos equipamentos em caso de incêndio [6].

No mercado existem vários tipos de extinguidores de incêndio, sendo eles:

- Gás FM-200
- Gás IG-55
- Gás CO<sub>2</sub>

### 8.1 Gases inibidores de incêndio

O Gás químico FM-200 é uma das melhores soluções de combate a incêndio para as salas de equipamentos de TI, o sistema de combate com gás será conectado a um sensível sistema de detecção e será o primeiro a ser acionado. O gás é espalhado pela área, não deixando resíduos que danifiquem os equipamentos sensíveis ou que requeiram um custo de limpeza dos equipamentos [32].

O Gás inerte IG-55 é natural sem cor e inodoro. Por ser um gás inerte não ataca a camada de ozônio e não faz aumentar o efeito estufa. Seu desempenho é reduzir o oxigênio do ambiente até que o incêndio se extingue [32].

O Dióxido de Carbono (CO<sub>2</sub>) também é um gás natural, não conduz a corrente elétrica, atua na inibição da combustão efetuando a troca de oxigênio, não gera resíduo e é muito eficiente na proteção de equipamentos eletrônicos. Por efetuar a troca do oxigênio do ambiente acaba gerando risco de asfixia nas pessoas que se encontrarem na área durante a ação do CO<sub>2</sub>. Normalmente é adotado um sistema de proteção automático com temporizador [33].

Na figura 12 mostra uma bateria (conjunto) de cilindros de FM-200 [34].



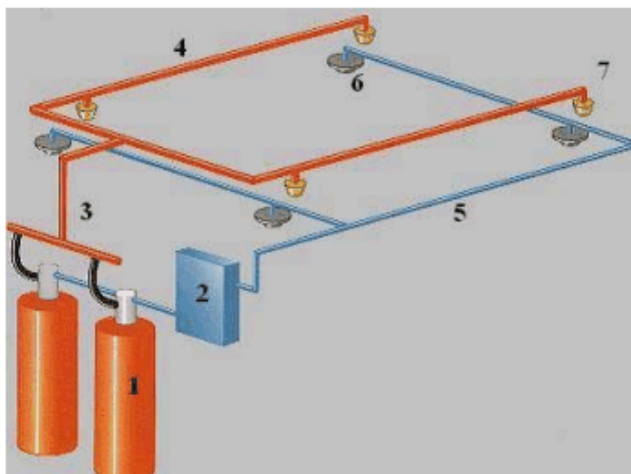
Fonte: <http://www.indiamart.com/amcon-techno/products.html>

FIGURA 12 – Detalhe de bateria de cilindros FM-200.

## 8.2 Sistema fixo de proteção contra incêndio

A proteção contra incêndio de equipamentos ou instalações críticas em uma empresa tem sido baseada cada vez mais em sistemas fixos de supressão utilizando agentes extintores gasosos. Os sistemas fixos de proteção contra incêndio são aqueles cujo propósito é a supressão local de um incêndio, através de uma instalação fixa geralmente de atuação automática. Estes sistemas destinam-se efetuar uma descarga de gás de cilindros de armazenamento, através de tubagem fixa até o local de risco. Os sistemas de proteção fixos funcionam automaticamente, sendo necessário ter ligação a um sistema de detecção automática de incêndio (detectores de fumaça ou de calor) [32].

A figura 13 mostra os itens do sistema fixo de proteção contra incêndio: 1 - cilindro de gás, 2 - Painel de controle, 3 - Coletor de gás, 4 - Circuito de Extinção, 5 - Circuito de detecção de incêndio, 6 - Detector de incêndio e 7 - Difusores de gás [33].



Fonte: <http://www.ajinkyafire.com/clean-agent-systems.html>

FIGURA 13 – Detalhe sistema fixo de proteção contra incêndio.

## 9 SEGURANÇA E CONTROLE DE ACESSO

Para obter uma boa segurança dentro e fora do Data Center, novas tecnologias estão surgindo e sendo melhoradas a cada momento. É necessário saber qual é a real necessidade de segurança do Data Center, pois quanto maior for o nível de segurança maior será o investimento [6].

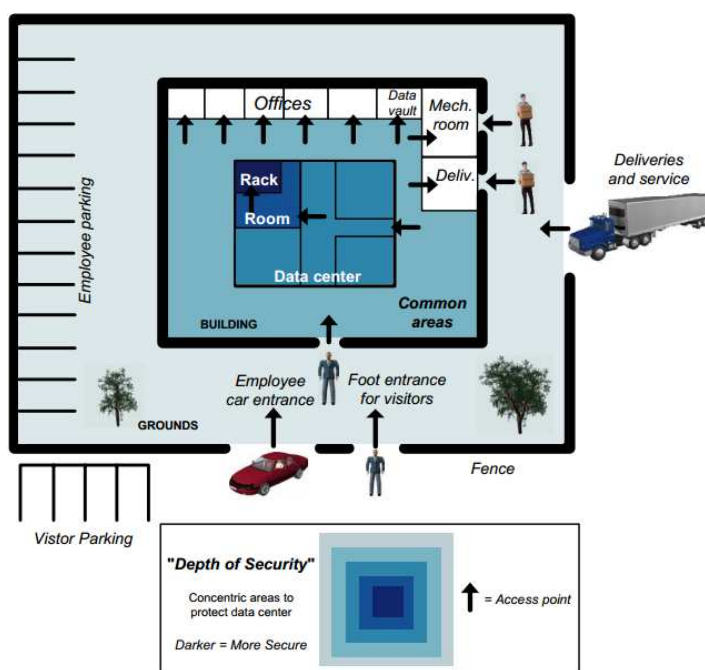
Existem diversos tipos de segurança e controle de acesso, sendo eles:

- Monitoramento por Circuito fechado de TV (CFTV).
- Sensores de presença.
- Leitores Biométricos.
- Alarmes contra invasão.

### 9.1 Segurança em Camadas

Zonas concêntricas podem ter diferentes métodos de acesso ou métodos cada vez mais exigentes, oferecendo proteção adicional ao chamado segurança em profundidade. Com a segurança em profundidade, uma área interna é protegida tanto por seus próprios métodos de acesso, quanto pelas áreas que a rodeiam.

Na figura 14 podemos observar uma empresa onde as áreas mais escuras são as áreas mais seguras [35].



Fonte: [http://www.apcmedia.com/salestools/SADE-5TNRPL\\_R1\\_EN.pdf](http://www.apcmedia.com/salestools/SADE-5TNRPL_R1_EN.pdf)

FIGURA 14 – Segurança em camadas

### 9.1.1 Métodos de identificação confiabilidade x custo

Os métodos de identificação de pessoas são divididos em três categorias gerais de confiabilidade cada vez maiores, porém, isso refletirá em um aumento significativo no custo do equipamento [35]:

- O que você tem (*What you have*)
- O que você sabe (*What you know*)
- Quem você é (*Who you are*)

O método “o que você tem” (*What you have*) é o menos confiável e mais acessível. É definido por algo que a pessoa usa ou leva consigo, como por exemplo, uma chave, um cartão ou um pequeno objeto (*token*<sup>8</sup>). Pode ser uma chave de metal ou um cartão com um processador de bordo que troca informações com um leitor (*Smart card*).

Pode-se utilizar um cartão com uma banda magnética que contenha informações sobre a pessoa que terá acesso. Neste cartão contém um transmissor ou receptor que se comunica com o leitor a partir de uma distância curta (cartão de proximidade ou *token* de proximidade).

Este método é uma forma menos confiável de identificação, já que não há garantia de que ele está sendo usado pela pessoa correta, pois pode ser compartilhado, roubado ou perdido.

O método “o que você sabe” (*What you know*), é mais confiável e com um custo moderado. É uma senha, código ou procedimento que será utilizado para abrir uma fechadura codificada, realizar uma verificação em um leitor de cartão ou acessar um computador através de um teclado.

Uma senha apresenta um dilema de segurança, se for fácil de lembrar, ela provavelmente vai ser fácil de adivinhar, se for difícil de lembrar, ela provavelmente vai ser difícil de adivinhar, por este motivo irá provavelmente ser escrita, reduzindo a sua segurança.

O método “o que você sabe” é mais confiável do que “o que você tem”, mas senhas e códigos ainda podem ser compartilhados, e se forem escritos carregam o risco de serem descobertos.

O método “quem você é” (*Who you are*), é o mais confiável. Refere-se à identificação por reconhecimento de características físicas únicas e naturais. A tecnologia utilizada para esta identificação é a biometria.

---

<sup>8</sup> Token - Um dispositivo eletrônico gerador de senhas.

## 9.2 Biometria

A biometria é a ciência e tecnologia de medição e análise de informações biológicas, em TI, a biometria se refere a tecnologias que medem e analisam as características do corpo humano, tais como impressões digitais, retinas e íris, padrões de voz, padrões faciais e medições de mão, para fins de autenticação.

Com a proteção de biometria, os profissionais de TI podem obter o controle de acesso físico e lógico. Com a segurança física, um dispositivo biométrico pode ser configurado para abrir uma porta do Data Center para proteger seus elementos físicos. Controle de acesso lógico protege a rede remotamente através de dispositivos instalados em computadores individuais que farão este tipo de acesso [21].

Leitores de impressão digital, há anos têm sido os mais populares dispositivos de biometria no mercado, pois tem um custo mais acessível, fácil instalação e uma boa confiabilidade [6].

Técnicas de exploração biométrica foram desenvolvidas para uma série de recursos humanos que se prestam a uma análise quantitativa [35]:

- Iris (padrão de cores)
- Face (posição relativa dos olhos, nariz e boca)
- Retina (padrão de vasos sanguíneos)
- Manuscrito (dinâmica da caneta como ela se move)
- Voz

## 9.3 Monitoramento CFTV

De acordo com Paulo Sérgio Marin a vigilância da empresa é dividida em dois tipos normalmente, sendo vigilância física, feita por seguranças e vigilância eletrônica, por equipamentos eletrônicos e CFTV, podendo ser analógicos ou digitais sendo câmeras IP [6].

O sistema de vigilância CFTV em um Data Center deve apresentar as seguintes funções e devem cobrir as seguintes áreas [6]:

- Permitir a segurança e o monitoramento de pessoas.
- Centralizar o monitoramento de forma simultânea de todas as câmeras em uma sala para controle.
- Manter registros visuais das áreas monitoradas durante eventos de alarme.
- Manter a gravação com uma forma de evidências de ações criminosas como provas.



- Manter gravações de imagens em áreas monitoradas e a atividade dos empregados.
- Áreas de circulação e acesso comum.
- Espaços de serviços.
- Salas técnicas (ar condicionado, telecomunicação e redes, cabines primárias, perímetros internos e externos).

É importante levar em consideração as instalações das câmeras em lugares adequados de acordo com a norma ANSI/BICSI-002 que traz alguns requisitos quanto à iluminação de certos espaços do Data Center para uma operação adequada de sistemas CFTV convencionais, conforme a tabela 6 [29].

TABELA 6 – Luminosidade mínima para CFTV em Data Center.

<b>Espaço do Data Center</b>	<b>Luminosidade mínima (lux)</b>
Perímetros externos	1.5
Perímetros internos	4
Entradas de veículos	10
Espaços de acesso restrito	20
Estacionamento	10

Fonte: Paulo Sérgio Marin (2011)

## 10 CONCLUSÃO

O Data Center é o coração de muitas empresas. Nestas, todos os processos dependem de seu bom funcionamento para uma boa evolução das atividades. Os melhores Data Centers são aqueles que permanecem disponíveis durante um longo período de tempo e que sejam seguros contra violações. Para que o Data Center alcance a elevada confiabilidade e disponibilidade, ele deve ser planejado e estruturado seguindo as melhores técnicas disponíveis no mercado.

Com base nos dados coletados, foram apresentados layouts de Data Centers, tanto para projetos de grande porte, quanto para projetos básicos, onde foi possível observar que cada parte da infraestrutura de um Data Center tem fundamental importância no projeto de construção e que para atingir a máxima eficiência, ele deve ser fundamentado nas normas apresentadas neste trabalho, pois como foi visto, estas diminuem os riscos de falhas e garantem um maior desempenho, evitando paradas inesperadas e perda de dados.

Com a pesquisa, foi possível compreender que não é obrigatório implantar de imediato todas as recomendações contidas neste trabalho, visto que cada projeto deverá levar em conta o orçamento da empresa e a sua disponibilidade de recursos. Devem ser analisadas as reais necessidades de cada empresa. Os projetos de atualizações de Data Centers também podem ser realizados em etapas, de acordo com as necessidades de melhorias.

Quando analisadas as melhores práticas e técnicas mais utilizadas, assim como nos estudos de casos, pudemos concluir que com o avanço tecnológico e o aumento de dados das empresas, torna-se imprescindível a utilização de novas tecnologias.

Durante o desenvolvimento desta monografia, as maiores dificuldades encontradas foram acerca de fontes de informações, pois as empresas que possuem Data Centers não divulgam as técnicas utilizadas na construção, por serem informações sigilosas, que podem por em risco a segurança das mesmas. Na grade curricular do curso de Engenharia de Computação não foram abordados assuntos pertinentes a esta área de TI, exigindo estudos complementares.

Finalizando as pesquisas, foi possível selecionar as melhores práticas, baseadas em fundamentos teóricos e práticos, o que resultou neste documento que poderá ser utilizado como fonte de pesquisa para pessoas interessadas em começar um projeto de construção ou atualização de Data Center.

Pode-se ainda concluir que o presente trabalho possibilitou o estudo e o entendimento de práticas e técnicas para melhorar ou construir um Data Center seguro. Através da elaboração da análise bibliográfica, foi possível entender melhor as ferramentas

utilizadas nos projetos, além do entendimento global de como deve ser um Data Center seguro com maior disponibilidade.

As práticas e técnicas expostas, se implantadas, podem trazer melhorias e maior segurança, pois muitas empresas dependem do Data Center para manter suas atividades funcionando, contribuindo assim para a continuidade de seus negócios.

## REFERÊNCIAS BIBLIOGRÁFICAS

- [1] The Green Grid. Disponível em: <<http://www.networkworld.com>>. Acesso em: 26 abr. 2012.
  
- [2] Network World. Disponível em: <<http://www.thegreengrid.org>>. Acesso em: 26 abr. 2012.
  
- [3] IBM®. Disponível em: <[http://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe\\_PR360.html](http://www-03.ibm.com/ibm/history/exhibits/mainframe/mainframe_PR360.html)>. Acesso em: 10 mar. 2012.
  
- [4] MILLER, Rich. Data center knowledge. Disponível em: <<http://www.datacenterknowledge.com/archives/2012/01/23/google-spent-951-million-on-data-centers-in-4q/>>. Acesso em: 09 mar. 2012.
  
- [5] SOARES, Edileuza. Computerworld. Disponível em: <<http://computerworld.uol.com.br/negocios/2011/05/02/data-center-o-eterno-desafio-de-ganhar-espaco-e-cortar-custos/>>. Acesso em: 08 mar. 2012.
  
- [6] MARIN, Paulo S. Data centers: Desvendando cada passo: conceitos, projeto, infraestrutura física e eficiência energética. 1. ed. São Paulo: Érica, 2011.
  
- [7] VERAS, Manoel. Datacenter: Componente central da infraestrutura de TI. Rio de Janeiro: Brasport, 2009.
  
- [8] FURUKAWA. Disponível em: <[http://portal.furukawa.com.br/arquivos/i/itm/itmax/1184\\_GuiadeRecomendaAAao.PDF](http://portal.furukawa.com.br/arquivos/i/itm/itmax/1184_GuiadeRecomendaAAao.PDF)>. Acesso em: 18 abr. 2012.
  
- [9] Colocation America. Disponível em: <[http://www.colocationamerica.com/data\\_center/tier-standards-overview.htm](http://www.colocationamerica.com/data_center/tier-standards-overview.htm)>. Acesso em: 21 abr. 2012.
  
- [10] Techtarget. Disponível em: <<http://searchcio.techtarget.com/news/1312614/Five-tips-on-selecting-a-data-center-location>>. Acesso em: 10 mai. 2012.

- [11] Portugal Telecom. Disponível em: <<http://www.telecom.pt/NR/rdonlyres/3855264A-959C-4642-9710-DCA9573365EE/1458346/NovoConceitodeDataCenter.pdf>>. Acesso em: 30 mai. 2012.
- [12] Continuity Central. Disponível em: <<http://www.continuitycentral.com/feature0334.htm>>. Acesso em: 24 mai. 2012.
- [13] DELL. Disponível em: <<http://www.dell.com/br/empresa/p/powerededge-4020s/pd>>. Acesso em: 31 mai. 2012.
- [14] Techlider. Disponível em: <<http://kfxpower.wordpress.com/2011/01/19/seis-tendencias-em-data-center/>>. Acesso em: 31 mai. 2012.
- [15] Dicas de Decorações. Disponível em: <<http://dicasdedecoracoes.com/piso-elevado-tate/>>. Acesso em: 01 jun. 2012.
- [16] EXAME.com. Disponível em: <<http://exame.abril.com.br/tecnologia/noticias/ibm-vende-data-centers-em-containers>>. Acesso em: 14 jun. 2012.
- [17] Lautan Kencana. Disponível em: <<http://lautankencana.com/data-center-solutions>>. Acesso em: 14 jun. 2012.
- [18] Grupo POLICOM. Disponível em: <<http://www.grupopolicom.com.br/Arquivo/CATALOGO%20DC%20-%20A%20EDICAO.pdf>>. Acesso em: 15 jun. 2012.
- [19] Computerworld. Disponível em: <<http://computerworld.uol.com.br/tecnologia/2011/05/12/data-center-movel-e-a-novidade-da-ibm-para-o-brasil/>>. Acesso em: 20 jul. 2012.
- [20] IBM Disponível em: <<http://www-03.ibm.com/press/br/pt/presskit/34498.wss>>. Acesso em: 20 jul. 2012.
- [21] Tech Target Disponível em: <<http://searchdatacenter.techtarget.com/news/1233541/Data-center-physical-security-drives-biometrics-technology>>. Acesso em: 25 jul. 2012.

- [22] EMERSON Network Power Disponível em:  
<<http://www.emersonnetworkpower.com/en-US/Brands/Liebert/Documents/White%20Papers/UPS%20Trap%20Doors%20for%20SMB.PDF>>. Acesso em: 12 set. 2012.
- [23] ACECO TI Disponível em:  
<[http://www.acecoti.com.br/new/solucoes\\_infra\\_energia.asp](http://www.acecoti.com.br/new/solucoes_infra_energia.asp)>. Acesso em: 12 set. 2012.
- [24] UOL Disponível em: <<http://tecnologia.uol.com.br/ultimas-noticias/redacao/2010/04/27/com-capacidade-para-30-mil-servidores-novo-data-center-do-uol-coloca-computacao-verde-em-pratica.jhtm>>. Acesso em: 12 set. 2012.
- [25] Faculdade Vila Matilde Disponível em:  
<<http://www.faatesp.edu.br/publicacoes/NBR-5419.pdf>>. Acesso em: 02 out. 2012.
- [26] UNICAMP Disponível em:  
<[http://www.iar.unicamp.br/lab/luz/ld/normas%20e%20relat%F3rios/NRs/nbr\\_5410.pdf](http://www.iar.unicamp.br/lab/luz/ld/normas%20e%20relat%F3rios/NRs/nbr_5410.pdf)>. Acesso em: 02 out. 2012.
- [27] IBDA Disponível em:  
<<http://www.forumdaconstrucao.com.br/conteudo.php?a=28&Cod=607>>. Acesso em: 28 set. 2012.
- [28] Infra Engenharia Disponível em: <<http://www.infraengenharia.com.br>>. Acesso em: 8 out. 2012.
- [29] BICSI advancing information technology systems Disponível em:  
<[http://www.bicsi.org/uploadedfiles/BICSI\\_002\\_Sample.pdf](http://www.bicsi.org/uploadedfiles/BICSI_002_Sample.pdf)>. Acesso em: 8 out. 2012.
- [30] Tech Target Disponível em: <<http://searchdatacenter.techtarget.com/tip/Using-ASHRAE-specs-for-data-center-metrics>>. Acesso em: 11 out. 2012.
- [31] NETRiver Disponível em: <<http://www.netriver.net/seattle-data-center/data-center-hvac>>. Acesso em: 11 out. 2012.
- [32] R-Secure Disponível em: <<http://www.r-secure.com/>>. Acesso em: 17 out. 2012.
- [33] Allianz Disponível em: <<http://www.allianz.pt>>. Acesso em: 19 out. 2012.

- [34] Narpad Corporation Disponível em: <<http://www.narpad.com/tabid/88/Default.aspx>>. Acesso em: 19 out. 2012.
- [35] APC Disponível em: <[http://www.apcmedia.com/salestools/SADE-5TNRPL\\_R1\\_EN.pdf](http://www.apcmedia.com/salestools/SADE-5TNRPL_R1_EN.pdf)>. Acesso em: 8 nov. 2012.
- [36] Gestão Dinâmica Disponível em: <<http://www.gestaodinamica.com.br/pt-br/faq-suporte-em-informatica/o-que-e-e-porque-utilizar-cabeamento-estruturado.html>>. Acesso em: 13 nov. 2012.
- [37] How To Geek Disponível em: <<http://www.howtogeek.com/70494/what-kind-of-ethernet-cat-5e6a-cable-should-i-use/>>. Acesso em: 14 nov. 2012.
- [38] Tecmundo Disponível em: <<http://www.tecmundo.com.br/web/1976-o-que-e-fibra-optica-.htm#ixzz2CWfdHOK7>>. Acesso em: 16 nov. 2012.
- [39] Meridian Technologies Disponível em: <[http://www.meridian-tech.com/downloads/Articles/Fiber%20Bandwidth%20\(MM%20vs.%20SM\).pdf](http://www.meridian-tech.com/downloads/Articles/Fiber%20Bandwidth%20(MM%20vs.%20SM).pdf)>. Acesso em: 16 nov. 2012.