# SEGURANÇA FÍSICA EM DATACENTERS: ESTUDO DE CASO

Rogério Carvalho Rosa [1]
Maria Cristina Aranda [2]
Pedro Domingos Antoniolli [3]

Artigo recebido em março de 2017

## 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. Segurança física.

## 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.

**Key words**: Datacenter. Tier. Classification. Information security. Physical security.

[1] Egresso do curso de Tecnologia em Segurança da Informação da Fatec Americana. Email: rogeriorosa91@hotmail.com.
[2] Docente do curso de Tecnologia em Segurança da Informação da Fatec Americana. Email: mcrisaranda@gmail.com.
[3] Docente do curso de Tecnologia em Segurança da Informação da Fatec Americana. Email: pedroantoniolli@yahoo.com.br.

## 1 INTRODUÇÃO

A Tecnologia da Informação (TI) evolui de forma significativa ao longo dos anos. O Instituto Brasileiro de Geografia e Estatística – 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 crítica nos ambientes empresarias, nos quais há crescente dependência de TI, seja para proporcionar agilidade, integração ou ainda melhor qualidade da informação. Nesses ambientes, a segurança da informação é fundamental, seja na criação, manuseio, armazenamento, ou descarte desta informação.

Uma pesquisa global em segurança da informação realizada pela empresa PWC (2014), constatou que a informação tem sido considerada um dos ativos mais valiosos da empresa. Esse valor é proveniente tanto pelo conhecimento que a informação traz, como também pela pronta aplicação dessa informação no processo decisório (TURBAN; VOLONINO, 2013). Este trabalho problematiza a busca de melhorias de segurança física de datacenters de empresas de médio porte, uma vez que o comprometimento das informações armazenadas nestes locais pode gerar perdas de grande monta para tais organizações, ameaçando inclusive a sua sustentabilidade (TURBAN; VOLONINO, 2013).

## 2 REFERENCIAL TEÓRICO

Inicia-se o referencial teórico pela conceituação de segurança da informação.

### 2.1 Segurança da Informação

Aurélio (2001) conceitua segurança como o 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-se de medidas adequadas para assegurar a boa condução das atividades nesse ambiente.

Uma vez que a informação empresarial pode ser manipulada de diversas formas, e passa por diferentes ativos de TI, deve ser alvo de mecanismos que evitem com que sofra algum tipo de acesso indevido (SEMOLA, 2003).

Segundo a norma ISO/IEC 27002 (2013), a segurança da informação é a proteção da informação contra ameaças, no sentido de garantir a continuidade do negócio, minimizando riscos para este e maximizando os beneficios para a empresa, o que requer a adoção de um conjunto adequado de mecanismos de controle, incluindo políticas, processos, procedimentos, e estruturas organizacionais.

Com base em ISO/IEC 27002 (2013), a Segurança da Informação possui alguns princípios básicos: 1) confidencialidade - a informação não deve ser revelada às pessoas não autorizadas; 2) integridade - garantir a exatidão da informação; 3) disponibilidade: - a informação deve estar disponível a quem tiver direito de acessá-la; 4) autenticidade - garantía da identidade do usuário que a manipulou; 5) não repúdio - rejeição ou interrupção de acesso autorizado.

Dessa forma, é fundamental que haja nas Organizações políticas de segurança da informação que, de acordo com 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". Nesse sentido, uma ameaça ocorre sempre que houver a quebra de um ou mais principios descritos anteriormente (CERTBR, 2003).

Para Fraser (1997, p.7), "a política de segurança da informação constitui-se em documento formal, com procedimentos, regras e recursos para o manuseio adequado das informações empresariais".

Nesse sentido, Campos (2006) afirma que a política de segurança da informação deve conter um conjunto de regras para servir como premissas do comportamento das pessoas no tocante à segurança da informação, visando a proteção das informações e dos recursos tecnológicos da empresa, e 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. O autor reforça ainda que uma política de segurança deve estar integrada às demais políticas da empresa, bem como com o planejamento estratégico, e metas. Campos (2006) afirma que a estrutura de uma política de segurança da informação compreende um conjunto de diretrizes, formadas por normas/regras, e tais normas por seus procedimentos associados, que devem ser seguidos por quem faz uso dessa política.

Para Ferreira (2003), existem três tipos de políticas de segurança: 1) regulatória - especificações legais, descrevendo detalhes sobre a maneira de se executar determinada atividade e responsabilidades / sanções por não cumprimento; 2) consultiva - auxilia e suporta a execução de determinada atividade, sugerindo métodos e ações, e; 3) informativa - na qual não existem sanções se não for cumprida, porém pode contemplar advertências caso tais informações sejam ignoradas.

## 2.2 Segurança em *Datacenters*

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. Segundo Marin (2011), um *datacenter* compreende um ambiente no qual estão equipamentos que armazenam informações críticas para a continuidade do negocio de uma ou mais organizações, independentemente do setor em que atuam. Para Paloalto (2016), um *Datacenter* centraliza as operações de TI de uma empresa, armazenando e gerenciando seus dados. Nesse sentido, há normas específicas para determinar os criterios de segurança dos *Datacenters*, entre essas a ANSI/TIA-942. A TIA (*Telecommunications Industry Association*) é uma organização que representa a indústria da informação e da comunicação global de tecnologia, desenvolvendo normas, iniciativas políticas, oportunidades de negócios, inteligência de mercado, e eventos, tendo seu foco em melhorias em telecomunicações, internet, cabeamento, satélites, e credenciada pela ANSI (*American National Standardas Institute*) (ANSI/TIA-942, 2005).

De acordo com Veras (2009), a ANSI/TIA-942 é uma norma que especifica os requisitos mínimos para a infraestrutura de *Datacenters*, de acordo com o grau de disponibilidade e redundância de sua infraestrutura.

Segundo a norma ANSI/TIA-942 (2005) existem quatro níveis de disponibilidade de infraestrutura do *datacenter (*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 (o elo mais vulnerável).

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

a) N: Equipamento, caminho, serviço necessários sem nenhuma redundância;

b) N+1: Equipamento, caminho, serviço necessário mais um de redundância. Esse tipo de redundância não irá interromper a operação caso ocorra a falha ou manutenção de um único equipamento, caminho ou serviço (ex.: Energia Elétrica + Nobreak);

c) 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.: Energia Elétrica + Nobreak + Gerador);

d) 2N: Dois equipamentos, caminho, serviço. Se apenas um equipamento apresentar falha ou manutenção, não ocasionará nenhum impacto na operação (ex.: Energia Elétrica A + Energia Elétrica B);

e) 2(N+1): Dois equipamentos, caminho, serviço, e mais redundâncias para cada um dos elementos, tolerante a falhas, e nenhum impacto na operação (ex.: Energia Elétrica A + Energia Elétrica B + Nobreak A+ Nobreak B + Gerador A + Gerador B).

De acordo com a norma ANSI/TIA-942 (2005), os quatro níveis de classificação dos *Datacenters* variam de acordo com a sua infraestrutura e disponibilidade, conforme se observa na Figura 1.

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 |

Figura 1 - Níveis de *Datacenter*
Fonte: Zucchi (2013)

A norma ANSI/TIA-942 (2005) afirma ainda que o *Datacenter* classificado como TIER I (Básico) está sujeito às interrupções em suas atividades, tanto as planejadas quanto as não. Tal *datacenter* pode possui quadro de distribuição de energia e refrigeração, e pode ter ou não um piso elevado, *nobreak*, gerador (motor). Se o *Datacenter* desse nível possuir um *nobreak* ou gerador, estes serão normalmente sistemas de módulo único, o que ocasionará pontos de falhas. Nesses casos, para se realizar a manutenção preventiva ou reparação dos equipamentos, os sistemas são desligados (ANSI/TIA-942, 2005).

De acordo com informações da norma ANSI/TIA-942 (2005), os *Datacenters* TIER II (componentes redundantes) são um pouco menos suscetíveis às interrupções planejadas ou não. Possuem piso elevado, *nobreaks* e geradores, na estrutura de (N+1), porém em um único segmento. Quando se faz necessária a manutenção, ocorre então o desligamento dos sistemas de energia.

O *Datacenter* TIER III (paralelamente sustentável) possui equipamentos de refrigeração e alimentação de energia 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, se o investimento for justificável.

O *Datacenter* TIER IV (tolerante a falhas) possui equipamentos de refrigeração e alimentação de energia redundantes e ativos, proporcionando tolerância às falhas (ANSI/TIA-942, 2005). Em TIER IV, equipamentos que não são construídos com múltiplas entradas de energia devem utilizar uma chave de transferência automática para que não haja nenhum tipo de interrupção (ANSI/TIA-942, 2005).

O TIER IV possui capacidade para suportar atividades planejadas de manutenção, sem interrupção, pois os equipamentos de elétrica e refrigeração possuem redundância 2(N+1). Assim, o *Datacenter* TIER IV terá inatividade apenas quando acionado o alarme de incêndio, ou iniciado o desligamento de emergência (EPO), em situação de desastr.

De acordo com ANSI/TIA-942 (2005), as classificações dos *Datacenters* são formadas pela avaliação individual de quatro áreas: 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*.

### 2.2.1 Classificação na Área de Telecomunicações

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 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): a) falhas nos sistemas ou equipamentos do provedor de acesso; b) falha de manutenção no caminho e/ou sala dedicada aos provedores; c) falha em equipamentos de rede, *switches* ou roteadores (caso não haja redundância); d) um evento não planejado (catástrofe) pode ocorrer na sala de entrada ou na via de comunicação com a sala principal, interrompendo os serviços do *Datacenter*.

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 norma ANSI/TIA-942 (2005), são: a) os equipamentos dos provedores de acesso, ligados na mesma rede elétrica e apoiados por sistemas individuais de climatização, podem gerar indisponibilidade, caso um dos dois componentes (energía e climatização) venha a falhar; b) equipamentos dentro da sala principal ligados à mesma rede elétrica, e apoiados por sistemas individuais de contingencia (*nobreaks*), podem sofrer interrupções se o nobreak ou rede elétrica falharem; c) evento não planejado (catástrofe) pode ocorrer na sala de entrada ou na sala principal, ou no caminho de interligação das salas.

Além desses requisitos, o TIER III de infraestrutura para Telecomunicações deve ser servido por no mínimo dois provedores de acesso, que devem seguir a mesma regra de distância e de caminhos distintos (ANSI/TIA-942, 2005).

| 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 |

Quadro 1 - Requisitos da Área de Telecomunicações por Nível de Classificação
Fonte: Adaptado de ANSI/TIA-942 (2005)

Um outro ponto recomendado é que todo o cabeamento e equipamentos, além de identificados, devem ser documentados (FURUKAWA, 2016).

A infraestrutura de Telecomunicações TIER IV deve 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. 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.

No Quadro 1, notam-se os principais requisitos dos quatro níveis de classificação da infraestrutura de Telecomunicação (ANSI/TIA-942, 2005).

### 2.2.2 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, além dos requisitos do TIER I, uma proteção mínima contra eventos físicos, intencionais, acidentais, naturais, ou falha humana (MARIN, 2011).

Ainda de acordo com o autor, as proteções mínimas são: a) barreiras de vapor nas paredes e tetos da sala principal dos equipamentos; b) todas as portas devem ser de madeira maciça, com armação de metal; c) todas as paredes devem ter a mesma altura; d) carga mínima suportada deve ser de no mínimo 8,4 kPA nas áreas dos equipamentos, de acordo com a norma GR-63-CORE. De acordo com Marin (2011), o TIER III deve possuir um conjunto de proteções específicas contra eventos físicos, intencionais, acidentais, naturais ou falha humana, sendo: a) entradas redundantes no *Datacenter*; b) acessos redundantes, com pontos de verificação para garantir o acesso separado de fornecedores e funcionários; c) não debe haver janelas no perímetro do *Datacenter*; d) a construção deve proporcionar proteção contra radiação eletromagnética; e) controle de acesso em todas as entradas, com apoio de sistemas de informação; f) os *Datacenters* devem ser protegidos por sistema de detecção de intrusão (sensor de movimento e/ou infravermelho), e monitorado por circuitos de câmeras fechado de televisão (CFTV); g) 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 para TIER III, o TIER IV da área de arquitetura deve possuir controle sobre todos os aspectos de suas instalações, incluindo local externo ao prédio para uma unidade de gerador, e próximo ao mesmo a existencia de uma área para armazenamento dos tanques de combustível utilizados pelo gerador (MARIN, 2011).

Os Quadros 2, 3, 4 se destinam às comparações dos quatro níveis de classificação da área de Arquitetura, com base na norma ANSI/TIA-942 (2005).

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

| 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 |

Quadro 2 - Requisitos da Área de Arquitetura (local) por Nível de Classificação
Fonte: Adaptado de ANSI/TIA-942 (2005)

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

| 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 |

Quadro 3 - Requisitos da Área de Arquitetura (Resistencia ao fogo) por Nível de Classificação
Fonte: Adaptado de ANSI/TIA-942 (2005)

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

| 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 |

Quadro 4 - Requisitos da Área de Arquitetura (Segurança) por Nível de Classificação
Fonte: Adaptado de ANSI/TIA-942 (2005)

### 2.2.3 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, e atendimento prioritário, assim como ocorre com os hospitais, que durante uma interrupção, recebem alta prioridade. Além disso, a alimentação deve ocorrer de modo subterrâneo, minimizando assim a exposição dos circuitos a raios, árvores, acidentes de transito, e vandalismo.

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 falha no fornecimento externo de energia. Os geradores devem estar configurados para fornecer a tensão e corrente adequados para os sistemas *nobreaks*. Adicionalmente, deverá ser fornecido sistema para a refrigeração do ambiente, evitando-se a sobrecarga térmica, e desligamento dos equipamentos (VERAS, 2009).

Ainda de acordo com Veras (2009), o combustível utilizado nos geradores deverá ser o diesel, por ter combustão mais rápida que o gás. Controles do armazenamento devem ser tomados, e o reabastecimento dos geradores deve ser monitorado para que não ocorram falhas. O sistema de *nobreaks* pode consistir em módulos individuais ou grupos de vários paralelos. Sistemas de baterias podem ser fornecidos para cada modulo, ou para um grupo de módulos (VERAS, 2009).

A norma ANSI/TIA-942 (2005) exige que a capacidade mínima de fornecimento de energía dos sistemas geradores de energia seja de 5 a 30 minutos, devido a eventos imprevisíveis, que possam ocasionar falhas nos geradores. Além disso, a estrutura dos geradores deve possuir um sistema de monitoramento capaz de identificar a capacidade atual de armazenamento das baterías, e gravar as tensões, impedância, ou resistência que passam para o sistema de UPS (ANSI/TIA-942, 2005).

Unidades de ar condicionado devem ser fornecidas para os sistemas de geradores, 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). 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).

Todos os equipamentos devem possuir mecanismo de aterramento e sistema contra raios, além de documentação sobre tais riscos (ANSI/TIA/EIA-J-STD-607-A (2002), que leva em conta a localização geográfica e tipo de construção do edifício. Tais requisitos 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.

Com base no cumprimento desses requisitos é possível definir o TIERs para a Elétrica. O TIER I fornece o mínimo de distribuição de energia para atender os requisitos da carga elétrica do *Datacenter*, o que implica em pouca ou nenhuma redundância, ocasionando a paralisação dos serviços, caso ocorra falha (ANSI/TIA-942, 2005). No TIER I podem ser utilizados geradores e sistemas de *nobreaks*, porém estes são sistemas de módulos únicos, e sem redundância. Em relação ao aterramento, embora não sendo necessário no TIER I, pode ser requerido para atender aos requisitos dos fabricantes dos equipamentos.

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 os circuitos/PDU que originam a energia recebida. É necessário o aterramento para o TIER II, e 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, incluindo geradores e sistemas de *nobreaks.* O armazenamento mínimo de combustível para os geradores deve ser suficiente para 72 horas de funcionamento.

Adicionalmente, Veras (2009) afirma que todos os equipamentos do *datacenter* devem possuir fontes redundantes, e/ou utilização de conversão automática, de preferencia com um sistema de monitoramento dos equipamentos, gerando alarmes em situações de não conformidade.

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 em qualquer falha, a carga seja migrada automáticamente para o outro equipamento, evitando-se interrupções na operação (ANSI/TIA-942, 2005).

A seguir, com base na normal ANSI/TIA-942 (2005), o Quadro 5, comparativos entre os níveis de classificação da área de Elétrica.

| 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 |

Quadro 5 - Requisitos da área de elétrica (sistema de UPS e geradores) por nível de classificação
Fonte: Adaptado de ANSI/TIA-942 (2005)

### 2.2.4 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 sua vida útil (ANSI/TIA-942, 2005).

Segundo Veras (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 refrigeração com água são mais adequados para *datacenters* maiores, porém requerem instalação de tubulações. Para Veras (2009), alguns equipamentos com altas cargas de calor podem exigir condutor de ar, ou pisos de acesso para fornecer o resfriamento adequado.

Para definir o sistema de proteção contra incêndio é preciso analisar os fatores de risco do *datacenter* (ANSI/TIA-942, 2005), que compreendem quatro dimensões: i) a segurança de pessoas ou propriedades afetadas pela operação; ii) a ameaça de fogo para os ocupantes em áreas confinadas ou à propriedade exposta; iii) a perda econômica do negócio devido ao tempo de inatividade; iv) a perda do valor do equipamento (ANSI/TIA-942, 2005).

Segundo Marin (2011), existem sistemas de detecção de alerta precoce para se evitar os danos e perdas durante os estágios iniciais de um incêndio, tais como sistema de detecção de fumaça por aspiração, ou por amostragem de ar que utilizam ionização convencional, ou ainda detectores fotoelétricos. Ainda de acordo com o autor, um sistema de extinção de incêndios fornece o próximo nível de proteção, proporcionando nível mais elevado de confiabilidade e mitigação de riscos. Adicionalmente, há sistemas de supressão de incêndio de agente limpo (gás não tóxico), que fornecem o mais alto nível de proteção, tanto pelo fato de não gerar residuos a serem eliminados (como a agua), e permitirem um retorno mais rápido à operação após um evento de princípio de incendio (MARIN, 2011).

A classificação da área de Mecânica, para o TIER I inclui unidade de ar condicionado simples com capacidade de resfriamento para manter a temperatura crítica do espaço e umidade relativa do ar, sem unidades redundantes, o que pode causar interrupção em caso de manutençoes. Caso o *datacenter* possua um gerador, todos os equipamentos de ar condicionado devem ser alimentados por ele (ANSI/TIA-942, 2005).

No TIER II, com base na norma ANSI/TIA-942 (2005), além dos requisitos do TIER I, 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, além de capacidade para opeação contínua, durante 365 dias / ano (ANSI/TIA-942, 2005).

Segundo Marin (2011), o sistema de climatização em um TIER III deve possuir os requisitos do TIER II, porém com unidades redundantes suficientes para mitigar falha ou manutenção no quadro elétrico. Este nível de redundância pode ser obtido quando fornecidas duas fontes de energia para cada unidade de ar condicionado (ANSI/TIA-942).

Para Veras (2009), os equipamentos de refrigeração do *datacenter* devem possuir redundância N+2.

Para TIER IV da área Mecânica, além do cumprimento dos requisitos do TIER III, há necessidade de redundância 2(N+1), conforme ANSI/TIA-942 (2005). No Quadro 6, as comparações entre os TIERs e seus respectivos requisitos da área de Mecânica.

| 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 |

Quadro 6 - Requisitos da área de elétrica (sistema de climatização e combate a incêndio) por nível de classificação
Fonte: Adaptado de ANSI/TIA-942 (2005)

## 3 MÉTODO

Marconi e Lakatos (2010) afirmam que uma pesquisa, para ser realizada, requer a definição clara e objetiva de um problema que motive sua realização. Assim, para este artigo a questão base investigada compreende: “Que requerimentos devem ser atendidos para que um Datacenter empresarial se enquadre no padrão de classificação em segurança da informação TIER IV?”.

Marconi e Lakatos (2010) explicam ainda que uma pesquisa pode ser classificada sob quatro perspectivas: natureza, forma de abordagem do problema, objetivos, e procedimentos técnicos. Em relação à sua natureza, esta pesquisa é considerada aplicada, por discutir os conceitos sobre segurança física de Datacenters, e aplica-los a um caso prático. Quanto à forma de abordagem do problema, utilizando-se ainda os criterios de Marconi e Lakatos (2010), este estudo é qualitativo, especificamente, porque não há intenção de utilizar técnicas e métodos estatísticos na interpretação dos resultados. Adicionalmente, o foco é na

interpretação dos dados, no processo e o que ele representa. Em relação aos objetivos, esta pesquisa caracteriza-se como uma pesquisa descritiva, pois busca, a partir da literatura, a identificação dos criterios nos quais o Datacenter em estudo se enquadra, bem como identificar os criterios requeridos para que o Datacenter apresente um melhor nível em termos de segurança da informação. Quanto aos procedimentos técnicos, esta pesquisa valeu-se de estudo bibliográfico, bem como análise documental, e observação direta, por conveniencia, uma vez que o pesquisador atua na empresa foco.

## 4 RESULTADOS E DISCUSSÃO

Com liderança no mercado em seu segmento, a Organização analisada nesse artigo, denominada aqui como Empresa X, iniciou suas atividades há mais de trinta anos, possuindo atualmente mais de 13 mil colaboradores no mundo. No Brasil a Empresa X possui filiais em diversos Estados. Sua estrutura de TI é composta de três áreas: i) telecomunicações, responsável pela rede e telefonía; ii) *datacenter*, responsável por todos os servidores de TI, e; iii) operações, responsável pela manutenção e *backup* dos dados corporativos. A segurança da informação é fundamental, uma vez que a unidade de negocios brasileira deve estar *compliant* com as normas da sua matriz, no Reino Unido. O estudo de caso é baseado, além da pesquisa bibliográfica, no conhecimento adquirido pelo pesquisador, por conveniência, pois ele atua como colaborador da Empresa X. Dessa forma, será analisado o cenário e toda a infraestrutura da Empresa X, bem como a análise de possíveis pontos de falhas.

O *datacenter* está localizado no 1º andar do edifício, juntamente com sanitários, e outros departamentos, com grande movimentação de pessoas. A área de telecomunicação possui um único caminho para acesso. Os *links* de *internet* e de voz possuem redundância de fontes (Link principal Operadora A + Link de redundância Operadora B). O cabeamento para esses *links* chegarem até a empresa é aéreo. A partir da entrada da empresa, o cabeamento é subterrâneo. Tal cenário apresenta riscos e pontos de falhas.

Os equipamentos dos provedores de serviços não possuem redundância, nem fontes de alimentação alternativas. Já os equipamentos considerados críticos da Empresa X, possuem redundância física e lógica, e fontes de alimentação redundantes. No entanto, apenas o cabeamento dentro da *datacenter* está identificado, o que está em desacordo com a norma TIA/EIA-606-A (2002).

Os pontos de falhas na área de telecomunicações, com risco de interrupção dos serviços estão identificados: a) nos equipamentos dos provedores de serviços; b) na manutenção no caminho de entrada dos serviços; c) nos eventos não planejados, que podem ocorrer no caminho de entrada dos serviços; d) no cabeamento aéreo, sujeito a acidentes e vandalismos.

Já em relação à arquitetura, é possível observar na Figura 2 que o *datacenter* se encontra ao lado de um banheiro, próximo às tubulações de água. Além disso, o *datacenter* possui janelas externas, reduzindo-se o nível de proteção e aumentando-se a temperatura do ambiente, também em desacordo com a norma ANSI/TIA-942. O acesso ao *datacenter* é único, através de porta de vidro, porém sem sistema de controle de acesso via *software*. Além dos itens citados, o *datacenter* não possui piso elevado, dificultando a passagem de novos cabos, bem como a organização dos existentes. Há monitoramento por camêras (CFTV). Alguns pontos de falhas na área de Arquitetura de *datacenter* compreendem: a) caso

tubulação de água apresente vazamentos, pode-se gerar riscos e danos aos equipamentos; b) falhas no circuito de câmeras podem ocasionar perda de registros de acessos ao *datacenter*; c) frágil proteção devido à existência de porta de vidro e janelas.

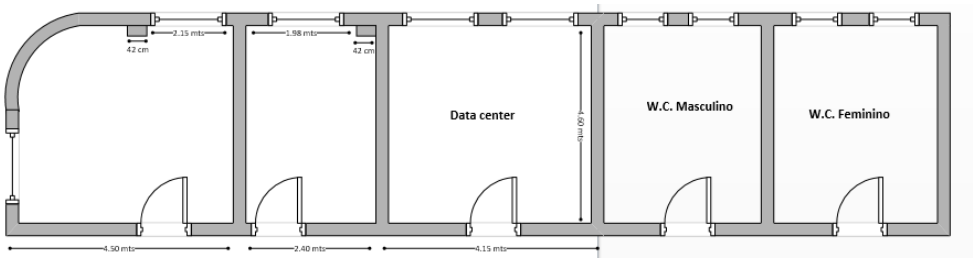


Figura 2 - Localização do Datacenter
Fonte: Próprio Autor

A terceira categoria de classificação é a área de elétrica, composta pela Companhia de energia elétrica da cidade, e um modulo único de gerador a óleo diesel, com sistema único de UPS (*nobreak*). A Companhia fornece a energia através de cabeamento aéreo até a entrada única da empresa. A partir desse ponto, todo o cabeamento é subterrâneo até a sala de entrada de energia elétrica, localizada a 20 metros do prédio. A sala não possui equipamentos para a climatização, onde estão os quadros de energia.

Conforme a Figura 3, 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 pela energia para todo o prédio, em caso de falta de energía externa. A sala do gerador não possui climatização.

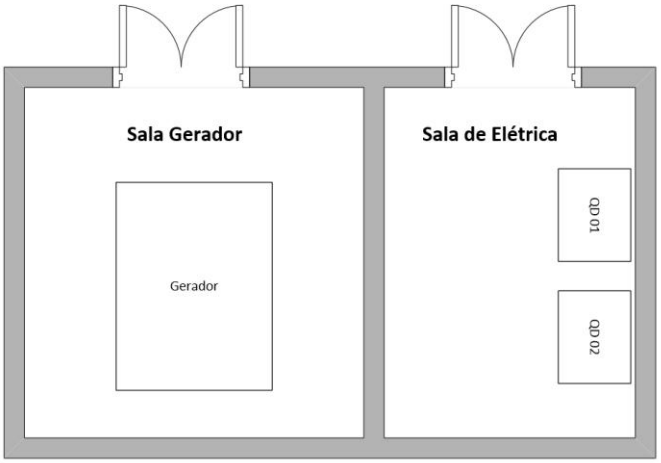


Figura 3 - Sala de entrada de energia elétrica e sala do gerador
Fonte: Próprio Autor

Dentro do *datacenter*, existe um modulo de UPS, responsável por estabilizar a energia elétrica originada do PDU-01 (quadro de energia dedicado), conforme a Figura 4, e repassar energia para os equipamentos. Caso haja falta de energía externa, o sistema de UPS é responsável pela energía de todo o edificio, até que o gerador entre em operação.

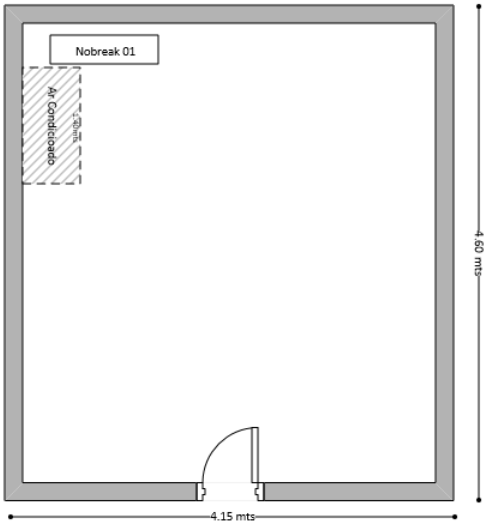


Figura 4 - *Layout* do *Datacenter*
Fonte: Próprio Autor

O sistema de UPS possui a capacidade atual de fornecimento de energía para o *datacenter* durante quarenta minutos, tempo suficiente para desligar todos os equipamentos de forma correta, caso o gerador não entre em operação. Na infraestrutura atual do *datacenter* não existe sistema de monitoramento da carga, e de condições da bateria. Um outro fato a se mencionar é que todos os *racks* e equipamentos possuem aterramento.

Alguns pontos de falhas na área de elétrica constituem-se de: a) falha ou manutenção no *nobreak*; b) falha ou manutenção do PDU-01 dentro do *datacenter*; c) falha ou manutenção nos quadros de elétrica; d) falha de manutenção no cabeamento elétrico; e) evento não planejado pode ocorrer no caminho de entrada do cabeamento elétrico.

Em relação à área de mecânica, o *datacenter* possui apenas um modulo convencional de ar condicionado. Caso venha a falhar e/ou passe por manutenção, todo o ambiente será afetado com aumento da temperatura. Não existe sistema de controle de umidade relativa do ar, nem equipamento para monitorar a temperatura do ambiente.

Referente aos sistemas de proteção contra incêndio, o *datacenter* possui apenas extintores de pó químico, estando vulnerável a incendios que estejam em nível avançado.

Concluindo, se a Empresa X buscasse certificação para o *datacenter*, com base nas normas citadas, seria clasificado como TIER I, em todas as áreas de avaliação, com disponibilidade de 99,671 %, e *downtime* de 28,8 horas por ano.

### 4.1 Proposta de Melhoria

Esta seção tem como objetivo propor melhorias na infraestrutura do *datacenter*, colocando-o em melhores níveis de segurança, com base nas normas citadas.

A primeira melhoria é a implementação de uma política de segurança para o *datacenter*, descrevendo com detalhes responsabilidades, atividades e procedimentos a serem realizados, entre outros. Adicionalmente, são propostas melhorias em todas as áreas de avaliação. Nesse sentido, na área de telecomunicação, as melhorias propostas compreendem: a) identificação de todos o cabeamento, *racks*, réguas de energia, tomadas e quadro de

energia, facilitando qualquer manutenção/serviço; b) criação de um novo caminho de entrada apartado do atual, para a entra de serviços de *internet* e de voz, para que as operadoras, possam providenciar dupla abordagem dos serviços (entrada 1 e 2, conforme Figura 5).

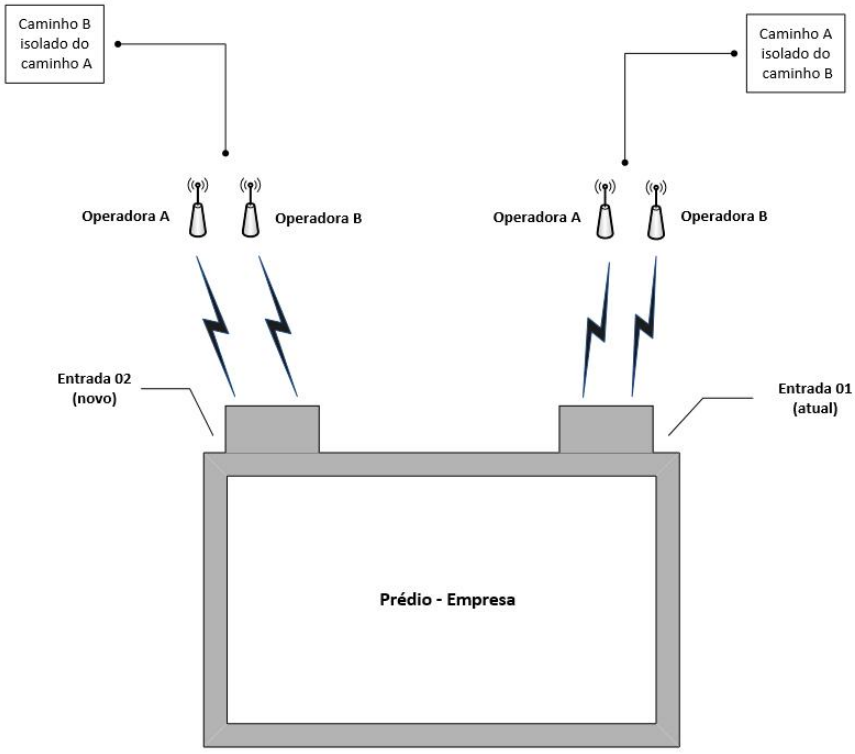


Figura 5 - Entrada de serviços de telecomunicação
Fonte: Autor

Para a área de arquitetura, as melhorias propostas consistem de: a) alteração da localização do *datacenter* (Figura 6). Com isso, mitiga-se o risco de inundações por vazamento nas tubulações de água dos banheiros; b) criação de uma sala dedicada para os equipamentos de UPS, disponibilizando maior espaço dentro do *datacenter*, além de instalação de sistema de climatização; c) controle de acesso nas duas entradas do *datacenter*, com monitoramento via *software;* d) remoção das janelas do *datacenter*, aumentando-se a segurança, e diminuindo-se a temperatura; e) substituição da porta de vidro, por estrutura metálica; f) instalação de piso elevado no *datacenter*, possibilitando a melhor organização e manutenção do cabeamento.

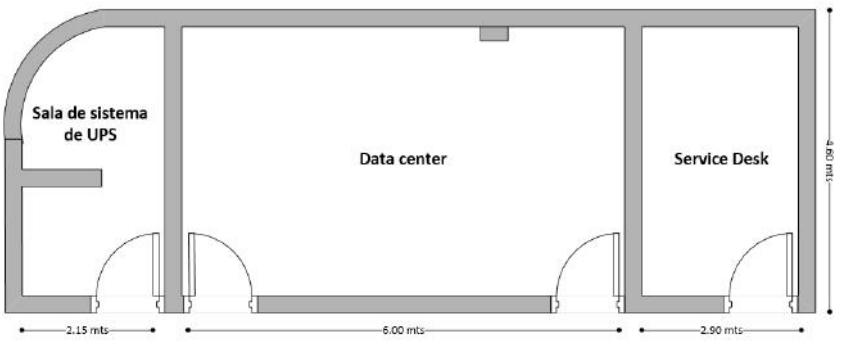


Figura 6 - Alteração no *Layout* do *Datacenter*.
Fonte: Autor

Para a área de Elétrica do *datacenter*, as melhorias sugeridas são: a) criação de uma nova sala de entrada de elétrica, totalmente apartada da atual (Figura 7); b) solicitar que a operadora disponibilize dois circuitos de energia elétricas (independentes), um para cada sala de elétrica (Figura 7); c) aquisição de um novo modulo de *nobreak*, criando-se redundância do sistema de UPS (Figura 8); d) ampliação de mais um quadro no *datacenter* (QDC) (Figura 9), em redundância, com disponibilização de dois circuitos para cada *rack*.

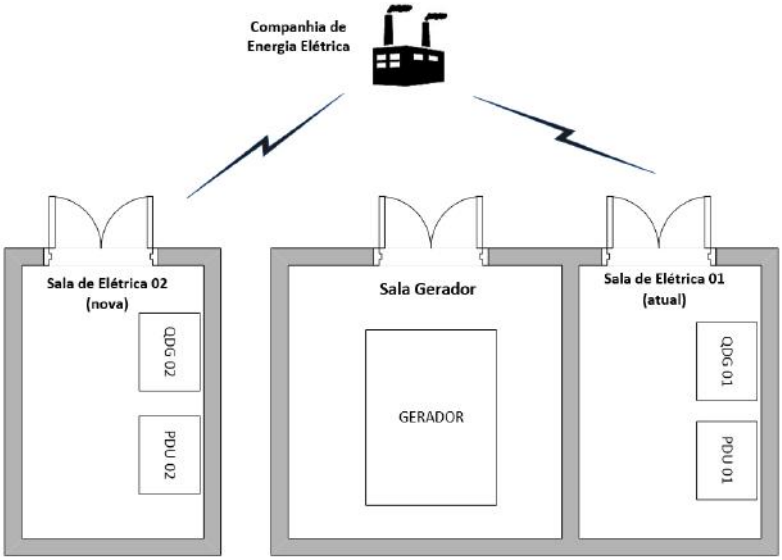


Figura 7 - Entrada de Energia Elétrica
Fonte: Autor

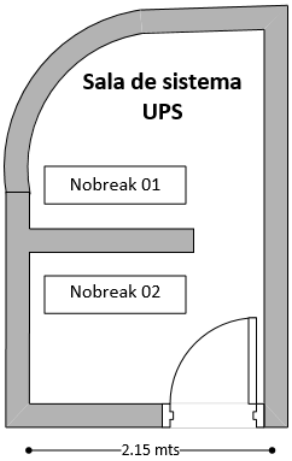


Figura 8 - Sala do Sistema do UPS
Fonte: Autor

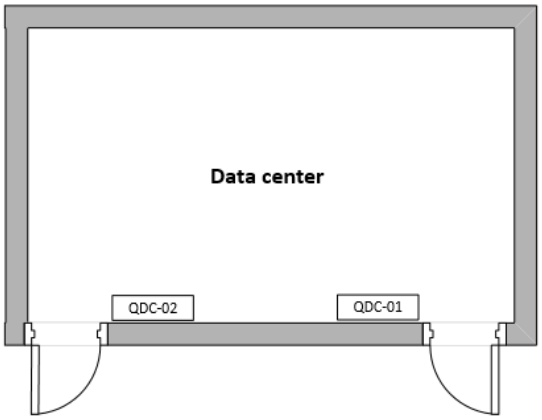


Figura 9 - Quadros de energia do Datacenter QDC-01 e QDC-02
Fonte: Autor

Com as melhorias propostas na área de Elétrica, a infraestrutura elétrica possuirá o cenário demonstrado pela Figura 10. 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 haja falha de energia externa, o gerador entra automáticamente em operação, mitigando o risco de interrupções. Os PDUs receberão a energia dos quadros gerais, distribuindo-a para o prédio e para os *nobreaks* da sala de sistema UPS que estabilizarão a energia, repassando-a para os quadros do *datacenter* (QDC). Cada QDC deve possuir um disjuntor para cada *rack*, fazendo que cada *rack* receba dois circuitos de energia elétrica, um de cada QDC. Finalizando-se a redundância da área de elétrica, todos os equipamentos devem possuir fontes redundantes.

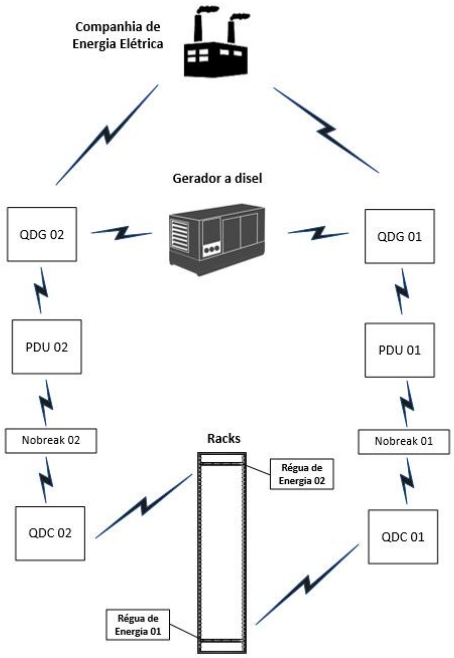


Figura 10: Cenário de Elétrica, após melhorias
Fonte: Autor

Para a área de Mecânica, as melhorias propostas foram divididas em climatização, e em controle e combate a incêndio. As melhorias propostas para a climatização são: a) instalação de ar condicionado redundante nas salas de elétrica e do gerador; b) instalação de ar condicionado redundante na sala de sistemas de UPS; c) instalação de ar condicionado redundante no *datacenter*; d) instalação de um termostato inteligente, que permite enviar alertas em caso de problemas de climatização. Para as melhorias relativas ao sistema de prevenção e controle de incendios, foram considerados: a) instalação de sistema detector de fumaça óptico nas salas de elétrica, gerador, sistema de UPS, e *datacenter*; b) instalação de sistema de supressão, que utiliza o composto sólido e estável (SBK), não pirotécnico, à base de sais de potássio; c) instalação de sistema de aspiração nas salas de elétrica, gerador, sistema de UPS, e *datacenter*; d) instalação e configuração de um sistema de desligamento de emergência, caso ocorra algum incêndio.

Assim, com essas melhorias realizadas, o nível geral de classificação do datacenter subiría para TIER II, pasando a uma disponibilidade de 99,741 %, e *downtime* de 22 horas/ano.

## 5 CONSIDERAÇÕES

Os equipamentos alocados dentro de um *datacenter* dependem diretamente da sua infraestrutura para operar com eficiência. Para que tal *datacenter* alcance maior nível de disponibilidade e segurança, o mesmo deve ser planejado e estruturado seguindo normas e requisitos de segurança da informação. Nesse sentido, ese estudo realizou uma pesquisa sobre a infraestrutura de um *datacenter*, seus requisitos e níveis de classificação. Para isso, foi feita revisão da literatura, e na sequencia um estudo de caso, no datacenter da Empresa X.

Foi apresentado o cenário atual do datacenter da empresa em estudo, com o intuito de se identificar itens não aderentes à norma, com importância fundamental para maior desempenho, evitando-se perda de dados e interrupções.

A classificação atual do *datacenter* da empresa X baseou-se nos critérios identificados na literatura.As melhorias propostas compreendem alterações na infraestrutura física das quatro áreas de avaliação. Os benefícios advindos das melhorias propostas compreendem o aumento da segurança da informação, e a redução de pontos de falhas, tanto por eventos não planejados, ou manutenções, contribuindo assim para a continuidade do negócio.

As implementações das melhorias são dependentes da disponibilidade de recursos, bem como do orçamento da Empresa X, com opção de implementações por fases.

Considera-se ainda que o presente trabalho possibilitou o estudo e o entendimento de práticas e normas de segurnaça física em *datacenters*,.não sendo um trabalho completo sobre o tema, mas sim um ponto de partida para trabalhos futuros, em especial considerando *datacenters* de empresas de pequeno porte, geralmente com restrições orçamentárias.

## 6 REFERÊNCIAS

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, B. H. F. **Dicionário da língua.** Brasília. Nova Fronteira, 2001.
BRITO, M. J. **Tecnologia da informação e mercado futuro: o caso da BM&F**. Tecnologia da informação e estratégia empresarial. São Paulo: FEA/USP, 1996.
CAMPOS, A. **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, C. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books, 2000.
FERREIRA, F. N. F. **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2003.
FRASER, B. ***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.
MARCONI, M. A., LAKATOS, E. M. **Técnicas de Pesquisa**. São Paulo:Editora Atlas. 5ª edição, 2010.
MARIN, P. S. ***Datacenters*: desvendando cada passo: conceitos, projetos, infraestrutura física e eficiência energética**. 1. Ed. São Paulo: Érica, 2011.
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, M. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Elsevier, 2003.

SIEWERT, C.V. **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, E.; VOLONINO, L. **Tecnologia da informação para gestão**. São Paulo: Bookman, 2013.
VERAS, M. ***Datacenter*: componente central da infraestrutura de TI**. Rio de Janeiro. Brasport, 2009.
ZUCCHI, W. L. **Construindo um *datacenter***. Revista USP. São Paulo: USP, 2013.