DO CPD AO *DATA CENTER* - A EVOLUÇÃO TECNOLÓGICA DA COMPANHIA DE SANEAMENTO BÁSICO DO ESTADO DE SÃO PAULO (SABESP)[1]

Ana Cristina Dominici

Resumo:

Quando lançou suas ações na Bolsa de Nova Iorque, a Sabesp precisou adaptar-se à Lei Sarbanes-Oxley e aumentar a segurança dos seus dados e equipamentos. Isto motivou a reforma do antigo CPD para transformá-lo em um *data center*, além da criação de um site secundário *disaster recovery*. Toda a parte elétrica, a climatização, o cabeamento estruturado e de telecomunicações, e os sistemas de acesso e controle de incêndio passou a seguir as normas ABNT, garantindo uma classificação *Tier* III (não certificada) à instalação. Este foi o principal benefício obtido com a mudança, já que a disponibilidade do CPD sempre foi alta, a virtualização de servidores já era feita e a diminuição de pessoal se deu devido à evolução tecnológica natural, com a leitura de canhotos de contas d´água feita pelos bancos, impressão de contas feita no momento da leitura, digitalização de arquivos, e terceirização da impressão dos demais relatórios.

Palavras-chave: CPD. *Data center*. *Tier*. ABNT NBR 14565. ANSI/TIA-942-A. ANSI/BICSI 002. *The Uptime Institute*.

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização "Datacenter: Projeto, Operação e Serviços" da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Datacenters, sob orientação do Professor Djan de Almeida do Rosário.

1 INTRODUÇÃO

Os antigos CPDs (Centro de Processamento de Dados) eram grandes salas climatizadas, com *mainframes* e vários outros servidores físicos, equipamentos de rede, impressoras, unidades leitoras de fita e de disco. O número de pessoas circulando por entre os equipamentos era grande, o que aumentava o risco de indisponibilidade dos serviços.

Os CPDs evoluíram para *data centers* acompanhados da adoção de normas como a ABNT NBR 14565, a ANSI/TIA-942-A, ou as definidas pelo *The Uptime Institute*. Estas normas garantem a confiabilidade e a disponibilidade de um *data center*, já que, com elas, ele passa a contar com sistemas redundantes que suprem falhas nos sistemas principais em caso de problemas causados por motivos conhecidos ou não (Marin, 2016, p. 35).

A Sabesp (Companhia de Saneamento Básico do Estado de São Paulo), cujo *data center* é objeto deste estudo, é uma sociedade anônima de economia mista fundada em 1973, que atualmente é responsável pelo fornecimento de água, coleta e tratamento de esgotos de 368 municípios do Estado de São Paulo.

É a maior empresa de saneamento das Américas e a quarta maior do mundo em população atendida. São 27,9 milhões de pessoas abastecidas com água e 21,6 milhões de pessoas com coleta de esgotos. Para abastecer toda esta população existem 240 estações de tratamento de água, que juntas permitem a produção de 119 mil litros de água por segundo. São 73,4 mil quilômetros de redes de água e 8,9 milhões de ligações.

O objetivo deste estudo de caso é identificar quais os benefícios obtidos pela Sabesp com a evolução do CPD para um *data center* e gerar um registro histórico das mudanças de infraestrutura de TI na empresa. Foi conduzido com base em documentos, bibliografias e uma entrevista com um dos responsáveis pelo *data center* da Sabesp. A pesquisa foi básica e empírica, já que foi uma investigação sobre a evolução de um objeto nos últimos anos e as informações foram obtidas com base em literatura existente sobre a área de Informática. Foi uma pesquisa qualitativa, porque é uma situação única e

não pode predizer casos análogos futuros, podendo apenas ajudar na compreensão de outros casos ou em um problema mais geral.

2 O CPD DA SABESP

Até os anos 90 o CPD da Sabesp tinha grandes *mainframes* instalados em gabinetes com CPUs, unidades de fita, de disco e console. Os primeiros servidores ficavam em prateleiras metálicas e eram compostos de torre, monitor, teclado e *mouse*. O cabeamento não era estruturado e os cabos formavam uma cascata atrás das prateleiras, dificultando a movimentação de pessoas para manutenção. Os quadros de força não eram organizados, e o condicionamento de ar era suprido por 12 *fancoils*. O *no-break* era alimentado por aproximadamente 500 baterias Satúrnia. Apesar da existência de uma fechadura eletrônica com senha, o acesso ao CPD era livre. O sistema de combate a incêndios era baseado em *sprinklers* e extintores e não havia redundância na infraestrutura.

Além dos *mainframes* e servidores, no CPD também ficavam 6 grandes impressoras matriciais e 2 enormes impressoras a laser, onde eram impressos todos os documentos da empresa e todas as contas de água dos municípios atendidos pela Sabesp. Uma leitora ótica era utilizada para ler códigos de barras de todas as contas de água pagas nos bancos. A operação dos equipamentos era feita em esquema de rodízio por 24 operadores, em 4 turnos.

3 *DATA CENTERS*

Os primeiros computadores ocupavam salas inteiras e eram construídos com válvulas. Seus tamanhos começaram a diminuir quando foram criados os circuitos integrados transistorizados. Na medida em que diminuíam de tamanho, sua capacidade de processamento e armazenamento aumentava exponencialmente. As empresas

começaram a utilizar vários servidores, e enquanto um ficava com sua capacidade ociosa, outro ficava sobrecarregado.

Começou-se a perceber que os recursos computacionais estavam sendo utilizados de forma ineficiente e, para evitar a subutilização da capacidade de processamento de CPUs, do consumo de memória e de disco, servidores virtuais começaram a ser criados nos servidores físicos com uma configuração o mais enxuta possível. Os servidores físicos que abrigam os servidores virtuais passaram a ter seus recursos melhor aproveitados e passaram a ser alocados em *racks* dentro dos *data centers*. Segundo Lowe, Green e Davis (2016, p. 502), a virtualização existe desde os anos 1960, quando foi criada para permitir a execução simultânea de tarefas em um mainframe.

Os requisitos - e custos - de um projeto de *data center* dependem dos níveis de disponibilidade e redundância que são esperados dos seus sistemas críticos, que são: Distribuição elétrica, Climatização, Cabeamento de rede e de telecomunicações, Sistemas de combate a incêndios e Sistemas de segurança do site. A Figura 1 mostra como os sistemas estão relacionados.

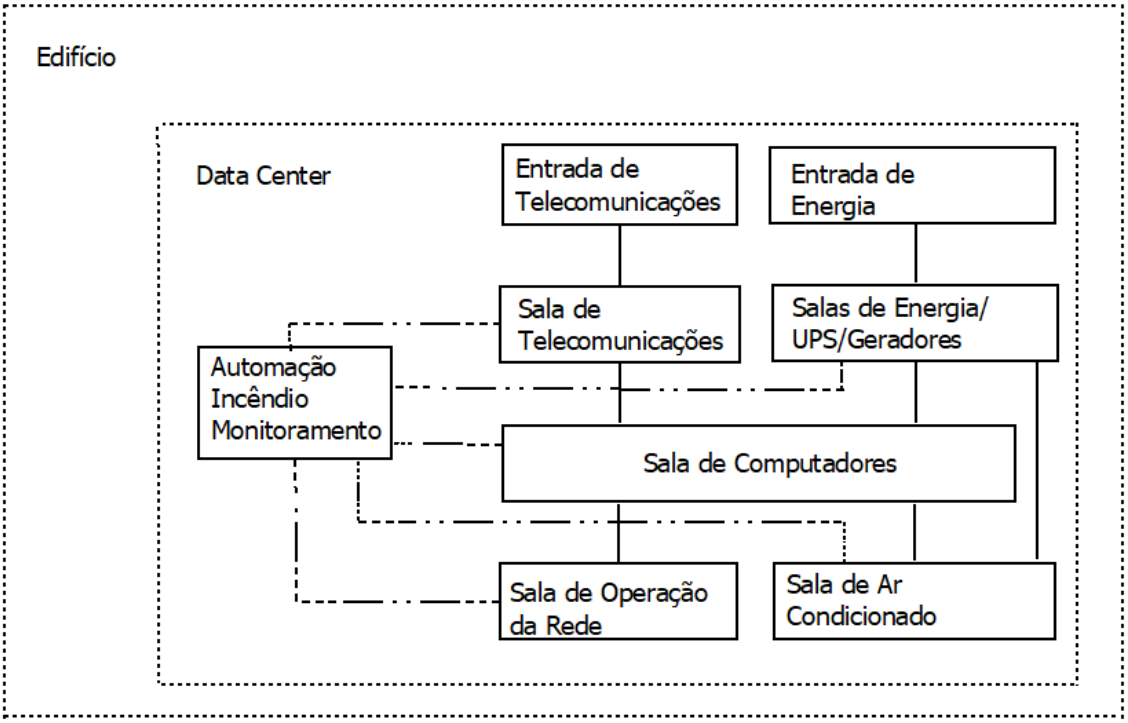

Figura 1. Diagrama geral das relações entre os diversos ambientes e seus componentes. Fonte: Norma ABNT NBR 14565:2013, Anexo F, p. 117, adaptado pela autora.

O sistema de distribuição elétrica é o sistema mais crítico de um *data center*. Para garantir uma disponibilidade o mais próxima possível de 100% são agregados aos componentes da distribuição convencional grupos geradores a diesel, sistemas UPS (*no-break*), baterias, chaves de transferência, estabilizadores, transformadores e PDUs (*power distribuition units*).

Depois do sistema de distribuição elétrica, o sistema mais importante é o de climatização, que deve funcionar de forma ininterrupta. A instalação deve ser de uso exclusivo do *data center* e deve ter redundância.

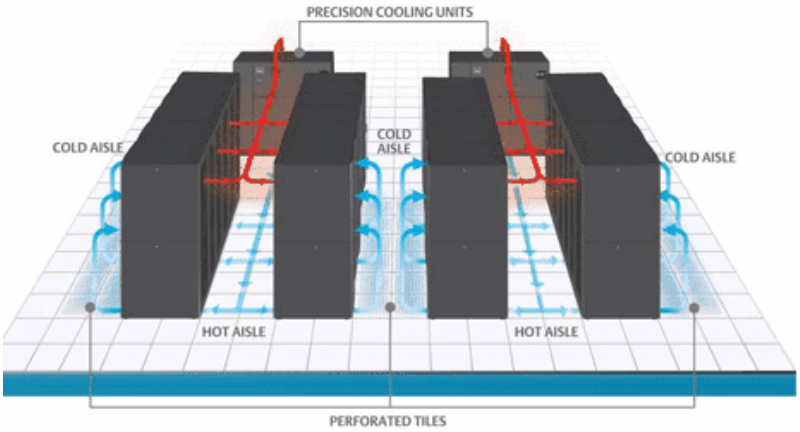

Figura 2. Configuração de corredores frios e quentes. Fonte: CopperLed, 2017.

Unidades CRAC (*Computer Room Air Conditioner*) podem ser utilizadas na configuração de corredores quentes e frios dentro do *data center*, insuflando ar frio sob o piso elevado com placas perfuradas (ou pelo teto, quando não se utiliza piso elevado) para formar os corredores frios (Figura 2). O corredor quente é gerado na parte posterior dos *racks*, onde há a saída do ar que passou pela eletrônica para retirar o calor gerado devido à sua operação, e por onde é feito seu encaminhamento para a unidade CRAC instalada neste corredor.

A proteção contra incêndios em um *data center* começa no mesmo momento em que se inicia sua construção. Suas paredes devem retardar a queima em uma ocorrência de incêndio, os espaços acima e abaixo da sala de computadores devem suportar o fogo sem propagá-lo e as portas corta fogo devem sempre ser mantidas fechadas.

O combate aos incêndios se dá por meio de detectores de calor e *sprinklers*, preferencialmente do tipo *pre-action*, que mantém seco o encanamento que leva água até o *sprinkler*, além de gases inertes como FM-200. A instalação de extintores de incêndio de uso manual é obrigatória e, para incêndios que atingem a parte elétrica, o recomendável é utilizar extintores que contém agentes químicos secos, apesar de serem prejudiciais aos equipamentos eletrônicos.

Circuitos fechados de TV (CFTV) e câmeras auxiliam na vigilância eletrônica do site e devem cobrir as áreas de circulação e acesso comum, espaços de serviços e manutenção, salas técnicas, elevadores, escadas, corredores, *halls* e a sala de computadores.

Junto à equipe de segurança, também são utilizados sistemas eletrônicos para garantir o controle de acesso ao *data center*. Este controle deve ser aplicado de forma diferenciada ao pessoal que trabalha no *data center*, visitantes e prestadores esporádicos de serviços. O acesso de visitantes deve ser evitado, já que os *data centers* não podem ser encarados como "cartão de visitas" da empresa. A preocupação com a segurança deve ser uma rotina, e não apenas uma preocupação isolada em um dado momento.

O sistema de controle de acesso mais comum utilizado é o cartão de proximidade, que pode ser associado à digitação de uma senha. Os meios mais seguros são os que fazem uso da biometria associada, como impressão digital, leitura da geometria da mão, leitura da íris, da retina, padrão vascular, reconhecimento de voz ou facial. A utilização da biometria deve respeitar os direitos de imagem, garantidos pela Constituição.

Todos estes sistemas são gerenciados através de ferramentas conhecidas como *Data Center Infrastructure Management* (DCIM). Seu principal objetivo é obter informações em tempo real sobre os recursos utilizados e, através de sensores, dados sobre a umidade, temperatura, etc., de modo que os gestores do *data center* possam agir para garantir a segurança da infraestrutura e da operação. Através do DCIM os gestores conseguem uma visualização completa dos equipamentos e da infraestrutura, incluindo cabeamento, climatização, parte elétrica e movimentação de equipamentos. A ferramenta também auxilia no controle do consumo de energia e no aumento da eficiência operacional.

Não é o *data center* o bem mais valioso de uma empresa, mas sim a informação. A área de TI é encarregada de mantê-la íntegra, confidencial e disponível, por isso é importante que existam rotinas de *backup* de dados em tempo real e armazenamento em outra localidade, de modo que os dados não sejam comprometidos em caso de incêndio.

O local de instalação do *data center* deve ser escolhido de forma cuidadosa, evitando locais de risco como terrenos abaixo no nível de rios e sujeitos a inundação. Deve-se também evitar locais sujeitos a vibrações ou impactos de alta intensidade, como por exemplo, rodovias, vias públicas de trânsito pesado ou intenso, ferrovias e metrô. Fontes de radiofrequência e de eletromagnetismo também podem afetar negativamente o *data center*.

4 DISPONIBILIDADE, CONFIABILIDADE E REDUNDÂNCIA

A classificação de um *data center* é baseada, principalmente, nas suas características de disponibilidade, confiabilidade e redundância. Para garantir que o *data center* opere com níveis de disponibilidade próximos de 100%, ele precisa ter sistemas redundantes capazes de suprir a falta de seus sistemas principais em casos de falhas ou paradas (programadas ou não).

A disponibilidade de um determinado sistema é o tempo durante o qual ele **está** em operação em relação ao tempo em que ele **deve estar** em operação. Pode ser calculada da seguinte forma:

$$Disponibilidade = \frac{MTBF}{MTBF + MTTR} = \frac{tempo\ do\ sistema\ em\ operação}{tempo\ total\ em\ que\ o\ sistema\ existe\ entre\ falhas}$$

Sendo:

- MTBF (*Mean Time Between Failures*), tempo médio entre falhas;
- MTTR (*Mean Time To Repair*), tempo médio de reparo.

Fonte: Marin, 2016

A disponibilidade de cada sistema componente do *data center* deve ser calculada individualmente, considerando que sua topologia pode ser em série e/ou paralela. A disponibilidade da infraestrutura sempre se refere ao sistema como um todo.

$$Disponibilidade_{paralelo} = (S1 + S2) - (S1\ x\ S2)$$

$$Disponibilidade_{série} = (S1)\ x\ (S2) = \left(\frac{MTBF_1}{MTBF_1 + MTTR_1}\right)\ x\ \left(\frac{MTBF_2}{MTBF_2 + MTTR_2}\right)$$

Sendo:

- S1, um componente ou sistema qualquer, como um servidor, um *switch*, etc.;
- S2, um segundo componente ou sistema qualquer, interconectado ao primeiro.

Fonte: Marin, 2016.

A confiabilidade pode ser entendida como a distribuição do tempo entre falhas de um sistema ou componente, e é definida como a probabilidade de um sistema não apresentar falhas antes de uma quantidade de horas bem determinada.

$$Confiabilidade = e^{-\frac{t}{MTBF}}$$

Sendo:

- t, tempo;
- e, número de Euler;
- MTBF (*Mean Time Between Failures*), tempo médio entre falhas.

Fonte: Marin, 2016

5 EFICIÊNCIA ENERGÉTICA

O consumo energético de um *data center* é elevado. Para resfriar a grande quantidade de equipamentos elétricos em seu interior, o sistema de climatização gasta praticamente a mesma quantidade de energia que os equipamentos consomem.

De acordo com uma pesquisa do Gartner (2007, apud HAYNES, 2016, Posição do Kindle 4928), a área de TI é responsável pela emissão global de 2% do gás carbônico na atmosfera, o mesmo valor emitido pela Indústria Aeronáutica. A emissão de CO_2 na atmosfera depende da matriz energética adotada por cada país e, como no Brasil a matriz energética é limpa e baseada em hidrelétricas, o impacto ambiental é menor que em outros países.

A eficiência do uso de energia elétrica de um *data center* é dada pelo PUE (*Power Usage Effectiveness*), e é calculada através da seguinte fórmula:

$$PUE = \frac{C_{infraestrutura}}{C_{ti}}$$

Sendo:

$C_{infraestrutura}$ a carga total da infraestrutura (ou carga total do site), em kW;
C_{ti} a carga total dos equipamentos de TI instalados no site, em kW.
Fonte: Marin, 2016.

Data centers mais recentes e bem projetados chegam a ter um PUE de 1,4. As instalações do Facebook e do Google alcançam um valor menor, mas o modo de construção dos seus *data centers* não é o mesmo utilizado por empresas comuns (CARAPOLA, 2016, Livro 1, p. 23).

Outra métrica é o DCiE (*Data Center infrastructure Effectiveness*), que é o inverso do PUE:

$$DCiE = \frac{1}{PUE} = \frac{C_{ti}}{C_{infraestrutura}} \; x \; 100\%$$

Sendo:

PUE, *Power Usage Effectiveness*
$C_{infraestrutura}$ a carga total da infraestrutura (ou carga total do site), em kW;
C_{ti} a carga total dos equipamentos de TI instalados no site, em kW.
Fonte: Marin, 2016.

Medidas simples como a distribuição adequada de servidores nos *racks*, a utilização de painéis cegos nos espaços do *rack* onde não há servidores, a remoção de cabos que não são mais utilizados, e um bom desenho de *layout* podem aumentar a eficiência energética do *data center*.

6 CLASSIFICAÇÃO E CERTIFICAÇÃO DOS *DATA CENTERS* SEGUNDO O *THE UPTIME INSTITUTE*

O *The Uptime Institute* é formado por um grupo de empresas que se dedicam a quantificar e qualificar a eficiência e a disponibilidade de *data centers*, criando um padrão para o projeto, construção e operação dos mesmos.

O padrão definido pelo *The Uptime Institute* estabelece quatro classificações *tier* de infraestrutura de *data centers*, com base na sua disponibilidade, e também especifica os procedimentos para verificar periodicamente se o *data center* ainda está em conformidade com estas classificações. As classificações *tier* descrevem a topologia de infraestrutura do *data center* necessária para suportar suas operações.

O *Uptime* tem um programa de certificação de *data centers* com base em seus padrões e dividido em duas fases: projeto (*design*) e instalação (*facility*). A certificação de projeto é concedida a *data centers* cujo projeto foi submetido ao *Uptime* para avaliação e que atenderam às suas especificações. No caso da instalação, a certificação é concedida mediante auditoria do *Uptime* na infraestrutura instalada e isso somente depois do projeto ter sido previamente aprovado e certificado pela instituição.

A classificação da infraestrutura do *data center* será determinada pelo sistema de menor classificação *tier*. Por exemplo, caso o sistema elétrico seja *Tier* III e o sistema mecânico *Tier* II, a classificação do *data center* será *Tier* II.

Para validar a conformidade com as classificações, são consideradas apenas as redundâncias dos sistemas de distribuição elétrica e climatização do site. **Nenhum** outro sistema contribui para a classificação *tier* de um site, nem os sites secundários de *disaster recovery*, que são avaliados de forma independente do site primário.

Segundo o *The Uptime Institute*, os *data centers* podem ser classificados em:

- *Tier* I: *Data center* básico (N, de "*need*")

É aquele que não apresenta componentes ou sistemas redundantes em sua infraestrutura de distribuição elétrica e mecânica, ou seja, tem apenas a capacidade requerida para suportar a carga do site.

- *Tier* II: *Data center* com componentes redundantes (N + 1, "*need plus* 1")

Um *data center Tier* II tem componentes redundantes, porém uma única estrutura de distribuição, tanto de energia elétrica quanto de ar-condicionado. É a classificação *tier* mais comum, já que os *Tiers* III e IV são muito mais caros.

- *Tier* III: *Data center* com manutenção e operação simultâneas (2N, "*need times* 2")

Um *data center Tier* III tem todos os componentes redundantes e caminhos alternativos de distribuição não energizados.

- *Tier* IV: Infraestrutura tolerante a falhas (2(N + 1), "*redundant need plus* 1")

Um *data center* tolerante a falhas tem vários sistemas independentes e fisicamente isolados com componentes redundantes que podem ser acionados imediatamente em caso de necessidade. Além disso, conta com vários caminhos de distribuição independentes, sempre energizados, que atendem simultaneamente os equipamentos críticos de TI da sala de computadores.

A aderência às normas ABNT NBR 14565, ANSI/TIA-942-A ou a ANSI/BICSI 002 **não** gera certificação.

7 O *DATA CENTER* DA SABESP ATUALMENTE

Em 2002, para facilitar a obtenção de empréstimos junto a órgãos internacionais e aumentar seus investimentos em Saneamento Básico, a Sabesp lançou suas ações na Bolsa de Nova Iorque (NYSE) e precisou adaptar-se à Lei Sarbanes-Oxley (SOX). Foi necessário aumentar a segurança dos dados e dos equipamentos e, por isso, pouco tempo depois, o CPD localizado no segundo andar de um edifício de três andares foi reformado para tornar-se um *data center* e incluir uma sala cofre. Além disso, foi criado também o primeiro site de *disaster recovery* da empresa.

Após uma nova reforma feita em 2014, foi inaugurada no mesmo prédio a estrutura atual do *data center* da Sabesp, com 128 m². A sala cofre foi construída com placas modulares e com proteção contra incêndio, intrusão, água e fumaça. Foram instalados no *data center* cerca de 70 servidores físicos, distribuídos em *racks* de 42Us e com piso elevado reforçado. O cabeamento estruturado passou a ter uma melhor distribuição com switches *Top of Rack* e foi feita a substituição dos cabos UTP por cabos de fibras óticas (FO). O combate a incêndios faz uso do gás FM-200 e o acesso ao seu interior se faz por meio de biometria.

O equipamento de climatização é exclusivo da sala cofre. Os quadros de força têm dois circuitos, disjuntores de maior capacidade e medidores de tensão. Quase todos os equipamentos possuem duas fontes e os que possuem apenas uma têm chaves STS (chaves estáticas de transferência). Atualmente são quatro *no-breaks*, os quais, junto com o gerador e o tanque de combustível redundantes, suprem a energia do *data center* em caso de interrupção do fornecimento pela concessionária.

A impressão das contas d´água no momento da leitura do consumo, na residência dos clientes, e a substituição dos relatórios que antes eram impressos por arquivos digitais tornou desnecessária a utilização das grandes impressoras na Sabesp, e o pouco que ainda precisa ser impresso passou a ser encaminhado para uma empresa terceirizada. A leitura dos códigos de barras das contas pagas agora é feita pelos bancos

no momento do pagamento, que enviam uma vez por dia os arquivos com os dados para a Sabesp para posterior processamento.

O acesso ao *data center* agora é feito apenas pelo pessoal estritamente necessário, mas ainda ocorrem eventualmente visitas de pessoal alheio à Superintendência de Informática.

A implantação do *data center* não causou diminuição de pessoal, já que isso se deu naturalmente graças à evolução tecnológica natural, como a impressão das contas de água no momento da leitura, da leitura dos canhotos das contas pelos bancos e pela terceirização da impressão. Hoje são 8 operadores, em 4 turnos. A virtualização de servidores também já era adotada e a disponibilidade do CPD sempre foi alta.

Com 97m², o novo site de *disaster recovery* foi construído dentro das dependências da Sabesp, a cerca de 8km de distância do site principal, mas o local escolhido tem alguns pontos negativos, como ser sujeito a enchentes e estar próximo à portaria da empresa. A infraestrutura instalada é praticamente igual à do site principal.

Construídos pela Aceco TI, os dois *data centers* com infraestrutura equivalente a um *Tier* III garantem uma disponibilidade individual de 99,98% à empresa com seus sistemas críticos redundantes. Apesar de o site secundário estar instalado em um local não adequado, foram tomadas todas as providências necessárias na execução da obra para que a segurança do *data center* DR fosse garantida, como a construção da cabine secundária acima de 1,45 m do nível da rua, a construção da sala cofre no 1º andar do prédio onde está instalado e a utilização do acesso biométrico nos acessos ao NOC, Sala UPS, Sala TELECOM e Sala Cofre.

Para gerenciar os dois *data centers* foi adquirida a ferramenta de DCIM VDC (*Visual Data Center*), que permite a visualização dos data centers em 3D, identificar se existe a necessidade de expansão da infraestrutura, monitorar as conexões, monitorar o consumo de energia elétrica, monitorar a temperatura e a umidade do data center, gerenciar câmeras IP, listar o inventário completo dos ativos do data center, monitorar os alarmes de todos os equipamentos mecânicos, elétricos e de energia e identificar novos equipamentos instalados.

Os *data centers* da Sabesp não possuem certificação do *The Uptime Institute*, mas foram construídos respeitando as normas ABNT NBR 14565.

8 CONCLUSÃO

Carapola (2016, Livro 1, p. 2) explica que o principal objetivo de um *data center* é fornecer disponibilidade ininterrupta de serviços críticos para a tecnologia de TI nele alocada. Já Lowe, Green e Davis (2016, Posições do Kindle 1563-1564) dizem que a única razão para a existência de um *data center* é a geração de dinheiro para a empresa.

Para atender à Lei Sarbanes-Oxley, a Sabesp investiu na modernização do seu CPD, transformando-o em um *data center* moderno, com uma sala cofre no seu interior e também criando um site de *disaster recovery*.

Os benefícios obtidos pela Sabesp com implantação do *data center* são a normalização das instalação elétricas e do cabeamento, o aumento da segurança no acesso às instalações, e um maior cuidado em cada intervenção, que agora é planejada, documentada e aprovada por um grupo de gestores. Estas mudanças garantem que os clientes e fornecedores da empresa sejam melhor atendidos e que não sejam gerados prejuízos para a Sabesp.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 14565: Cabeamento estruturado para edifícios comerciais e *data centers*. Rio de Janeiro, 2013.

BROSSO, Inês. Biometria Aplicada em Sistemas de Segurança Corporativa. In: SILVA, Leandro Augusto da; MARTINS, Valéria Farinazzo Martins; OLIVEIRA NETO, João Soares de. (Org.). Tendências Tecnológicas em Computação e Informática. São Paulo: Editora Mackenzie, 2013. p. 97-124.

CARAPOLA, Art. *The Data Center Builder's Bible - Book 1: Defining Your Data Center Requirements: Specifying, Designing, Building and Migrating to New Data Centers.* 3. ed. *NewVista Advisors, llc and Art Carapola*, Edição do Kindle, 2018. v 1.

CARUSO, Carlos A.A.; STEFFEN, Flávio Deny. Segurança em Informática e de Informações. 4. ed. São Paulo: Editora Senac, 2013.

FACCIONI FILHO, Mauro - Normas e classificação de datacenters. Palhoça: UnisulVirtual, 2017.

HAYNES, George - *Data Center Infrastructure & Organization. Americana Press*, Edição do Kindle, 2016.

LAHTI, Christian B.; PETERSON, Roderick - *Sarbanes-Oxley - IT Compliance Using Open Source Tools.* 2.nd.ed. *Syngress*, 2007. 445p.

LOWE, Scott D. Lowe; GREEN, James; DAVIS, David M. - *Building a Modern Data Center: Principles and Strategies of Design*. Estados Unidos da América: *ActualTech Media*, Edição do Kindle, 2016.

MACHADO, Cristiane Salvan et al. - Trabalhos acadêmicos na Unisul : apresentação gráfica. 2.nd.ed.rev. e atual. Palhoça: Editora Unisul, 2013.

MARIN, Paulo Sérgio – *Data Centers* – Engenharia: Infraestrutura Física. São Paulo: PM Books, 2016.

WILL, Daniela Erani Monteiro - Metodologia da Pesquisa Científica. Palhoça: UnisulVirtual, 2016.

VISHWAKARMA, Jai - *Building a Data Center - Field Guide: From requirements to implementation*. Edição do Kindle, 2012.

SITES

ACECO TI. Certificações. Disponível em <http://www.acecoti.com/pt-br/acecoti/certificacoes>. Acesso em 02 de setembro de 2018.

AQUIM, Tatiane. *Uptime Institute*: A Aplicação do Padrão *Tier* no Brasil. 10 de outubro de 2017. Disponível em <http://www.datacenterdynamics.com.br/focus/archive/2017/10/uptime-institute-aplica%C3%A7%C3%A3o-do-padr%C3%A3o-tier-no-brasil>. Acesso em 13 de março de 2019.

COPPERLED. *5 easy ways to cool your data center*. Disponível em < http://www.copperled.com/news_detail/newsId=40.html>. Acesso em 12 de outubro de 2018.

DATA CENTER DYNAMICS. Aceco TI inaugura sala-cofre da Sabesp. Disponível em <http://www.datacenterdynamics.com.br/focus/archive/2015/01/aceco-ti-inaugura-sala-cofre-da-sabesp>. Acesso em 02 de setembro de 2018.

_____. *Data Center* Médio da Sabesp ganha o *Data Center Dynamics Awards Brazil* 2014. Disponível em <http://www.datacenterdynamics.com.br/focus/archive/2014/12/data-center-m%C3%A9dio-da-sabesp-ganha-o-datacenterdynamics-awards-brazil-2014>. Acesso em 02 de setembro de 2018.

DCI. Após dez anos na Bolsa de NY, Sabesp triplica valor de mercado e ações valorizam 601%. Disponível em <https://www.dci.com.br/financas/apos-dez-anos-na-bolsa-de-ny-sabesp-triplica-valor-de-mercado-e-ac-es-valorizam-601-1.312835>. Acesso em 20 de outubro de 2018.

GARTNER. *Gartner Estimates ICT Industry Accounts for 2 Percent of Global CO_2 Emissions*. Disponível em <https://www.gartner.com/newsroom/id/503867>. Acesso em 25 de setembro de 2018.

GREEN 4T - Sala-cofre certificada: as normas que regulamentam sua instalação e manutenção, e os testes aos quais é submetida. 24 de maio de 2017. Disponível em <http://green4t.com/blog/2017/05/24/sala-cofre-certificada-normas-que-regulamentam-sua-instalacao-e-manutencao-e-os-testes-aos-quais-e-submetida/>. Acesso em 08 de julho de 2018.

LAIA, Wilson - Dos Grandes CPDs aos Datacenters – Partes I e II. 26 de março de 2013. Disponível em <https://www.tiespecialistas.com.br/dos-grandes-cpds-aos-datacenters-parte-i-2/>. Acesso em 08 de julho de 2018.

LEGRAND. Aplicações Normativas. Disponível em <http://www.legrand.com.br/sites/cemarlegrand.com.br/files/produtos/recursos/lcs2/lcs2_esp_aplicacoes_normativas.pdf>. Acesso em 20 de setembro de 2018.

MARIN, Paulo Sérgio - Atualização de normas e desenvolvimentos em cabeamento estruturado. 2013. Disponível em <https://docplayer.com.br/14999177-Atualizacao-de-normas-e-desenvolvimentos-em-cabeamento-estruturado-prof-dr-paulo-sergio-marin-engo-engenheiro-eletricista.html>. Acesso em 08 de julho de 2018.

OPTIMUM PATH INC - Visual Data Center. Disponível em <http://www.optimumpathinc.com/Products-VDC.html>. Acesso em 15 de março de 2019.

PORTAL FATOR BRASIL. Aceco TI constrói sala cofre para Sabesp. Disponível em < http://clippingprodeb.blogspot.com/2014/03/portal-fator-brasil-aceco-ti-constroi.html>. Acesso em 02 de setembro de 2018.

REVISTA *DATACENTER. ¿Por que es recomendable implementar pasillos frios y pasillos calientes?* Disponível em https://revistadatacenter.wordpress.com/2014/01/18/por-que-es-recomendable-implementar-pasillos-frios-y-pasillos-calientes/>. Acesso em 12 de outubro de 2018.

ROUSE, Margaret - *Uptime Institute, Inc.*. Janeiro de 2007. Disponível em <https://searchdatacenter.techtarget.com/definition/Uptime-Institute-Inc>. Acesso em 13 de março de 2019.

SABESP. Perfil. Disponível em <http://site.sabesp.com.br/site/interna/Default.aspx?secaoId=505>. Acesso em 20 de setembro de 2018.

_____. Relatórios de Sustentabilidade. Disponível em <http://site.sabesp.com.br/site/uploads/file/relatorios_sustentabilidade/sabesp_2017_RS_portugues.pdf>. Acesso em 20 de setembro de 2018.

SIEMON. *Data Center Topologies*. Disponível em <https://blog.siemon.com/standards/tia-942-a-distributed-data-center-topology>. Acesso em 20 de setembro de 2018.

THE UPTIME INSTITUTE - Uptime Institute. [ca 2019]. Disponível em <https://pt.uptimeinstitute.com/>. Acesso em 13 de março de 2019.