SEGURANÇA INFORMÁTICA E DAS COMUNICAÇÕES

- Ficha de Apoio -

CAPÍTULO 2. SEGURANÇA FÍSICA

1. **Controlo de Acessos**
2. **Tecnologias de Controlo de Acesso, Topologia e seu Funcionamento**
3. ***Data Center* (Centro de Dados)**
4. **Sistemas Activos e Passivos de Segurança**
5. **Sistemas de Segurança**
6. **Protecção contra Incêndios**
7. **Deteção e Extinção de Incêndio**
8. **Climatização**

O acesso físico pode ser compreendido como o tipo de sistema que torna o acesso físico a uma determinada área, totalmente controlada, sendo que somente pessoas autorizadas são permitidas a entrar. Estas medidas que podem ser tomadas para garantir a segurança e existência de algo ou alguém contra roubo, espionagem, sabotagem ou qualquer dano. No contexto da segurança da informação e sistemas, os elementos a proteger são a informação, os produtos e as pessoas.

A implementação de um processo de segurança informática na organização passa por um conjunto de várias etapas, de onde se destacam a identificação de vulnerabilidades e analise de risco, o desenvolvimento e implementação de politicas e procedimentos, a resposta a incidentes e a formação de utilizadores e administradores de sistemas.

A segurança física é feita nas imediações da empresa e leva em consideração a prevenção de danos causados por desastres locais ou ambientais, como terremotos, inundações e incêndios. Por isso, investigar a ocorrência de eventos climáticos passados é importante ao se planear os métodos de segurança física para protecção de funcionários, equipamentos, dados e do local. Além disso, ela trata de métodos para evitar o acesso de pessoas não autorizadas a áreas em que se encontram dados e informações críticas da empresa. Uma forma de fazer isso é implantar recursos de identificação de funcionários, como o uso de crachás, senhas e cadastro de digitais. Para ter uma boa segurança física é importante controlar a entrada e saída de equipamentos, materiais e pessoas da empresa por meio de registos de data, horário e responsável. Quando há a entrada de visitantes na empresa, eles não devem andar sozinhos, o ideal é que sejam acompanhados por algum funcionário até o local de destino e registrados no sistema. Outro tipo de

reforço para a segurança local é usar mecanismos, como fechaduras electrónicas, câmaras e alarmes, para controlarem o acesso aos ambientes que guardam *backups* e computadores com dados confidenciais. Para desenvolver uma boa segurança física é preciso analisar qual é o perfil da empresa, o tipo de protecção necessária, os investimentos possíveis e definir uma política de controlo de acesso físico que se encaixe ao modelo de negócio.

O principal papel da segurança física é manter pessoas não autorizadas ou não desejadas fora das instalações e do acesso a bens da organização e garantir o comportamento dos colaboradores como especificados nas regras. Os termos mais específicos relacionados com a área de informática não variam muito deste conceito, antes o expandem, pois passam a incluir a protecção de dados.

Para o planeamento e desenho da segurança física, tem de se procurar um conjunto de respostas a outras tantas questões, e entre as quais salientam:

- O que se esta a proteger?
- Qual a importância da informação a proteger?
- O que é mais importante, a confidencialidade, a integridade ou a disponibilidade?
- De quem ou de que ameaças nos estamos a proteger?

No fundo estas são as todas as questões que se colocam em uma análise prévia para a criação de uma política de segurança.

1. Controlo de acessos

Conjunto de subsistemas que permitem efectuar a gestão de um edifício, controlando os seus utilizadores e podendo restringir o seu acesso a determinados locais e até registar os seus movimentos.

O objectivo básico de um Sistema de Controlo de Acessos é extremamente simples: controlar quem pode estar num dado momento, num determinado local.

Figura 1 – Modelo de controlo de acesso

Frequentemente, as organizações têm a necessidade de saber quem tentou entrar num dado local utilizando um acesso valido ou se houve uma tentativa de acesso não autorizado ou, ainda que autorizado, o fez fora das horas normais de serviço.

Com a utilização de sistemas integrados a partir de um identificador único, um utilizador autentificado pode aceder ao interior da organização, ser-lhe permitido o acesso com a sua viatura, abrir todas as portas até ao seu alojamento, incluindo este, efectuar pagamentos, identificar-se perante o sistema de robótica, no caso de um empreendimento habitacional/turístico e ver, inclusive, debitadas automaticamente na sua conta todas as despesas de restauração, jogos, entre outros.

O objectivo final pretende ser a gestão global dos edifícios no que diz respeito á circulação de pessoas, viaturas, bens e, eventualmente equipamento informático.

2. Tecnologias de Controlo de Acesso, Topologia e seu Funcionamento

Banda magnética

Utiliza cartões de banda magnética, no entanto, é pouco segura pois a banda magnética é afectada por campos magnéticos, o que leva a que por vezes os dados gravados sejam corrompidos, e facilmente copiada.

Figura 2 – Exemplo de banda magnetica

Código de barras

Utiliza cartões em que são impressos códigos de barras e é também pouco segura pois estes são facilmente copiados.

Figura 3 – Exemplo de um código de barras

Chip / Circuito integrado (*Chipcard*)

Utiliza cartões que possuem um circuito integrado (*chip*) inserido, o qual está ligado a pontos de contacto metálicos, que são acessíveis para permitir que um leitor adequado possa ler os dados gravados no circuito integrado.

É uma tecnologia segura pois não permite cópia dos dados gravados no circuito integrado e que tem tido um grande incremento de utilização nos cartões de crédito e débito bancários, porém a sua utilização em sistemas de controlo de acessos não conheceu grande sucesso devido principalmente à baixa de preços dos sistemas de tecnologia de proximidade.

Existem vários tipos de circuitos integrados (*chips*) inseridos em cartões plásticos, que diferem basicamente na capacidade da sua memória de armazenamento de dados.

O acesso aos dados de cada *chip* de cada cartão é efectuado mediante a inserção de um código PIN, contudo, caso sejam efectuadas mais de 3 (três) tentativas erradas, funde-se um fusível e o *chip* é definitivamente inutilizado, o que evita tentativas de fraude.

Contacto

Utiliza dispositivos (normalmente porta-chaves) que possuem um circuito integrado (*chip*) inserido numa cápsula metálica com o aspecto de uma pilha de relógio grande, daí serem usualmente designados no mercado por "*iButtom*", que, ao contactarem com o leitor, permitem a leitura dos dados gravados no circuito integrado.

É uma tecnologia segura pois não permite cópia dos dados gravados no circuito integrado, no entanto, a sua utilização em sistemas de controlo de acessos não conheceu grande sucesso devido principalmente ao seu alto custo.

O número gravado no chip de cada dispositivo de identificação é único e já vem gravado de fábrica, assim evita a sua duplicação e tentativas de fraude.

Proximidade

Utiliza dispositivos (normalmente cartões ou porta-chaves) que possuem um circuito integrado (*chip*) inserido, o qual permite a leitura dos dados gravados por aproximação a um leitor adequado, daí a sua designação – esta tecnologia veio substituir as todas as tecnologias anteriormente descritas (banda magnética, código de barras, *chip* e contacto), com as seguintes vantagens:

- **Facilidade de leitura** – Pode realizar a leitura do identificador sem o retirar da carteira (depende do alcance da antena do leitor);
- **Versatilidade** – Existência de identificadores em vários formatos: cartão, porta-chaves, entre outros; e
- **Não pode ser copiado.**

Figura 4 – Exemplos de controlos de proximidade

Funcionamento

Existem vários tipos de *chips* de proximidade de diversos fabricantes.

O mais comum do mercado é o que funciona a uma frequência de 125 KHz.

É composto basicamente por três partes: o *chip*, a antena e o encapsulamento.

O princípio de funcionamento é através de antenas de rádio frequência (RF), sendo um o leitor de proximidade e a outra o próprio dispositivo de identificação (cartão, porta-chaves, entre outras.).

Como o dispositivo de identificação não possui bateria, ele consegue suprir a necessidade de alimentação eléctrica para o seu funcionamento da forma seguinte:

A antena do leitor emite uma frequência constante de baixa potência, quando o dispositivo de identificação é detectado numa área próxima do leitor, que varia de 5 cm à 90 cm de acordo com o tipo de leitor, a antena do dispositivo de identificação recebe os sinais das ondas de rádio frequência do leitor e, através de seu circuito electrónico interno, inicia o processo de armazenamento de energia para poder funcionar.

A atingir uma determinada carga, o circuito electrónico interno do dispositivo de identificação transmite para o leitor o número gravado no seu *chip*. Na prática, tudo isto, ocorre durante o processo de aproximar o dispositivo de identificação ao leitor, tudo muito rápido e imperceptível ao utilizador.

O número gravado no chip de cada dispositivo de identificação é único e já vem gravado de fábrica, evitando a sua duplicação e tentativas de fraude.

Biometria

Segundo (Magalhães e Santos, sem data) "O termo biometria deriva do gregos bios (vida) + metron (medida) e, na autenticação, refere-se à utilização de características próprias de um indivíduo para proceder à sua autenticação e/ou identificação perante um SI de uma organização."
E este mecanismo de medição de características é usado a anos, («Sistemas Biométricos César Tolosa Borja Álvaro Giz Bueno», 2018) aplicado por nós, até em coisas simples como uma chamada de voz, onde podemos ter um número não gravado e o nosso cérebro tenta comparar a voz que recebemos através do telefone com alguma amostra já registada em nossa mente e caso não haja um reconhecimento da voz presumimos que falamos com um estranho.

Também é registado na história que a recolha de dados e identificação segundo elas é usado a muito tempo antes do surgimento das tecnologias recentes como os casos apresentados abaixo:

- "(…) no século IX, houve um pico de interesse por parte dos pesquisadores em criminologia, quando tentaram relacionar características físicas com tendências criminosas. Isso resultou em uma variedade de equipamentos de medição e grandes quantidades de dados colectados. Os resultados foram inconclusivos, mas a ideia de medir as características físicas de um indivíduo parecia eficaz e o desenvolvimento paralelo da identificação por impressões digitais tornou-se a metodologia de identificação internacional utilizada pelas forças policiais em todo o mundo".(«Sistemas Biométricos César Tolosa Borja Álvaro Giz Bueno», 2018).
- "No século II a.C., os governantes chineses já usavam as impressões digitais para lacrar documentos importantes. Foi a primeira vez na história que impressões digitais identificaram positivamente uma pessoa. Desde então, a técnica de reconhecimento de impressões digitais evoluiu e passou a ser empregada em grande escala, tornando-se o principal método para comprovar, de forma inegável, a identidade de uma pessoa". (Zurita et al., 2017).

Os exemplos apresentados são somente de biometria física, mas é importante destacar que temos também a biometria comportamental que se baseia no estudo da indentação do padrão comportamental da pessoa como por exemplo o padrão de digitação (Filho Lavareda Matos 2022 de mouse [Tan et al., 2019]).

Entre estes 2 tipos de biometria apresentados o mais preciso é o físico, que será debatido nas secções abaixo.

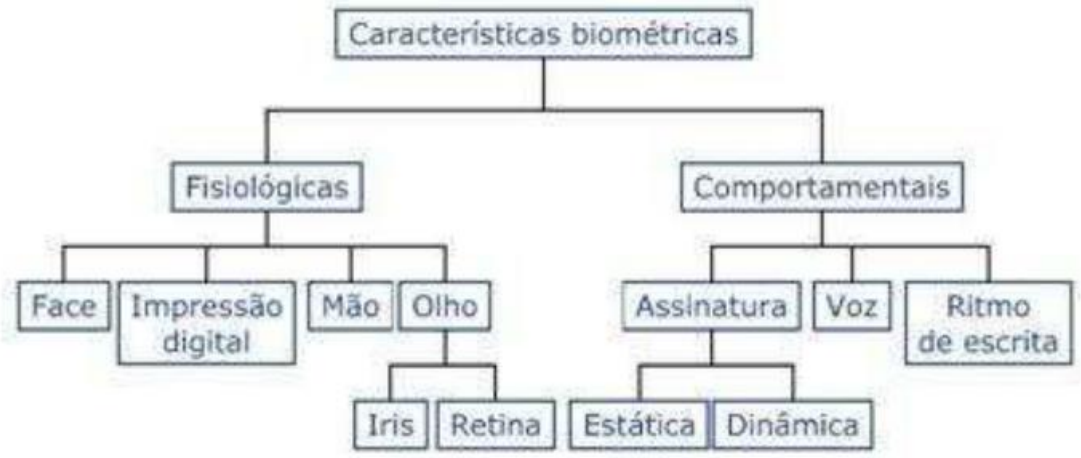

Figura 5 – Representação dos tipos de biometria

Principais tipos de biometria física

Reconhecimento da íris

O olho é composto por 8 partes principais (Helene e Helene 2011)sendo uma delas a iris que é a parte mais colorida do olho.

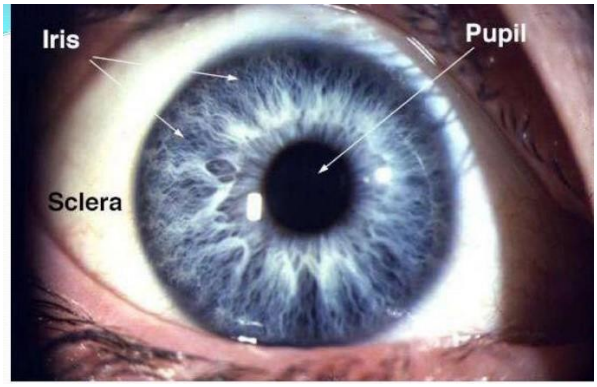

Figura 6 – Imagem representativa da Iris

O método de reconhecimento das iris baseia-se no facto de que com 11 milímetros de diâmetro, cada iri possui mais de 400 características como ligamentos arqueados, sulcos, cristas, criptas, anéis, corona, sardas e um colar em ziguezague (Daugman 2009).

Tendo em conta que esta não muda ao longo da vida é um órgão protegido pela córnea e pelo humor aquoso[1], mas visível externamente a uma distância de até 1 metro. O seu reconhecimento não é afectado por lentes de contactos nem óculos.(«Sistemas Biométricos César Tolosa Borja Álvaro Giz Bueno», 2018).

Para o seu reconhecimento geralmente é usada uma câmera que captura uma imagem de alta resolução da íris que a converte para tons de cinza e a imagem capturada é então analisada pelo sistema para extrair padrões de íris exclusivos, como a forma e a textura da íris. O sistema compara os padrões de íris extraídos com um banco de dados de padrões de íris armazenados para determinar se o usuário está autorizado.

Figura 7 – Ilustração da captura dos dados da Iris

Reconhecimento da retina

Para além das iris também é possível realizar o reconhecimento pela retina que é a camada mais interna do globo ocular, que é feita analisando os padrões de vasos dos vasos sanguíneos na parte de trás do olho que possuem um padrão único de olho para olho e de pessoa para pessoa. (Hugo et al. 2011).

[1] O humor aquoso é um líquido incolor que preenche as câmaras oculares, especificamente a cavidade do olho entre a córnea e o cristalino

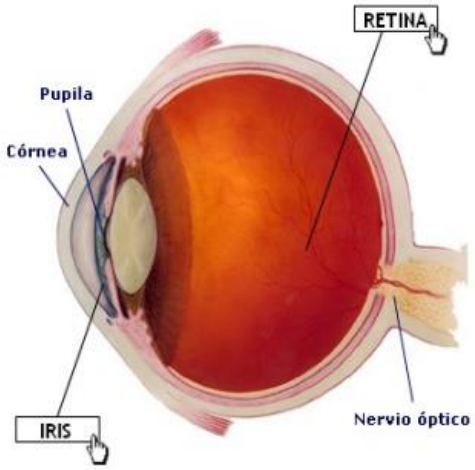

Figura 8 – Representação da Retina

Diferente da Iris o reconhecimento será comprometido caso o indivíduo esteja com óculos e para o reconhecimento, uma imagem da retina é capturada. A luz reflectida pelo objecto passa pela córnea e chega ao interior do olho através da pupila. A pupila funciona como a lente de uma câmera fotográfica, podendo se fechar ou se abrir, controlando a passagem da luz que chega até a retina. E é capturada a imagem que reflecte nos vasos sanguíneos e assim o sistema compara com o dado guardado na sua base de dados, para determinar se o usuário esta actualizado. («Sistemas Biométricos César Tolosa Borja Álvaro Giz Bueno», 2018).

Reconhecimento por impressão digital

Impressões digitais são características únicas de primatas, são formados a partir da sexta semana de vida e não variam as suas características ao longo da vida do indivíduo.(«Sistemas Biométricos César Tolosa Borja Álvaro Giz Bueno», 2018)

Este método é usado a muito tempo relatos históricos apontam para o seu uso mesmo antes do nascimento de Cristo, na China, com tábuas de barro usadas para identificar compradores e também em potenciais investigações criminais (Paoli, Dahia, e Amparo 2016).

Este processo foi estudado e teve como principal destaque da área o trabalho do agente da polícia argentina Juan Vucetich que aprimorou o formato de armazenamento de impressões digitais usando tinta e papel e sua classificação baseados em 4 padrões (Arco, Presilha Interna, Presilha Externa e

Verticilo) (Paoli, Dahia, e Amparo 2016). E com o passar do tempo esse método foi auxiliado com o uso de scanner sobre o papel para digitalizar a impressão digital. (Hugo et al. 2011). Agora o processo é realizado directamente do dedo da pessoa usando leitores de impressão digital baseados em processos ópticos.

O processo é realizado da seguinte forma:

- Colecta de Impressões Digitais: as impressões digitais são colectadas por meio de sensores.
- Análise de Impressões Digitais: a imagem digitalizada é então analisada por um software especializado que identifica os pontos característicos da impressão digital. Estes pontos são usados para criar um modelo matemático da impressão digital, que pode ser armazenado em um banco de dados e comparado com outras impressões digitais para fins de identificação.
- Reconhecimento: modelo armazenado é comparando com a impressão que o esta a ser passada pelo sensor no momento de autenticação do utilizador.

Figura 9 – Ilustração da captura dos dados da impressão digital

Reconhecimento facial

O reconhecimento facial é estudado desde 1960 que se focava em localizar características como olhos, ouvidos, nariz e boca e nessa época era necessária uma imagem 2D[2], mas com a evolução das tecnologias passou a ser possível o uso de sistemas 3D[3].

O processo e reconhecimento ocorre da seguinte maneira:

[2] 2D é a abreviação para duas dimensões. Refere-se a qualquer forma ou objecto que tenha apenas duas dimensões: largura e altura.

[3] 3D ou três dimensões, que inclui a profundidade além da largura e altura.

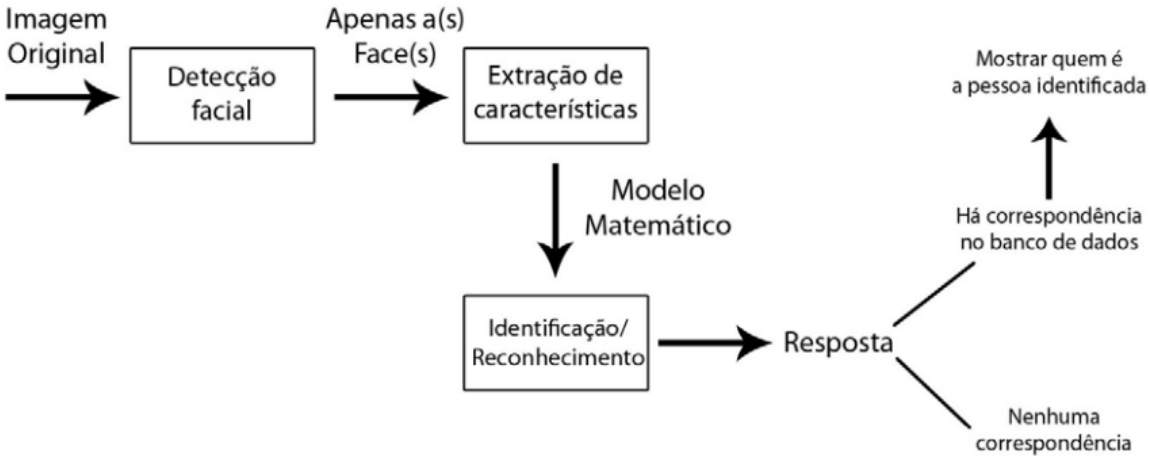

Figura 10 – Diagrama do funcionamento de reconhecimento facial

- Fase de detecção do rosto: onde é localizado a face que desejamos analisar;
- Analise do rosto: ocorre depois da captura da imagem da face, o *software* realiza uma leitura geométrica do rosto, identificando características como distância entre os olhos, entre a testa e o queixo, entre outros;
- Conversão da imagem em dados: através de algoritmos a imagem captura e transformada em dados; e
- Localização de uma correspondência: os dados obtidos são comparados com aqueles existentes na base de dados.

Características	**Reconhecimento de Retina**	**Reconhecimento de Íris**	**Impressão Digital**	**Reconhecimento Facial**
Método de Captura	Escaneamento da Retina	Escaneamento da Íris	Leitura da Impressão Digital	Análise da Geometria Facial
Nível de Intrusividade	Baixo (Não invasivo)	Baixo (Não invasivo)	Muito Baixo (Não invasivo)	Baixo (Não invasivo)
Precisão	Elevada	Elevada	Elevada	Variável
Velocidade de Verificação	Moderada a Rápida	Rápida	Rápida	Rápida

Estabilidade	Sensível a Condições Oculares	Sensível a Mudanças na Íris	Sensível a Condições da Pele	Sensível a Iluminação e Mudanças na Face
Nível de Aceitação Pública	Moderado	Moderado	Elevado	Elevado
Aplicações Comuns	Segurança de Alto Nível	Controle de Acesso Biométrico	Desbloqueio de Dispositivos	Identificação em Redes Sociais, Controle de Acesso
FAR (Taxa de Falsos Positivos)	Baixo	Baixo	Baixo	Variável, dependendo do sistema e configurações
FRR/FNRM (Taxa de Falsos Negativos)	Baixo	Baixo	Baixo	Variável, dependendo do sistema e configurações

Tabela 1 - Tabela comparativa entre os diferentes tipos de biometria

Desempenho de Sistemas Biométricos

O desempenho de Sistemas Biométricos é normalmente medido por várias taxas que ajudam a avaliar a eficácia e confiabilidade do sistema.

As principais taxas são:

- **FAR / FMR**: é a taxa que indica a probabilidade de um sistema erroneamente aceitar uma identidade válida. Em outras palavras é a taxa de ocorrência de falsos positivos[4]; e
- **FNRM / FRR**: é a taxa que indica a probabilidade de o sistema não reconhecer correctamente uma identidade válida. Que é determinada como uma ocorrência de falsos negativos[5].

[4] Falso positivo se refere a situações em que um teste ou sistema indica incorrectamente a presença de uma condição ou evento que não é verdadeiro.

[5] Falso negativo é quando o teste indica que algo não está lá, mas na verdade está.

Aspectos relevantes para comparação entre os tipos de biométria

Para a comparação entre sistemas biométricos para além do uso das taxas de desempenho são analisados os seguintes factores:

- **Universalidade**: refere-se à presença da característica biométrica em todos os indivíduos;
- **Unicidade:** refere-se ao factor de a característica sem única para cada pessoa;
- **Estabilidade:** refere-se à estabilidade da característica ao longo do tempo;
- **Capacidade de captura:** indica a facilidade com que a amostra biométrica pode ser adquirida;
- **Aceitação:** indica a disposição e facilidade das pessoas em usar o método biométrico; e
- **Resistência a fraude:** refere-se a dificuldade de enganar o sistema biométrico.

3. *Data Center* (Centro de Dados)

Figura 11 – Apresentação de um Centro de Dados

Centro de Dados (*Data Center*), ou Centro de Processamento de Dados, é um ambiente projectado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e sistemas de activos de rede, como switches, roteadores entre outros.

O surgimento da computação moderna**,** a partir da década de 90, revolucionou o mundo e ocasionou uma necessidade de eficácia e rapidez computacional para comportar e assegurar o desenvolvimento dessa tecnologia inovadora.

Com a finalidade de abrigar milhares de servidores e base de dados, e processar grandes quantidades de informação, os equipamentos geralmente são montados em *racks* ou armários metálicos. Possuem protecção contra incêndios, além de sistemas de resfriamento dos *racks*, para manter uma temperatura estável. Esses espaços são fundamentais para serviços e actividades de diversos sectores da economia: energia, iluminação, telecomunicações, Internet, transportes, tráfego urbano, bancos, sistemas de segurança, saúde pública, entretenimento, e muitos outros. A vida na maioria das cidades depende do bom funcionamento e da disponibilidade de um ou vários *Data Centers*.

Para além da componente empresarial, hoje em dia, é muito comum o uso das *Clouds* para uso pessoal, a utilização destas aplicações em computadores pessoais, *smartphones* e *tablets* é muito usual. Diversas organizações possuem serviços como este fazendo com que a existência de *Data Centers* seja de elevada importância para todos os ficheiros ou documentos que pretendemos guardar em *Cloud*.
A energia necessária para o funcionamento de um *Data Center* não pode falhar, visto que algumas empresas podem perder muito dinheiro com a falha de servidores. Os profissionais de TI, portanto, desenvolvem ambientes com *no-breaks*, que regulam a voltagem e a pureza da energia, e geradores, caso haja algum problema com o fornecimento de energia local. Além disso, a segurança é uma preocupação primordial, pois dados confidenciais podem estar contidos nos servidores.

PRINCIPAIS ÁREAS DE UM DATA CENTER

***Entrance Room* (ER):** A sala de entrada é um espaço de interconexão entre o cabeamento estruturado do *Data Center* e o cabeamento proveniente das operadoras de telecomunicação.

***Main Distribution Area* (MDA):** Inclui o *cross-connect* principal, que é um ponto principal de distribuição de um cabeamento estruturado de um *Data Center*, nesta área se faz as principais manobras do *Data Center*, é uma área crítica.

***Horizontal Distribution Area* (HDA):** É uma área utilizada para conexão com as áreas de equipamentos. Incluí o *cross-connect horizontal* (HC), e equipamentos intermediários.

***Zone Distribution Area* (ZDA):** Ponto de interconexão opcional do cabeamento horizontal. Posicionado entre o HDA e o EDA permite uma configuração rápida e frequente, geralmente posicionada em baixo do piso. Provê flexibilidade no *Data Center*.

***Equipment Distribution Area* (EDA):** Espaço destinado para os equipamentos terminais (Servidores, *Storage*) e os equipamentos de comunicação de dados ou voz (switches centrais "*core*").

CERTIFICAÇÃO TIER PARA *Data Center*

O Objectivo da certificação TIER (camada) é classificar e mensurar o nível da infra-estrutura de um *Data Center*. A segurança e a disponibilidade desse bem tão precioso são requisitos críticos para avaliar a qualidade de um *Data Center*. Para diversas empresas ficar "fora do ar" não é uma opção. A classificação Tier é justamente o que estabelece os níveis de operação, ou seja, aponta o quão preparados os *Data Centers* para evitar problemas de infra-estrutura, que podem comprometer a segurança das informações e a conectividade que gera acesso contínuo aos dados.

DIVISÃO DO SISTEMA TIER

O sistema Tier é classificado em quatro níveis (I,II,III,IV), e tem como função comparar a funcionalidade, capacidade e a disponibilidade de um *Data Center*, quanto maior o nível, maior a redundância da infra-estrutura e menor a probabilidade de interrupção em caso de crise. Por falar em redundância, ela pode ser entendida como uma duplicidade de equipamentos, sistemas, entre outros factores e tem como objectivo evitar o tempo de interrupção (*downtime*) por falhas e manutenção preventiva ou correctiva.

Porém, as exigências de classificação são específicas e diversas.

Classificações Tier:

Tier I: Classificação Básica

Este nível fornece condições básicas para atender os equipamentos de TI e não há obrigatoriedade de qualquer componente redundante da infra-estrutura. Algumas das necessidades exigidas são *no-breaks* (UPS), sistemas de climatização completos, chamados de componentes de capacidade, geradores e seus tanques com bombas de combustível e tudo isso é exigido que funcionem correctamente para toda área crítica de TI pensada para o *Data Center*. Apesar de todo esse aparato, durante manutenções correctivas ou preventivas o serviço não é capaz de ser mantido de forma contínua tendo assim que suspender ou pausar seu funcionamento.

Esse nível é ideal para pequenos negócios onde a Tecnologia de Informação esteja focada nos processos internos.

Resumo dos requisitos para Tier I:

- 99,671% de *uptime* (tempo de actividade);
- Não há exigência de redundância; e
- Pode sofrer 1,2 falha de equipamentos ou infra-estrutura de distribuição por ano.

Tier II: *Data Center* redundante

Este nível atende todos os requisitos da classificação anterior e tem como diferencial uma infra-estrutura parcialmente redundante, que oferece um pouco mais de agilidade em serviços de manutenção, fazendo com que as interrupções sejam apenas uma por ano, ajudando a reduzir os impactos dos equipamentos por conta de falhas na infra-estrutura. O nível II é voltado para pequenas instalações, cuja a criticidade do negócio é maior, podendo não suportar indisponibilidades durante horário comercial.

Resumo dos requisitos para Tier II:

- 99,749% de *uptime*;
- 22 horas de inactividade por ano; e

- Redundância parcial em energia / refrigeração.

Tier III: Sistema Auto Sustentado

O *Data Center* Tier III possui redundância para realizar qualquer manutenção preventiva que possa ser solicitada em toda a infra-estrutura sem que haja necessidade de se suspender nenhum serviço crítico de TI. Para que isso seja realizado, é necessário que todo equipamento de TI seja conectado a caminhos eléctricos diversos através das suas fontes redundantes.

Esse nível é ideal para empresas que disponibilizam suporte 24h x 7 dias na semana, negócios cujos recursos de tecnologia de informação suportam processos de negócios automatizados e empresas com vários turnos de horários com clientes e funcionários em diversas áreas regionais.

Resumo dos requisitos para Tier III:

- 99.982% de *uptime*;
- 1.6 horas de inactividade por ano; e
- 72 horas de protecção contra interrupção de energia.

Tier IV: Alta Tolerância a Falhas

Esta categoria é completamente redundante ao nível dos circuitos eléctricos, de arrefecimento e de rede. Esta arquitectura permite ultrapassar qualquer cenário de incidentes técnicos sem jamais interromper a disponibilidade dos servidores no local.

- 99,995% de *uptime*;
- Redundância integral; e
- 96 horas de protecção em casos de queda de energia.

Diante destes cenários, é importante destacar que cada empresa possui necessidades diferentes, e ao escolher um *Data Center*, é necessário avaliar tais necessidades para que se faça a escolha correcta. E, claro, escolher um *Data Center* que possui todas as exigências que o negócio precisa e vai garantir tranquilidade, disponibilidade, menor tempo de resposta e o principal: a segurança.

4. Estrutura do *Data Center*

Os *Data Centers* possuem equipamentos que contam com tecnologia avançada, como servidores, fontes de alimentação com grande capacidade, controlo de temperatura, sistemas de segurança e gestão avançados, tudo para proteger e permitir um funcionamento contínuo de toda Infra-estrutura. Toda a sua estrutura tem de ser pensada para proteger toda a informação contida nos seus servidores e para isso sistemas activos e passivos de segurança devem ser dimensionados e instalados de acordo com vários critérios. Um exemplo de uma norma, que cobre os requerimentos de protecção para este tipo de infra-estruturas é a *National Fire Protection Association (NFPA) 75 – Standard for the Protection of Eletronic Computer/Data Processing Equipement.*

ALIMENTAÇÃO ELÉTRICA

Responsável por toda a alimentação do edifício, deve garantir o fornecimento interrupto de energia elétrica ou oscilações no seu funcionamento, incluído UPS e geradores de socorro para falhas de alimentação.

INFRA-ESTRUTURA DA REDE

Constituída pelas ligações entre equipamentos de comunicação e armazenamento de dados, ou seja, o interligam os componentes principais do *Data Center*. Esta rede é constituída essencialmente por condutores de cobre, os cabos mais utilizados são os *Unshield Twisted Pair* (UTP) e os *Shielded Twisted Pair* (STP) e cabos de fibra óptica.

Obviamente que esta infra-estrutura para funcionar possui os equipamentos activos de rede que se encontram instalados nos bastidores. Equipamentos estes que são responsáveis pela comunicação adequada entre os diversos equipamentos de rede, maioritariamente são *switches* e *routers*.

Nos bastidores são instalados não só estes como outros equipamentos essenciais, casos de discos duros e servidores.

VENTILAÇÃO

O edifício deve permanecer numa temperatura adequada para o correcto funcionamento de todos os equipamentos, o que previne o sobreaquecimento, oscilações na temperatura também podem ser

prejudicais ao correcto funcionamento de qualquer equipamento. Por isso um bom sistema de ventilação e de arrefecimento é de elevada importância num *Data Center*.

São várias as formas de ventilação das salas de *um Data Center* e todas têm um objectivo comum, efectuar uma ventilação eficiente do sistema.

Um exemplo muito usual é o da utilização dos chamados "corredores de ar quente" e "corredores de ar frio". Nesta solução os bastidores ou *racks* podem ser agrupados para que o ar quente seja extraído depois de ter efectuado a ventilação dos equipamentos.

Isto consegue-se insuflando o ar frio pelo chão falso, neste tipo de soluções os "corredores de ar quente" podem ou não ser isolados. Importante referir que esta solução serve para aumentar a eficiência do equipamento de ventilação e assim poupar energia. A Figura abaixo, mostra um exemplo de aplicação de ventilação por sistema de corredor.

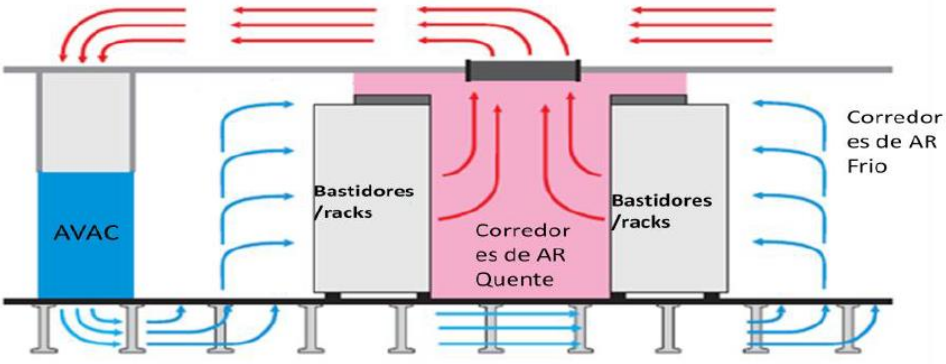

Figura 12 - Ventilação por sistema de corredor

A ventilação também pode ser efectuada de uma maneira mais comum, feita para que o ar frio seja encaminhado para os bastidores e depois o ar quente ser extraído pelo tecto falso, quando este existe. Mas fundamentalmente este tipo de ventilação pretende que o ar frio circule pelos equipamentos para os arrefecer. A Figura baixo, mostra um exemplo deste tipo de aplicação.

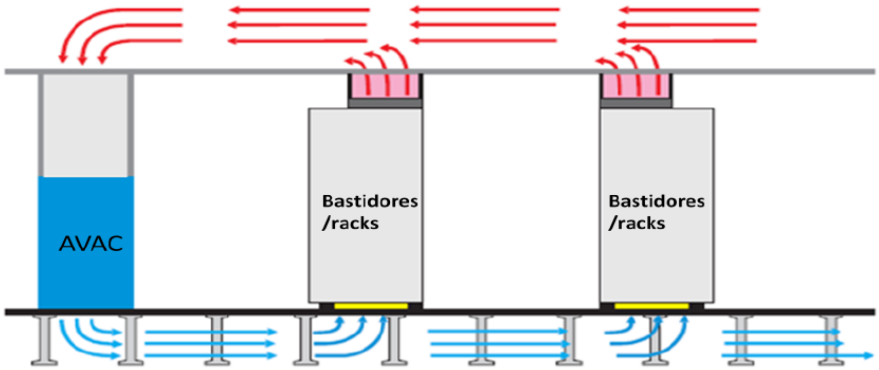

Figura 13 - Sistema convencional de ventilação

5. Sistemas Passivos de Segurança

A protecção passiva assume um papel de elevada importância no âmbito da protecção contra incêndio de um edifício e visa cumprir as seguintes funções: compartimentação, desenfumagem, protecção de estruturas e melhoria do comportamento ao fogo dos materiais de construção. Para isso a protecção passiva compreende todos os materiais, sistemas e técnicas que visam impedir ou retardar a propagação dos incêndios.

A protecção passiva contra incêndio pode dividir-se em cinco áreas:

- Resistência ao fogo de elementos estruturais e de elementos integrados em instalações técnicas, que inclui a manutenção das funções dos mesmos; A compartimentação vertical e horizontal dos edifícios, que inclui as paredes e lajes com características de resistência ao fogo e todos os sistemas complementares;
- As condições de evacuação dos edifícios, incluindo os locais e as vias de evacuação;
- Os materiais e elementos de construção e de revestimento, com a adequada reacção ao fogo ou a produtos de tratamento de materiais e elementos de construção que visam melhorarem o comportamento ao fogo desses materiais e elementos;
- Sistemas de desenfumagem passiva que compreendem a aplicação de aberturas de admissão de ar novo e de escape de fumo, bem como, condutas de desenfumagem e registos resistentes; e
- Sistema de sinalização de segurança, que é composto por conjunto de sinais e outros produtos de marcação com características fotoluminescentes.

Por isso num *Data Center* não deverá ser diferente, as propriedades dos materiais das salas onde são instalados todos os equipamentos necessitarão de uma redobrada atenção pela sua importância.
Alguns dos aspectos são:
Protecção contra danos externos para as salas de armazenamento, processamento e telecomunicações;

- As salas mencionadas devem ser separadas de outros compartimentos existentes por construção resistente ao fogo;
- Não devem ser instaladas perto áreas ou estruturas em que processos perigosos sejam efectuados;
- Tanto o chão falso como o tecto falso devem ser constituídos por materiais não combustíveis; e
- Apenas equipamentos electrónicos e equipamento de suporte são permitidos nas salas mencionadas, caso exista equipamento de escritório este deve ser de metal ou de material não combustível.

6. Sistemas Activos de Segurança

O sistema de protecção activa contra incêndio normalmente é constituído Sistemas Automáticos de Detecção de Incêndio (SADI), Sistemas Automático de Extinção de Incêndio (SAEI), extintores, *sprinklers*, alarme e iluminação de emergência.

O SADI deve ser instalado de tal forma que permita uma célere detecção de incêndio, os botões manuais e as sirenes de alarme devem desempenhar também um papel fundamental neste sistema.

O SAEI é o sistema responsável quando é necessário a protecção dos equipamentos, pois extingue o incêndio, permite uma redução do dano nos equipamentos e possibilita um fácil retorno de todo o serviço. Deverá ser utilizado gás como agente extintor de aplicação total.

Outro sistema de extinção utilizado são as redes de *sprinklers*, que nunca devem ser utilizados como primeiro meio de intervenção devido aos elevados prejuízos que acarretará. Sistemas de extinção que utilizam água não são aconselháveis para fogos de origem eléctrica, por isso a utilização de *sprinklers* só é adequada para protecção da estrutura e não para protecção dos equipamentos. Os extintores devem ser providenciados e ajustados para a classe de fogo existente no local.

7. Protecção contra Incêndios

Estas instalações apresentam um grande risco de incêndio pelo facto de abrigarem uma grande quantidade de carga combustível, muitos materiais inflamáveis como, plástico, borracha e tinta com muitas fontes de calor. Prevenir e combater a ocorrência de incêndios nos *Data Centers* não é apenas um questão de proteger as vidas humanas e estruturas mas também proteger a informação e imagem corporativa, já que possíveis danos a servidores e computadores podem significar a paralisação de empresas, custos avultados para substituição de equipamentos danificados e mais importante a perda de informação importante.

O maior risco de incêndio advém das instalações e componentes eléctricas, em que uma sobrecarga ou curto-circuito pode dar origem a um incêndio de grandes proporções. Outro aspecto importante de referir é o agrupamento de equipamentos electrónicos em diversos bastidores que consomem energia durante 24 horas e geram calor, por isso necessitarem de constante ventilação e arrefecimento, pois caso contrário, o aquecimento excessivo pode dar origem a um incêndio.

A segurança contra incêndios é bastante complexa, tanto a protecção passiva como a activa devem assegurar um grau elevado de protecção. A segurança física e estrutural do *Data Center* é tão importante como um SADI ou um SAEI, a utilização de divisórias corta-fogo, portas estanques corta-fogo, entradas e ductos blindados que não oferecem apenas uma segurança contra incêndios, mas também contra outros riscos físicos e estruturais como água, poeiras, fumos, interferências electromagnéticas, etc.

8. Deteção de Incêndio

Pelo facto de grande parte dos incêndios nos *Data Centers* terem origem eléctrica, e que normalmente produzem fogos que originam bastante fumo. Na Tabela abaixo são mostrados alguns exemplos de áreas de risco de um *Data Center* e o respectivo cenário típico de incêndio.

Compartimento/Equipamentos	Conteúdo	Cenário de incêndio
Salas de comunicações, armazenamento e processamento.	Equipamento eletrónico instalado em racks ou bastidores.	Desenvolvimento lento e produção de incêndios com bastante fumo dentro dos bastidores e racks.
Áreas de suporte técnico	Ferramentas, secretárias, armários, etc.	Baixa carga de incêndio e o cenário é o mesmo que nas salas de comunicações.
Alimentação elétrica e redes de comunicações	Várias zonas de alimentação a baixa tensão e cabos de comunicação	Baixa ou média temperatura que pode originar incêndios com bastante fumo.

Tabela 3 - Áreas de risco de um *Data Center*

Os detectores pontuais de fumo podem efectuar a detecção de incêndio nestes ambientes, mas iria verificar-se um atraso na detecção, potenciando os danos e as perdas aquando da ocorrência de um incêndio. Assim, devem ser instalados detectores de alta sensibilidade de modo a permitir uma detecção o mais precocemente possível e uma rápida intervenção humana ou por parte do sistema de extinção existente.
Os sistemas de detecção de aspiração de fumo, são os mais adequados para este tipo de instalações. Por ser um sistema activo que realiza uma análise constante do ar, determinando a quantidade de partículas de fumo presentes no mesmo, permitindo uma detecção precoce do incêndio.
Os detectores de aspiração devem cumprir os requisitos de normas, ao nível internacional existe por exemplo a Norma Europeia EN 54-20.

Segundo a EN 54-20 estes detectores são divididos em três classes que relacionam a sensibilidade do detector e a sua aplicação, conforme indicado na Tabela abaixo.

	Sensibilidade	Aplicação
Classe A	Muito Alta	Deteção muito precoce, zonas com um elevado grau de diluição de ar como, p. ex., condutas de ar condicionado de salas limpas.
Classe B	Alta	Deteção muito precoce de fogo na maioria das zonas onde são guardadas mercadorias de grande valor e/ou zonas de processamento.
Classe C	Normal	Deteção de fogo em zonas onde os detetores convencionais não são suficientes

Tabela 4 - Classificação dos detectores por aspiração segundo a EN 54-20

As tubagens deste detector podem ser instaladas juntos dos cabos no chão falso ou próximos dos *racks* onde estão instalados a maior parte dos equipamentos.

A detecção de incêndio num *Data Center*, passará sempre por cobrir todos os espaços existentes nas salas, chão e tecto falsos, tecto real e ventilação. Dependendo da configuração da sala a escolha do tipo de detecção terá de ter em conta obrigatoriamente o risco associado, sendo que a melhor solução passará sempre pela conjugação de detectores de fumo por aspiração com detectores pontuais de fumo ou térmicos. Nem sempre toda a detecção de incêndio passa pela instalação de detectores por aspiração, a utilização de detectores ópticos de fumo é muito utilizada. Por exemplo, a utilização de detectores ópticos no chão falso e tecto real em conjugação com uma detecção por aspiração nas grelhas de extracção de ar e por cima dos bastidores. A Figura abaixo, mostra um exemplo de detecção de incêndio por aspiração em grelhas de ventilação e bastidores.

Figura 14 - Deteção por aspiração em grelhas de ventilação e bastidores

9. Extinção de Incêndio

Como já foi mencionado neste capítulo, mas instalações de *Data Center*, existem vários meios de extinção de incêndio entre eles os extintores que devem ser adequados à classe de fogo existente no local onde este são instalados e os *sprinklers*, que sendo um meio de protecção e extinção de incêndio ativo só devem funcionar como protectores da estrutura e não como meios de primeira intervenção.

Para uma protecção dos equipamentos e para uma extinção eficaz do incêndio, devem ser utilizadas soluções de extinção por gás. Por um lado, uma solução de extinção que utilize água danificará sempre os equipamentos o que leva a tempos de paragem maiores e prejuízos mais avultados. Por outro lado, as soluções de extinção por gases levam a tempos de paragem muito pequenos, o que significa menos prejuízos, e os danos nos equipamentos é nulo.

De entre as opções de extinção por gases, as mais comuns são as que utilizam gases químicos ou gases inertes.

Este tipo de gases permite que o incêndio seja extinto, minimizando o impacto da extinção nos equipamentos e nos ocupantes do edifício. Com o desenvolvimento de novas formas de detecção e libertação do agente extintor, as soluções de protecção e extinção de incêndio em *Data Centers* são cada vez mais seguras e fiáveis.

PROCESSO DE EXTINÇÃO

Para se dar início ao processo de extinção é necessário a confirmação de alarme por parte de dois detectores automáticos de incêndio ou pela activação manual do sistema.

Num *Data Center*, a escolha recairá sempre por detectores de fumo, pontuais ou por aspiração, mas também é possível escolher o tipo de sistema, colectivo ou endereçável.

Em um sistema colectivo, obrigatoriamente todos os detectores automáticos estão ligados à central de extinção. Esta deverá ter capacidade no mínimo para duas linhas ou zonas, em *stub* (antena), devido à necessidade da dupla confirmação, ou seja, indicação de alarme em zonas distintas. Neste tipo de sistema todos os comandos são realizados na central de extinção, sendo que a indicação de alarme ou avarias do

sistema só poderá ser observada na mesma ou em painéis repetidores devidamente providenciados. A Figura abaixo, mostra um exemplo de um esquemático de detecção de incêndio colectivo nas zonas de extinção.

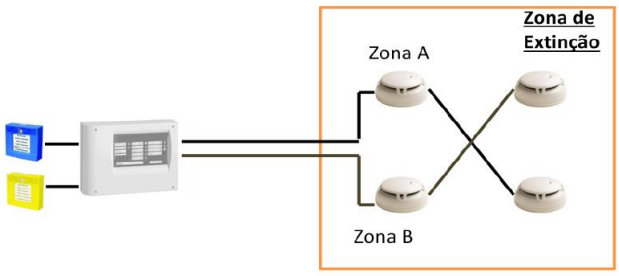

Figura 15 - Esquemático de zona de extinção com elementos coletivos

No entanto, com o desenvolvimento da tecnologia é possível que todos os elementos sejam endereçáveis, excepto os botões de activação e bloqueio. Com um sistema endereçável é possível indicar qual o elemento da linha que activou o alarme e a atribuição de um texto a este elemento ou zona de detecção em que o evento ocorreu. Este sistema torna-se mais versátil já que não existe a necessidade da ligação dos detectores à central de extinção e o controlo do sistema pode ser efectuado na central de detecção de incêndio ou na central de extinção. A confirmação por parte de dois detectores de zonas distintas também é obrigatória, mas por ser um sistema endereçável todo este processo é efectuado através de programação. A Figura abaixo mostra um exemplo de um esquemático de uma zona de extinção com elementos endereçáveis.

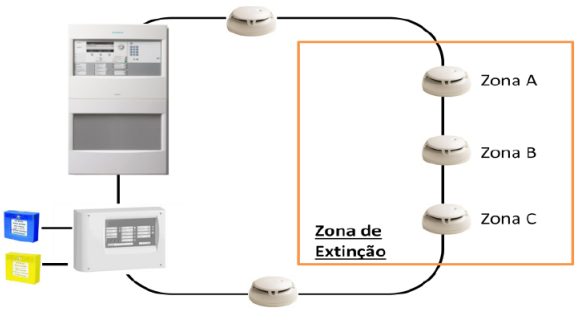

Figura 16 - Esquemático de zona de extinção com elementos endereçáveis

Os painéis óptico-acústicos são activados depois da dupla confirmação de alarme de incêndio na zona a proteger e são instalados nos locais de acesso às zonas de extinção. A Figura abaixo, mostra um exemplo de um painel óptico-acústico.

Relativamente aos contactos magnéticos das portas, estes não devem ser inibidores do processo de extinção, sendo que a sua utilização dependerá dos critérios do projectista. Já que a sua utilização dos contactos de porta não é obrigatória devem-se ter certos cuidados aquando do processo de extinção. Caso as portas de acesso não estejam encerradas todo o processo de extinção perderá efeito, por isso as portas de acesso devem possuir molas de fecho automático para que estejam sempre encerradas e caso exista um incêndio o agente extintor produza o efeito pretendido.
No processo de extinção com agentes gasosos um comando muito importante realizado pela central de extinção é o controlo sobre a ventilação, já que grande parte do sucesso da extinção deve-se à estanquidade da sala e para isso é necessário existir um controlo sobre os equipamentos de ventilação e os meios de alimentação da sala.

A Figura abaixo, mostra um exemplo de aplicação de um SAEI num *Data Center*, em que é possível observar todos os componentes mencionados anteriormente.

Figura 17 - Extinção de incêndio em *Data Center*

Legenda

1. Detectores de fumo por aspiração
2. Detectores de fumo/termos pontuais
3. Central de Extinção
4. Cilindro de agente extintor
5. Alarmes Sonoros
6. Botão manual de activação de extinção
7. Difusor
8. Painel óptico de aviso

AGENTES EXTINTORES

Como já mencionado os agentes extintores gasosos são os meios de extinção mais utilizados para a extinção em *Data Centers*, pois permitem uma rápida extinção, sem resíduos e por conseguinte sem necessidade de limpeza. Garantem ainda que depois do processo de extinção os equipamentos que não foram danificados pelo fogo continuam em funcionamento, minimizando assim os prejuízos.

A Tabela abaixo, compara as características dos gases inertes com os gases químicos.

Gases Inertes	Gases Químicos
São armazenados a altas pressões;	Armazenado em líquido;
Requerem tubagem e cilindros de alta pressão;	Cilindros e tubagem standard;
Requerem um maior número de cilindros, logo uma maior área de armazenamentos;	Requerem um número reduzido de cilindros, logo, uma área de armazenamento menor;
Custo reduzido do gás;	Custo elevado do gás;

Tabela 5 - Comparação entre gases inertes e gases químicos

No caso dos gases inertes, que são armazenados a elevadas a grandes pressões o desenvolvimento de válvulas que permitem uma descarga de gás constante e a pressões mais baixas do que aquelas a que o gás é armazenado, permitem uma redução do diâmetro das tubagens e reduzem também os picos de pressão existentes na libertação do agente extintor.

As Figuras abaixo mostram exemplos de uma válvula redutora de pressão e a montagem de um sistema de extinção por gases inertes.

Figura 18 - Válvula redutora de pressão – B0480

Figura 19 - Montagem de um sistema de extinção

Estudos efectuados comprovam também que as utilizações de agentes extintores gasosos utilizados na extinção em *Data Centers* podem interferir no funcionamento dos discos duros e em alguns casos danifica-los. Estas falhas podem ser causadas pelo elevado ruído emitido pela libertação do gás no processo de extinção.

A utilização de difusores, como o *Silent Nozzle* com válvulas de libertação de gás a pressão constante, permite uma redução do pico de libertação do agente extintor e reduzem o nível de ruído durante o processo de extinção, para um nível que seja adequado para estas instalações.

Este tipo de sistemas e avanço da tecnologia oferecem inúmeras soluções e vantagens na protecção de incêndio em *Data Centers*. A escolha do projectista relativamente aos sistemas de segurança contra incêndio passará pelos sistemas analisados neste capítulo que apesar do seu elevado custo de aquisição e instalação é inteiramente justificado pelo ainda maior custo de paragem ou substituição dos equipamentos danificados em caso de incêndio.

10. Climatização

Data Centers são infra-estruturas complexas e compostas por diversos componentes que, quando equalizados correctamente, permitem o processamento e armazenamento de informações cruciais para a continuidade dos negócios de empresas. Nessa composição, a climatização é um sistema crítico pois é o segundo sistema que mais consome energia do conjunto e, ao mesmo tempo, o responsável por manter o ambiente interno favorável à operação dos equipamentos que compõe o *Data Center*, como servidores, *storages*, *switches*, entre outros.

Para ilustrar a representatividade desse sistema, a climatização representa entre 40 e 50% do custo de energia eléctrica de um *Data Center*, perdendo apenas para o consumo de energia demandado pelos servidores.

O sistema de ar condicionado dedicado para *Data Center* tem três funções principais:

Controlo da temperatura: os servidores e demais equipamentos do *Data Center* aquecem muito durante seu funcionamento, correndo o risco de se auto desligarem ou queimarem, o que pode causar uma parada não programada no *Data Center* e a interrupção dos serviços. Essa dissipação de energia em forma de calor poderia levar a temperatura de um *Data Center* a ultrapassar facilmente os 50ºC, enquanto a temperatura ideal para funcionamento é ao redor de 25ºC. Assim, para manter essa temperatura mais baixa e estável, utiliza-se máquinas específicas de ar condicionado.

Controlo da qualidade do ar: para garantir a qualidade de pureza do ar no interior do *Data Center*, é importante que esteja livre das partículas solidas e contaminantes presentes no ar. A presença de poeira ou qualquer partícula pode prejudicar o funcionamento do sistema e causar uma parada. A limpeza do ar ocorre por meio de um sistema de filtragem presente nas unidades de ar condicionado.

Controlo da humidade: os equipamentos electrónicos são muito sensíveis. A baixa humidade do ar pode gerar carga electrostática que queima os componentes electrónicos dos servidores. Já a alta humidade pode causar a condensação de água dentro dos servidores. Além disso, as bactérias se proliferam nos dois extremos, então a humidade relativa precisa manter-se em torno de 50%.

Como os equipamentos de climatização são os que consomem mais energia dentro do *Data Center* além dos servidores, cuidados especiais devem ser tomados durante o projecto para aumentar a eficiência do sistema de refrigeração e consequente diminuição dos gastos com energia eléctrica. Existem várias técnicas de refrigeração que devem ser adoptadas durante o projecto de qualquer *Data Center* e recomendadas para promover eficiência energética. Dentre elas, destaca-se a colocação do ar condicionado o mais próximo possível dos servidores para evitar o gasto de energia com a movimentação do ar, o *free cooling,* que utiliza o ar externo para refrigerar internamente, optimizando o consumo de energia eléctrica, utilização de sistema com água gelada (*Chillers*), confinamento dos corredores quente ou frio, entre outros.

Por toda sua representatividade no funcionamento de um *Data Center*, o controlo climático também deve ser um importante ponto de atenção. Para que seja efectivo, são dispostos sensores em diferentes locais dentro do *Data Center* que são interligados em rede aos microprocessadores dos equipamentos obtendo-se um controlo mais preciso e eficiente.

O sistema de climatização de um *Data Center* é algo pouco notado quando funciona correctamente. Porém, como vimos, quando se torna ineficiente pode gerar inúmeros problemas, dentre eles o mais trágico: a interrupção do serviço. Com um projecto criterioso e bem elaborado que leva em consideração essas e outras variáveis mais técnicas é possível garantir uma atmosfera interna propícia para o funcionamento de todos os equipamentos e, consequentemente, a operação continua do *Data Center*.

11. Energia

A energia que chega da rede elétrica até os *Data Centers* é tratada para se tornar mais adequada para o consumo dos servidores. Como eles precisam estar sempre ligados, é essencial que haja uma fonte constante de energia alimentando-os.

Por isso, os *Data Centers* possuem redes redundantes de energia: se uma delas falhar, eles conseguem imediatamente trocar para outra. Uma rede de geradores e *no-breaks* também é parte da infra-estrutura elétrica dos *Data Centers*.

Dependendo de seu uso, os servidores podem consumir de 3 *kilowatts* (três mil *watts*) de energia por *rack* nos *Data Centers* menores até 12 a 15 *kilowatts* por *rack* nos maiores. Considerando que grandes Centros de Dados podem chegar a ter 600 *racks* de servidores, o consumo total de energia deles poderia chegar a 9 megawatts (9 milhões de *watts*).

Um computador doméstico, em comparação, consome cerca de 200 *watts* apenas, e considera-se que uma usina hidrelétrica que produza 19 *megawatts* de energia consegue abastecer uma cidade de 150 mil habitantes.

Esse é o principal motivo pelo qual *Data Centers* s grandes costumam ficar mais distantes dos grandes centros urbanos. Como eles consomem muita energia, é mais viável para as empresas posicioná-los em cidades menores ou em regiões periféricas, onde o custo da energia elétrica é menor. Isso à parte, é perfeitamente possível posicionar um centro de dados de grande porte no meio de uma cidade - embora seja consideravelmente mais caro em termos de energia.

12. Refrigeração

Os Servidores, porém, não são a única coisa que consome energia em um *Data Centers*. Enquanto funcionam, eles geram calor, e se não forem refrigerados eles podem levar a sala de servidores a temperaturas de mais de 50ºC, o que faz com que eles se desliguem automaticamente para prevenir danos ou incêndios.

Para evitar que isso aconteça, os *Data Centers* possuem sistemas redundantes de refrigeração de ar também. Diversos equipamentos de ar condicionado são responsáveis por reduzir a temperatura dos centros de dados a cerca de 24ºC a 25ºC. Isso, no entanto, demanda energia.

Segundo Robin (2011), a refrigeração consome um total de 40% a 50% da energia consumida pelos *racks*. Em outras palavras, se os *racks* de um *Data Centers* grande consomem 9 *megawatts* de energia, serão necessários outros 3,6 a 4,5 *megawatts* para a sua refrigeração.

É fácil perceber que se trata de um acréscimo considerável à conta de energia, e por esse motivo algumas empresas optam por instalar seus *Data Centers* em regiões mais frias. Nos países nórdicos como Noruega, Finlândia e Islândia, é possível utilizar um método de refrigeração chamado de "*free cooling*".

Em vez de usar equipamentos de ar condicionado para esfriar o ambiente, esse método canaliza o ar do ambiente (que já é frio) para dentro da sala dos servidores. Embora economize na conta, ele também pode trazer desvantagens: ar muito sujo pode contaminar os computadores com a poluição de áreas urbanas próximas, reduzindo a sua vida útil.

Uma possibilidade estudada por empresas para reduzir os custos com refrigeração é instalar os servidores no fundo do mar. A Microsoft, por exemplo, já vem testando essa possibilidade, embora ainda enfrente uma série de desafios.

13. Telecomunicações

É necessário, no entanto, que os computadores do *Data Centers* consigam se comunicar com o resto da internet para realizar seu trabalho. Isso significa ter uma rede robusta de telecomunicações para que os dados possam entrar e sair de lá.

Assim como a rede elétrica, a rede de telecomunicações dos *Data Centers* é redundante, e muitas vezes vem de mais de uma operadora diferente. Isso permite que o centro de dados continue a funcionar mesmo que uma das operadoras falhe. As redes chegam até o *Data Centers* e saem dele na forma de grossos cabos de fibra óptica que incluem diversas fibras.

Ao chegar no *Data Centers*, no entanto, a rede não vai diretamente para os servidores. Ela passa antes por uma sala de telecomunicações que possui roteadores e equipamentos que são responsáveis por distribuir as fibras entre os *racks*. Ela funciona como uma espécie de central dos correios, que recebe os pacotes e cartas e repassa-os para centrais menores que, por sua vez, entregam-nos ao destinatário final.

Em vez de pacotes de correio, no entanto, as salas entregam conexões. Quando você acede o seu e-mail, por exemplo, a informação sai do seu computador, trafega por diversas redes até um *Data Centers* e passa pela central de telecomunicações de lá, que determina para qual *rack* você deve ser direcionado para poder entrar em sua caixa de mensagens de maneira extremamente rápida.

A fibra óptica ainda é a tecnologia mais avançada de transmissão de dados que conhecemos. No entanto, as fibras vêm evoluindo de forma a permitir um trânsito mais rápido de informações. A maneira como a luz viaja dentro das fibras - e as cores de luz utilizadas - permitem que mais dados sejam transmitidos por meio delas. Mamede afirma, porém, que o volume de dados movimentados pelos grandes *Data Centers* quase nunca é revelado, pois trata-se de uma informação confidencial.

14. Segurança

Independente de seu uso, os *Data Centers* quase sempre armazenam dados confidenciais. Sejam eles os dados de empresas, sejam os de usuários de serviços na nuvem, o acesso a esses dados precisa ser rigorosamente controlado. E isso se reflete na própria arquitetura dos centros de dados.

Empresas com centros de dados de maior porte raramente revelam o endereço de seu *Data Centers*. No máximo, elas informam a cidade ou região na qual ele se localiza, para dificultar que pessoas mal-intencionadas tenham acesso ao edifício. A entrada nos *Data Centers* também costuma ser controlada por esse mesmo motivo

Segundo Mamede (2006), o acesso à sala dos servidores de um *Data Centers* é ainda mais restrito. Podem haver cinco ou mais pontos de controlo de acesso entre a entrada do centro de dados e a sala nas quais os computadores ficam. As entradas podem ser controladas por equipamentos como crachás, fechaduras, senhas e mesmo identificações biométricas, e a região geralmente tem monitoramento interno de circuito de câmaras.

https://zeittec.com.br/data-center-tier-3/

Fontes:

- Mamede, Henrique São (2006). Segurança Informática nas Organizações. FCA-Editora Informática.
- Robin, M. (2011) *Fire Protection for IT and Telecommunications Facilities*. Blatimore,