Data Center

Aula 05 - Sistema de Segurança e Automação

Apresentação

Olá, pessoal! Na aula passada, estudamos o sistema de climatização da sala de computadores, o qual é um dos pilares da infraestrutura crítica de um Data Center (DC). Nesta aula, estudaremos outros importantes sistemas: os que lidam com a segurança do site, com o controle de acesso e com a automação predial.

Como já vimos na aula 1, Data Centers são ambientes de missão crítica que não podem parar um só segundo e abrigam dezenas de equipamentos de altíssimo custo. Qualquer sinistro que aconteça, seja por questão natural, acidental ou mesmo intencional, causará prejuízos incalculáveis, principalmente para a reputação da organização.

Assim, sistemas de segurança, de automação e de prevenção contra incêndios tornam-se fundamentais. Nesta aula, estudaremos alguns desses sistemas utilizados em um DC.

Objetivos

Ao final desta aula, você deverá ser capaz de:

- Compreender os aspectos da segurança física de um Data Center e como eles são tratados pelas soluções de controle de acesso, monitoramento e gerenciamento do DC;
- Entender o que é um DCIM (*Data Center Infrastructure Management*);
- Saber que qualquer adição ou remoção de equipamentos de TI no DC precisa ser planejada para melhorar a eficiência deste;
- Conhecer os sistemas de vigilância e combate a incêndio de um Data Center.

Sistema de Segurança

A edificação de um Data Center deve ser extremamente segura, pois trata-se de um ambiente que abriga dezenas de equipamentos caríssimos e qualquer incidente que provoque sua parada pode ser catastrófico. Assim, é imprescindível a um Data Center possuir um bom sistema de segurança de todo o site.

Como o tema segurança é muito vasto, visto que se aplica a diversos aspectos, no caso de um Data Center, para simplificar a compreensão, podemos dividir a segurança em duas categorias: segurança física e segurança lógica.

Para a segurança física de um DC, é importante que os projetistas considerem os seguintes aspectos:

- Projeto do edifício (projeto civil) prevendo ameaças naturais (enchentes, terremoto, etc.);
- Controle de acesso (biométrico, cartão magnético, de aproximação, etc.);
- Monitoramento do site e vigilância por CFTV (sensores e câmeras);
- Detecção e alarmes (invasão, incêndio, etc.).

A segurança lógica diz respeito aos aspectos de confidencialidade, integridade e autenticidade de todas as informações presentes no DC. Como a área que estudamos é muito vasta e esta disciplina está voltada principalmente para os aspectos de infraestrutura física do DC, abordaremos aqui apenas a segurança física.

Acerca do primeiro aspecto da segurança física, o qual diz respeito ao projeto civil do edifício, é responsabilidade do projetista considerar possíveis desastres naturais, como terremoto, inundações, furações ou tempestades. O ideal é que o DC

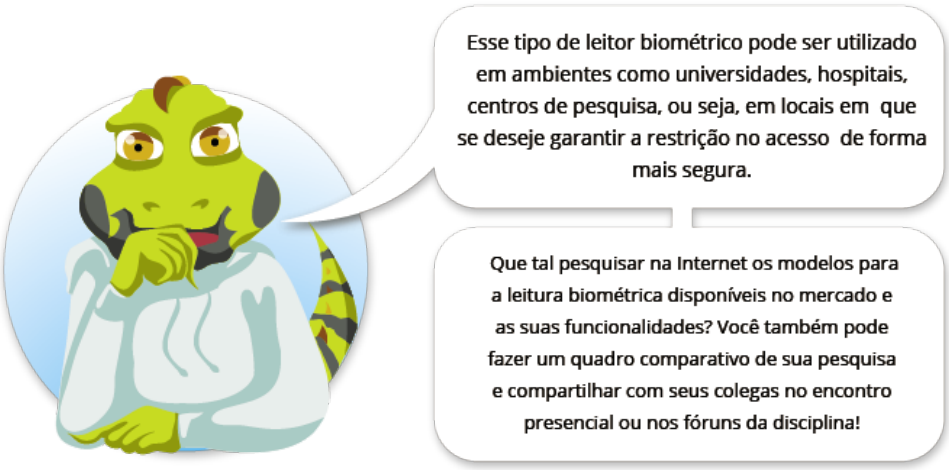
seja instalado em áreas livres desses problemas, mas, se isso não for possível, é fundamental que o projeto do prédio já esteja preparado estruturalmente para tais sinistros da natureza.

O controle de acesso a um Data Center é realizado normalmente por leitores que permitem a identificação de pessoas, sendo mais utilizados os leitores biométricos. A Figura 1 mostra um exemplo de leitor biométrico presente nas portas de acesso a um Data Center. Esse leitor é ligado em rede a um software de gerenciamento no qual há um cadastro contendo as digitais (normalmente a do polegar direito) dos usuários autorizados a entrarem no DC. Toda vez que a porta é aberta, ficam registrados data, hora, minuto, segundo e o respectivo usuário que a abriu.

Figura 01 - Leitor biométrico para acesso ao Data Center.

Fonte: Site da Magazine Luiza. http://blogdalu.magazineluiza.com.br/leitor-biometrico-substitui-a-chamada-em-sala-de-aula-2/11600/2011/11/. Acesso em: mar. 2017.

Os demais aspectos - monitoramento, vigilância e alarmes - serão vistos nas seções seguintes.



Automação com DCIM (Data Center Infrastructure Management)

Como toda a infraestrutura de um Data Center é algo relativamente complexo, é necessário o uso de ferramentas computacionais a fim de auxiliar no seu monitoramento e gerenciamento. Por exemplo, caso a pessoa que entrou na sala de computadores seja um cliente utilizando o serviço de *Collocation* de equipamentos, é preciso que o sistema de vigilância por câmeras esteja integrado ao controle de acesso para verificar se ela está trabalhando no corredor onde seu equipamento se encontra.

Pensando nessa problemática, os engenheiros criaram a categoria de sistemas chamada de **Data Center Infrastructure Management** (DCIM), a qual diz respeito a um conjunto de soluções que centralizam o monitoramento, a gerência e o planejamento das capacidades dos sistemas críticos de um DC. Essas soluções são compostas de softwares e hardwares integrados que coletam informações e agem quando necessário para o controle automatizado de todo o ambiente do DC. A ideia é centralizar todo esse monitoramento e controle no NOC (*Network Operation Center*), de modo que sua equipe possa observar o status do ambiente por inteiro e adotar as ações necessárias para qualquer eventualidade. A Figura 2 exibe um exemplo de NOC de Data Center com as informações disponibilizadas pelo DCIM.

Figura 02 - NOC de um Data Center.

Fonte: http://www.datacentermap.com/usa/florida/tampa/hivelocity_gallery.html. Acesso em: mar. 2017

Os subsistemas de um DCIM incluem, entre outros, o sistema de visualização de uso dos recursos e planejamento das capacidades, o sistema de vigilância por câmeras (CFTV), os diversos sensores presentes na sala de computadores e o sistema de combate a incêndio. Todos esses serão abordados nas próximas seções.

Atividade 01

1. Por que a segurança de um Data Center é tão importante? Justifique a sua resposta relacionando-a com o conceito de disponibilidade.
2. Cite pelo menos duas ameaças naturais que um Data Center pode sofrer.
3. O que é um Data Center Infrastructure Management (DCIM)?

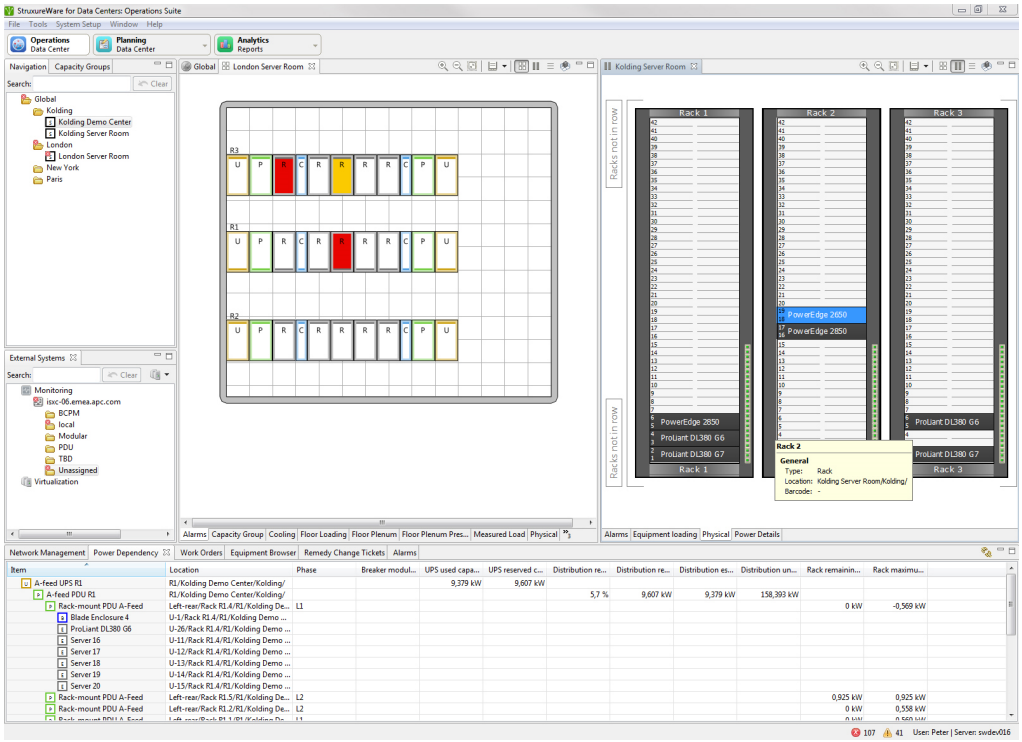
Gerenciamento e monitoramento

Uma das principais funções do NOC (*Network Operation Center*) é visualizar em tempo real tudo que acontece no Data Center. Para isso, é fundamental ao software de DCIM (*Data Center Infrastructure Management*) disponibilizar as informações

mais relevantes de maneira gráfica, objetivando um rápido entendimento do que está acontecendo com qualquer recurso crítico do DC.

O fabricante de soluções para Data Center APC desenvolveu um conjunto de softwares que compõem o seu pacote de DCIM, sendo tal conjunto chamado de *StruxureWare* for Data Centers. A Figura 3 apresenta um exemplo de tela desses softwares mostrando a situação de cada rack na sala de computadores em um determinado momento. O diagrama do centro da tela mostra as fileiras de racks com alguns destes em vermelho, sinalizando alguma situação crítica em sua operação, como sobrecarga no consumo de energia ou alta temperatura. No lado direito da tela pode-se observar o preenchimento de cada rack.

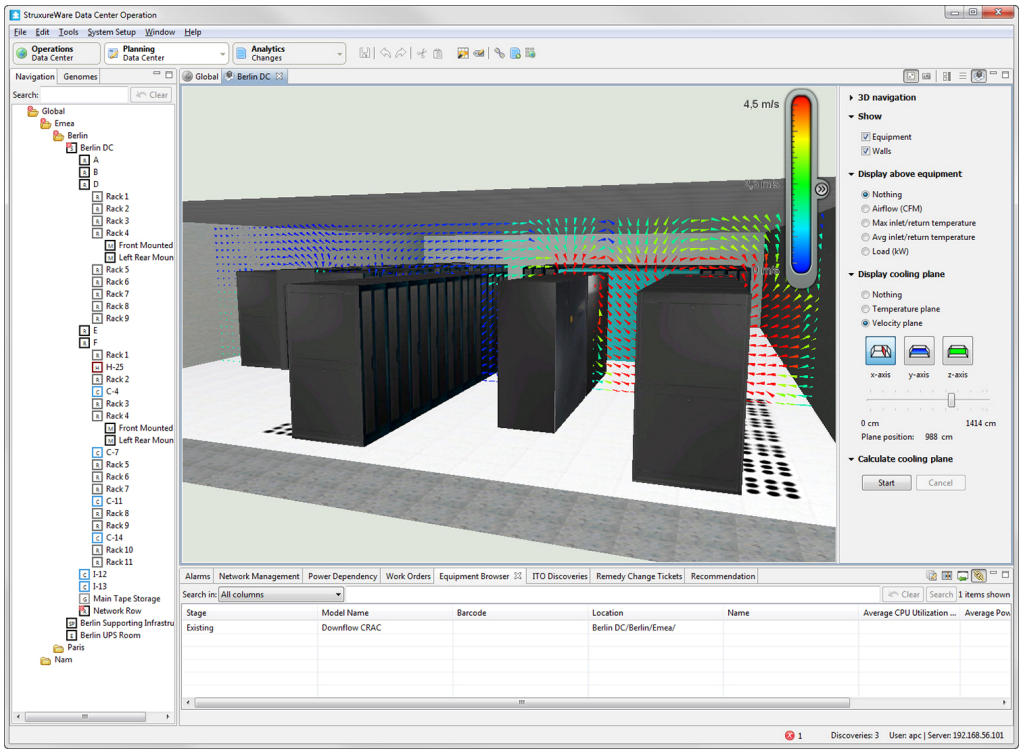
Figura 03 - Software StruxureWare for Data Centers da APC.



Fonte: Captura de tela do software StruxureWare for Data Centers da APC. http://www.apc.com/br/pt/. Acesso em: mar. 2017

Um dos módulos de software desse pacote é o *StruxureWare* Data Center *Operation* (SDCO), sendo este capaz de realizar o monitoramento em tempo real de todo o ambiente, calcular os níveis de eficiência energética e fazer um inventário de tudo o que está instalado e operando, entre outros recursos. A Figura 4 mostra uma tela do SDCO com as informações instantâneas das áreas fria e quente de um Data Center.

Figura 04 - StruxureWare Data Center Operation mostrando as áreas quente e fria de um DC.



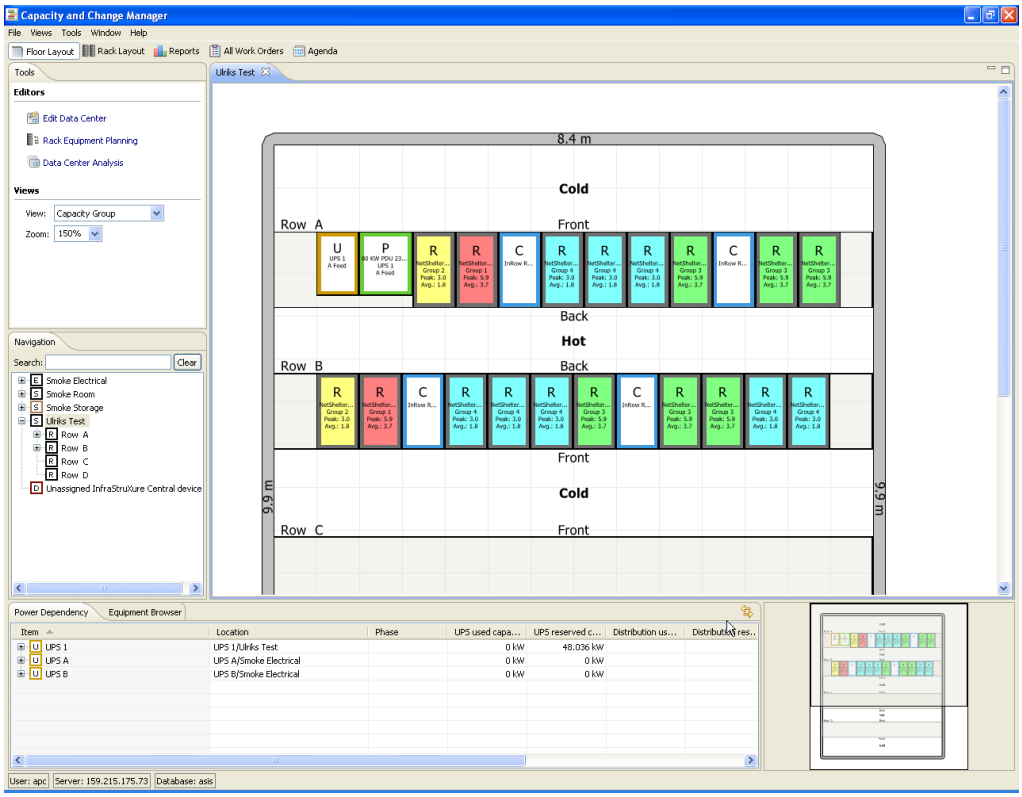
Fonte: http://business.leak.pt/wp-content/uploads/StruxureWareTM-Data-Center-Operation-para-Infraestruturas-Partilhadas.jpg. Acesso em: mar. 2017

Essa visualização das zonas quente e fria do Data Center só é possível a partir da leitura de diversos sensores de temperatura instalados nos racks e em outros locais da sala de computadores. Cruzando essas informações, é possível a visualização tridimensional de como está a refrigeração no ambiente e de qual rack está gerando mais calor em determinado instante.

Planejamento das capacidades

Uma outra função do NOC é planejar e implementar demandas para o Data Center, adicionando novos equipamentos quando necessário. Entretanto, toda nova adição de equipamentos de TI ao Data Center implica em maiores consumos de energia e, consequentemente, novas necessidades de refrigeração, assim como a remoção de qualquer equipamento pode desequilibrar a distribuição de energia e calor entre os racks. Para tratar dessas questões, o SDCO disponibiliza o software *Capacity and Change Manager*, visto na Figura 5.

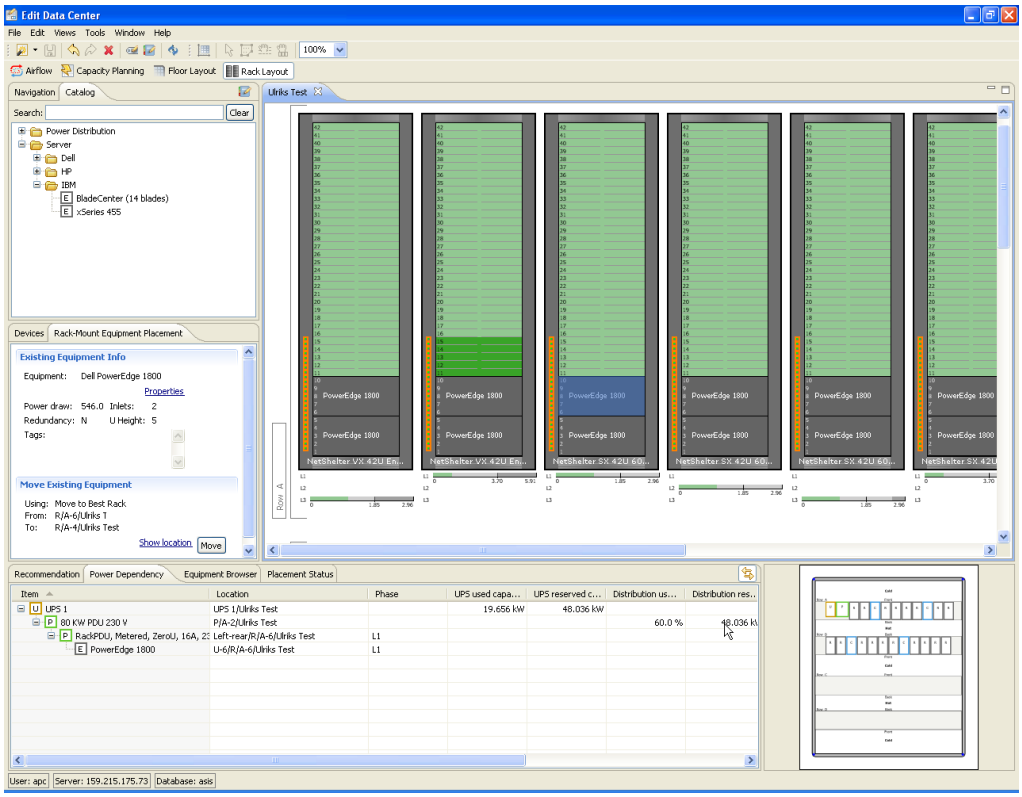
Figura 05 - Gerenciamento das capacidades e mudanças com o SDCO.



Fonte: Captura de tela do software Capacity and Change Manager da APC http://www.apc.com/br/pt/. Acesso em: mar. 2017.

A partir desse software (Figura 5), é possível "desenhar" com medidas exatas toda a sala de computadores do Data Center, em termos de espaços físicos e ocupação de cada rack. Além disso, os sensores de consumo de energia e de temperatura dão um panorama geral e preciso de como está o consumo de recursos e quais são as capacidades ociosas por rack de equipamento e, consequentemente, de todo o Data Center. Com essas informações e com o catálogo de equipamentos de TI dos principais fabricantes, o software sabe qual será o impacto energético do novo equipamento no DC e permite, ainda, indicar qual rack deve ser utilizado e em qual PDU esse novo equipamento deve ser ligado. A Figura 6 mostra um exemplo de tela da edição do Data Center para adição de um novo equipamento.

Figura 06 - Planejando a ocupação dos racks para a adição de um novo equipamento.



Fonte: Captura de tela do software Capacity and Change Manager da APC. http://www.apc.com/br/pt/. Acesso em: mar. 2017.

Atividade 02

1. Para que serve o NOC (Network Operation Center) de um Data Center?
2. Como é possível o software de DCIM fazer uma visualização tridimensional das áreas quente e fria da sala de computadores?
3. Por que é importante planejar a instalação de um novo equipamento de TI na sala de computadores?

Vigilância do Data Center

Um outro tipo de ameaça a um Data Center ainda não comentada é a de vandalismo realizado por pessoas com a simples intenção de prejudicar o funcionamento do ambiente e trazer diversos prejuízos às organizações que o

utilizam. Já pensou se um dos Data Centers do Google parasse? Quais prejuízos isso traria aos usuários do Gmail, do YouTube e ao próprio Google?

A vigilância de todo um Data Center é feita, geralmente, de duas formas: vigilância física realizada por pessoas (seguranças), e vigilância eletrônica feita por equipamentos de circuito fechado de TV (CFTV), isto é, câmeras de captura de imagens dos ambientes.

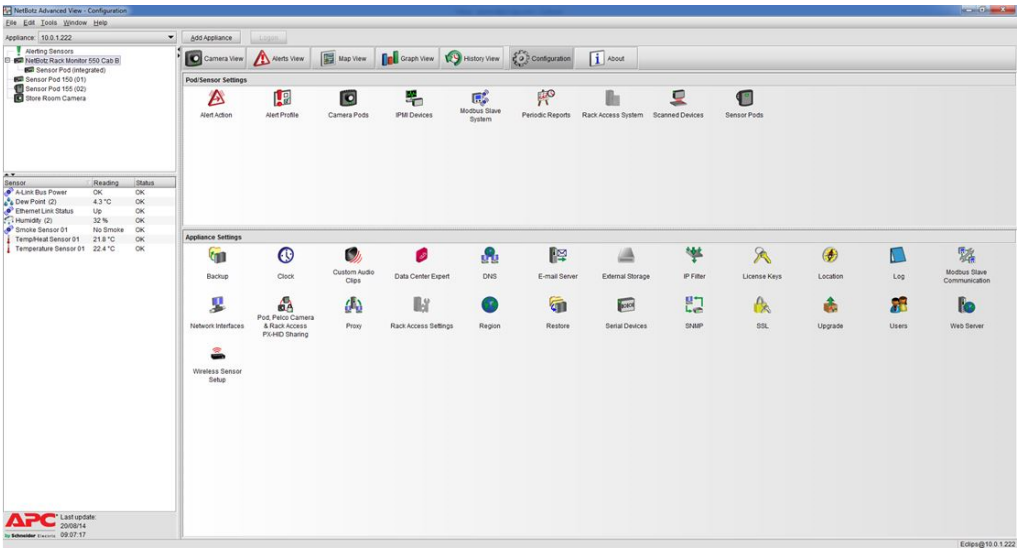
A Figura 7 mostra alguns equipamentos da APC para monitoramento e vigilância de ambientes.

Figura 07 - Kit NetBotz 400 da APC para monitoramento do DC.

Fonte: http://www.schneider-electric.com/en/product-range/61832-netbotz-400?N=459529965. Acesso em: mar. 2017.

Na Figura 7, a caixa inferior é uma espécie de switch que provê conectividade e energia para câmeras (equipamento superior) e sensores. Um dos sensores ligados nesse switch é o de temperatura, instalado na frente e na traseira de cada rack. Assim, esse switch coleta todas as informações desses diversos sensores (lembre-se que uma câmera também é um sensor) e as envia para o software NetBotz Advanced View apresentado na Figura 8.

Figura 08 - Software NetBotz Advanced View gerenciando os diversos sensores instalados.



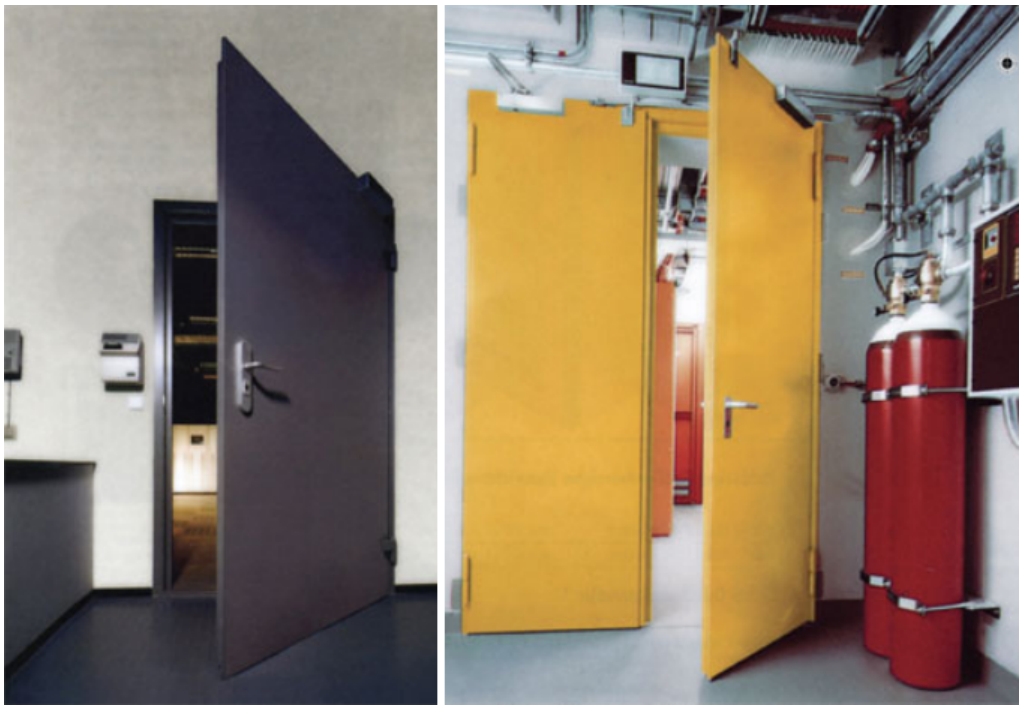
Fonte: http://ecl-ips.com/wp-content/uploads/2014/08/netbotz-advanced-view-4.3.0.-2.jpg. Acesso em: mar. 2017.

Proteção contra incêndio

Por se tratar de um ambiente com um número elevado de equipamentos e uma alta carga de energia, uma outra grande ameaça a um Data Center é a de incêndio provocado por curto-circuito nas instalações elétricas.

Uma das medidas simples para que um incêndio na edificação não entre na sala de computadores do Data Center é utilizar portas do tipo corta-fogo, como as vistas na Figura 9. Essas portas previnem que qualquer fogo fora da sala entre no ambiente, além de permitirem uma rápida abertura em caso de emergência. Elas são normalmente encontradas nas escadas que servem como rota de fuga em caso de incêndio em um edifício. Em relação aos Data Centers, essas portas devem ser bastante amplas para permitir a entrada de grandes equipamentos.

Figura 09 - Exemplos de portas corta-fogo instaladas em Data Center.



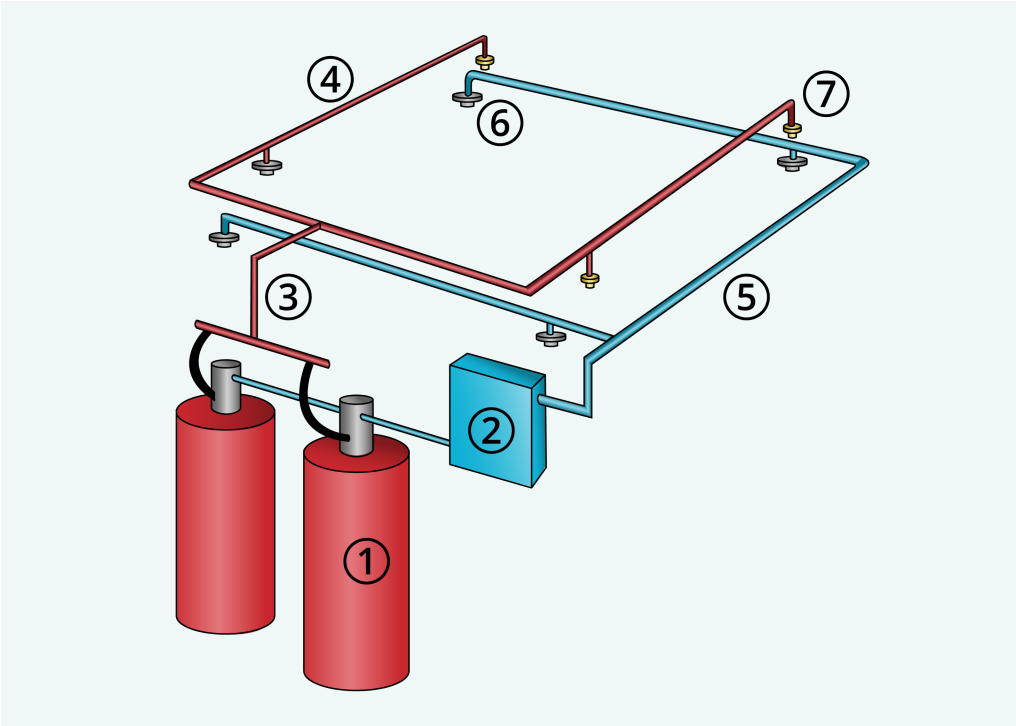
Fonte: Site da Acecoti, http://www.acecoti.com.br/solucoes. Acesso em: mar. 2017.

Marin (2011) define que um sistema de proteção contra incêndio deve ter três elementos básicos:

- **Detecção:** pode ser de fumaça, calor ou fogo;
- **Supressão:** refere-se aos sistemas de extinção de fogo (sprinklers de gases inertes não inflamáveis, como o gás FM-200);
- **Sistema:** inclui os sistemas de detecção, bem como os meios de acionar avisos sonoros e visuais (alarmes), além de notificar o departamento pertinente e acionar sistemas automáticos de contenção do incêndio.

Basicamente, o sistema de combate a incêndio na sala de computadores, mostrado na Figura 10, é composto dos seguintes elementos: 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 (*sprinkler*).

Figura 10 - Sistema de supressão de incêndio, por meio da utilização de gases inertes.



Fonte: Autoria própria (2017).

O gás utilizado nos Data Centers da UFRN é o **HFC-227ea** (heptafluorpropano). Esse gás extingue o fogo por uma ação física que resfria rapidamente as chamas e por uma reação química sobre os radicais livres do fogo. Ele é totalmente inofensivo para as pessoas que estão no ambiente, pois não retira o oxigênio deste. A Figura 11 mostra o cilindro do gás e os circuitos de detecção (duto flexível preto) e de extinção (duto rígido vermelho), presentes no Data Center do IMD.

Figura 11 - Cilindro de gás e dutos de detecção e combate a incêndio no DC do IMD

Fonte: Autoria própria (2017).

Chegamos ao fim desta aula. Viram o quanto é importante termos diversos mecanismos de segurança que garantam o bom funcionamento do Data Center? Esses mecanismos são extremamente relevantes para garantir a alta disponibilidade dos serviços deste.

Na próxima aula, iniciaremos os estudos dos equipamentos de TI presentes em um DC, começando pelos equipamentos de processamento e virtualização de computadores. Até lá!

Leitura Complementar

- 6 sistemas de um Data Center seguro e de alta disponibilidade: Disponível em: <http://www.redesecia.com.br/data-center/sistemas-de-um-data-center/.>

- Data Center Infrastructure Management (DCIM): Disponível em: <http://www.schneider-electric.com/b2b/en/solutions/system/s4/data-center-and-network-systems-dcim/.>

- Data Center II: Combate e Prevenção de Incêndios: Disponível em: <http://www.teleco.com.br/tutoriais/tutorialdcseg2/pagina_3.asp>

- Como fica a segurança do Data Center em 2017? Disponível em: <http://www.itforum365.com.br/seguranca/ameacas/como-fica-a-seguranca-do-data-center-em-2017.>

Resumo

Nesta aula conhecemos os sistemas de segurança e automação de um Data Center. Vimos que a segurança física de um DC depende de vários aspectos, sendo a automação fundamental para lidar com toda a complexidade de sua infraestrutura. Essa automação é feita por meio do trabalho integrado de softwares e hardwares, ambos provendo gerenciamento, monitoramento e ações para combater sinistros que possam causar a parada do DC. Um desses sinistros seria um possível incêndio na sala de computadores, então, vimos como é um sistema que detecta e combate incêndios no DC.

Autoavaliação

1. Quais são os aspectos de segurança física que um projetista de Data Center deve considerar?
2. Qual a diferença entre segurança física e segurança lógica em um Data Center?
3. Por que o gerenciamento e o monitoramento de um Data Center são imprescindíveis para a organização que o utiliza?
4. Do que é composto um sistema de vigilância de um Data Center?
5. Do que é composto um sistema de combate a incêndio?

Referências

MARIN, Paulo Sérgio. **Data Centers - Desvendando cada passo: conceitos, projeto, infraestrutura física e eficiência energética.** São Paulo: Érica, 2011.

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