

RESUMO

A segurança física dos Centros de Informática, apesar de constituir uma questão de vital importância para o seu funcionamento normal, é regra geral subalternizada, se não mesmo marginalizada, pela maioria dos responsáveis dos Centros.

Esta comunicação destina-se a chamar a atenção dos informáticos em geral, e dos gestores dos Centros em particular, para a delicadeza dos problemas ligados à instalação de Centros.

Nela serão abordados os seguintes temas:

- Análise das necessidades dos equipamentos informáticos de médio/grande porte

- Organização do Centro de Informática

- Planeamento e implementação do projecto de instalação

- Papel do especialista em segurança informática

1. INTRODUÇÃO

A crescente informatização das várias áreas da actividade do país vem criando problemas novos, que não existiam com a utilização dos métodos manuais ou mecanográficos de tratamento da informação.

Efectivamente, as crescentes e espectaculares possibilidades técnicas com que a informática nos vem apresentando são acompanhadas por um aumento de certo tipo de problemas:

- Custo elevado dos equipamentos e software (sobretudo este ultimo)

- Concentração de informações vitais (ficheiros volumosos ou bases de dados)

- Aspecto abstracto das informações gravadas em suporte magnético

Resulta daqui que os problemas de segurança tem que ser encarados com realismo, tornando-se indispensável uma reflexão profunda sobre o valor a informação tratada em termos empresariais e sociais.

São as conclusões dessa reflexão que irão possibilitar a tomada de decisões correctas quanto as medidas de segurança necessárias.

É bom lembrar que o critério que deve imperar na adopção de medidas de segurança (como aliás em tudo) é o bom senso. Por vezes adoptam-se medidas sofisticadas, quando afinal o problema poderia ser resolvido de forma mais simples ... e eficaz.

Constituindo as medidas de segurança um interface entre os riscos e o Centro propriamente dito, e sendo de experiência que esse interface não resulta a 100%, torna-se necessário examinar todas as situações possíveis de acontecer, por forma a evitar os "calcanhares de Aquiles".

2 – EXIGÊNCIAS DOS EQUIPAMENTOS

Os equipamentos de médio/grande porte apresentam exigências bastante restritivas no tocante a dois pontos:

- Climatização

- Alimentação eléctrica.

Vamos dissecar um pouco cada um destes pontos, embora em termos pouco profundos.

2.1.Climatização

O conjunto sala de exploração e arquivo de suportes magnéticos, é o que requer cuidados especiais na qualidade da climatização.

Para satisfazer as exigências dos equipamentos, expressas no quadro 1, há que conjugar uma serie de projectos:

- Chão e tecto falsos

- Equipamento de condicionamento e controlo da qualidade do ar

- Revestimento das paredes, chão e tecto primários

O dimensionamento do equipamento de climatização deve ser feito em função das cargas a suportar, devendo merecer um cuidado especial, pois a manutenção da temperatura, humidade e taxa de poeiras e gases dentro de certos limites vai possibilitar:

- A estabilidade das condições de funcionamento do equipamento informático

- A estabilidade das formas dos suportes e manutenção das suas prioridades físicas

- Eliminação da electricidade estática

- Diminuição das poeiras em suspensão, pela supressão das fibras secas e quebradiças, as quais, ao contrário das fibras humedecidas, tem mais tendência a propagar-se que a depositar-se

- Filtragem das poeiras e gases nocivos aos equipamentos e aos suportes magnéticos

- Saúde e conforto do pessoal

QUADRO 1 -Exigências dos equipamentos e suportes no tocante a temperatura e humidade

Por outro lado, a escolha e colocação do chão e tecto falsos, além dos acabamentos do chão, paredes e tecto primários devem ser criteriosamente estudados. Assim:

- Os materiais constitutivos devem ser desagregáveis

- As superfícies das paredes, chão e tecto devem ser perfeitamente lisas para evitar a acumulação de poeiras

- O chão e tecto primários devem ser pintados com duas camadas de tinta anti-poeira (a base de oxido de oxano) antes da instalação do chão e tecto falsos.

A escolha do tipo de sistema de climatização deve merecer estudo profundo.

Existem no mercado dois diferentes tipos de sistemas:

- Um clássico, consistindo numa central condicionadora única alimentando um circuito de frio, e em que a difusão do ar se faz através de condutas ou por intermédio de um "plenum" de ar sob o chão falso

- Um relativamente recente, em que as características do ar são controladas, não por uma central única, mas através de varias pequenas centrais autónoma criteriosamente dispostas dentro da própria sala.

O sistema clássico, utilizado desde há muito no condicionamento de unidades industriais e em grandes edifícios administrativos, apresenta fortes inconvenientes quando utilizado no condicionamento de salas de computadores:

- É um sistema caro e difícil de manter. A necessidade de recuso a um duplo sistema de compressores como medida de segurança, torna ainda mais embaraçosa e cara a sua utilização

-A utilização de condutas de difusão do ar, que são fatalmente longas pela própria necessidade de colocação do equipamento condicionador longe da sala do computador, torna muito rígido o próprio sistema, quando há necessidade de efectuar alterações na configuração informática, além de que se torna muito sujeito a avarias.

2.2. Energia eléctrica

A utilização de médios ou grandes equipamentos informáticos, exige um cuidado muito especial no Projecto e implantação do sistema de alimentação eléctrica.

Se os pequenos equipamentos não são muito sensíveis a pequenas variações na intensidade da corrente, os médios/grandes sistemas já acarretam exigências muito acentuadas na qualidade e estabilidade da energia eléctrica, não tolerando interrupções ou desvios para além de certos limites bastante estreitos

Essas exigências são especificadas no quadro 2.

QUADRO 2 - Exigências dos equipamentos informáticos em matéria de energia eléctrica

Vamos debruçar-nos um pouco sobre a escolha do tipo de alimentação eléctrica a escolher.

Há duas situações diferentes a analisar o Centro vai ser instalado num edifício já existente, possuidor portanto de uma rede de alimentação já instalada ou o centro vai para um edifício a construir de raiz.

No 1º caso há que se efectuar as alterações necessárias por forma a garantir as especificações expressas quando 2. No segundo caso, o projecto da alimentação eléctrica fará parte do projecto global do edifício, o que permitirá um melhor ajustamento às condições requeridas pelos equipamentos informáticos.

A instalação de um transformador independente e absolutamente aconselhável, pois a rede publica não apresenta a qualidade desejável para fins informáticos.

Os equipamentos informáticos são muito susceptíveis a um certo numero de fenómenos bastante frequentes nas redes publicas (é bom não esquecer que a rede pública não foi projectada para alimentar equipamentos informáticos):

- Microcortes

- Flutuações de tensão por períodos de 0,1 s ("flicker").

- Desequilíbrios na rede, traduzidos por tensões diferentes entre fases.

- Sinais parasitas

- variações de frequência (pouco frequentes)

A instalação de um conjunto de baterias tampão e de um grupo conversor obvia, de forma definitiva, os problemas que ainda possam subsistir apesar da existência de um transformador de alta tensão.

A instalação de terra para o computador deve merecer igualmente um cuidado especial, devendo para o efeito ser efectuado um estudo do terreno circundante para examinar as "terras" já existentes (a terra do computador deve estar afastada de qualquer outra terra, no mínimo de 15 metros, para evitar induções)

2.3. Riscos de origem accidental

2.3.1 Fogo

O sistema de detecção de incêndios bem como o agente extintor a utilizar devem ser criteriosamente escolhidos

No tocante a agentes extintores, o quadro 3 indica as características dos vários tipos existentes no mercado.

De salientar que quer a água, quer o Halon são de excluir na sala do computador, pois os seus efeitos são altamente perniciosos para os equipamentos (caso da água e o halon) e para as pessoas (o halon, em determinadas condições, dá origem a um gás letal)

O sistema de detecção e combate a incêndios não deve ser automático, pois podem -se criar situações muito perigosas.

O ideal é um sistema semi-automático, que só seja activado cerca de 1 minuto após ter sido accionado o sistema de detecção. Desta forma, o pessoal do Centro tem hipóteses de controlar a extinção do incêndio e, o que é muito importante, evitam-se situações de pânico, mesmo em caso de falso alarme.

2.3.2. Deficiências de climatização

Antes de se dimensionar um equipamento para climatizar um Centro de Informática, é necessária efectivação de uma série de estudos:

-Cargas a suportar (dissipação por efeito Joule no material e na iluminação, dissipação através das paredes e janelas, irradiação de calor pelas pessoas, etc.)

-Carta Psicrométrica (estudo de comportamento das misturas de ar e vapor de água)

QUADRO 3 - Agentes extintores. Características

-Análise dos gases e poeiras poluentes existentes nas imediações do edifício.

A falta de um destes estudos pode ocasionar problemas no funcionamento futuro do sistema de climatização.

Para além de se prever uma tolerância razoável (40%) no cálculo de carga calorífica por forma a que o equipamento de ar condicionado não funcione nos "limites", há que prever igualmente uma reserva de potência frigorífica para o caso de uma avaria do equipamento.

Essa reserva deve ser prevista através do recurso a um sistema duplo de refrigeração, em que um funcione como "back-up" do outro.

Os filtros do sistema devem ser igualmente objecto de um estudo cuidadoso, para se determinar a taxa de eficácia a que eles devem obedecer.

São de excluir os filtros de óleo por constituírem eles próprios um factor de poluição. Os mais eficazes são os electrostáticos embora necessitem ser precedidos por um filtro mecânico para obviar a passagem de partículas que danifiquem os fios iónicos

O sub-sistema de filtragem deve ser composto por dois tipos de filtros, um para partículas grosseiras (até 1 micron) e outro para partículas sub-micron.

O problema das poeiras e gases poluentes torna-se particularmente agudo para os suportes magnéticos, podendo originarem-se erros de leitura/escrita ou mesmo destruição de porções magnetizadas.

2.3.3. Deficiências na alimentação eléctrica

No ponto 2.2. já foram focadas as necessidades dos equipamentos informáticos no respeitante a esta matéria.

A não satisfação dessas especificações pode ocasionar graves problemas: perda da informação em memória, abortagem de programas, perda da informação em disco, etc.

A forma de obviar a esses problemas consiste em prever um sistema de alimentação de recurso composto por um conjunto de baterias tampão, um rectificador e um ondulator para a correcção das pequenas variações na fonte de alimentação.

Para as falhas de energia superiores a 10 minutos o recurso a um grupo electrogéneo é uma boa solução.

2.3.4. Catástrofes naturais

Os sismos as inundações e as tempestades eléctricas constituem os acidentes naturais que podem afectar mais profundamente um Centro de Informática.

Os seus efeitos podem ser anulados ou diminuídos através de uma serie de medidas preventivas:

Edifício com estrutura anti-sismica

-Pára-raios eficazes colocados no telhado do edificio

-Localização do Centro num r/c elevado. Em particular, a sala de exploração deve estar numa sala interior isolada do resto do edificio.

-- Isolar o edificio com uma gaiola de Faraday no caso da região onde se encontra o Centro ser muito afectada por tempestades eléctricas.

2.3.5 Campos magnéticos e electromagnéticos

Os campos magnéticos gerados por ímans permanentes afectam a informação registada em suporte magnético.

Para obviar os acidentes com este tipo de campos é necessário tomar medidas muito restritivas no acesso a sala de exploração e ao arquivo de suportes magnético.

Para além disso, é indispensável instruir o pessoal que trabalha na sala de exploração, ou que a ela tem acesso, no sentido de não colocar objectos metálicos sobre os "diskpac" (tesouras ou canivetes, por ex.) nem os badges magnéticos utilizados em muitos dispositivos de controlo de acessos.

Efectivamente, estes objectos aparentemente inofensivos podem provocar a desmagnetização de pequeníssimas porções dos suportes magnéticos.

No tocante a radiações electromagnéticas há que ter especial atenção as emissões de radar, pois podem introduzir sinais parasitas nos circuitos do computador ou afectar a informação gravada nos suportes magnéticos.

Estas radiações podem ser obviadas pela colocação, nas janelas do edificio, de grades de alumínio, as quais funcionarão como reflector das radiações. Se esta medida não resultar, uma gaiola de Faraday a isolar o edificio resolverá o problema.

No entanto, a melhor solução ainda é a colocação do Centro longe dessas fontes de "poluição" electromagnética.

2.4.1. Vandalismo

-O vandalismo pode causar sérios danos num Centro de informática, porquanto é intencional.

2.4. Riscos de origem voluntária

o vandalismo pode assumir varias formas: desde a destruição de ficheiros e programas, até a sabotagem

do ar condicionado (através das tomadas de ar exteriores)

Neste domínio há que tomar uma serie de medidas preventivas:

- limitação rigorosa dos acessos à sala de exploração
- Controlo sobre as aplicações que correm no Centro (auditoria interna sistemática)
- Controlo rigoroso das entradas no Centro de Informática
- Colocação das tomadas de ar em local não acessível do exterior
- Sala de exploração não acessível do exterior.

3 - PLANEAMENTO E IMPLEMENTAÇÃO DO PROJECTO DE INSTALAÇÕES

3.1.necessidades em segurança

Grande parte dos problemas surgidos com a instalação física de Centros advém de uma deficiente definição das necessidades e da inexistência do planeamento e controlo da implementação dessas mesmas instalações

Os gestores dos Centros e os Informáticos sabem que a partir de determinados níveis de configuração informática, os equipamentos necessitam de instalações especialmente preparadas.

Para além das especificações das necessidades dos equipamentos em climatização, energia eléctrica e espaço que os construtores indicam, os responsáveis dos Centros pouco mais informação possuem sobre as especificações a exigir aos empreiteiros que irão executar os diferentes trabalhos de preparação do Centro.

Há necessidade de ter ideias claras sobre os problemas levantados pela instalação física de um Centro, quer no tocante às necessidades dos equipamentos e pessoal quer no que diz respeito ao planeamento e controlo da implementação dessas mesmas instalações.

É evidente que os gestores e os informáticos em geral não têm obrigação de dominar esta matéria, pois ela envolve o domínio de um numero relativamente grande e diversificado de conceitos.

A solução é pois recorrer a um especialista para colaborar com os gestores e informáticos na definição das necessidades, na elaboração dos cadernos de encargos, na selecção das melhores propostas, no planeamento da execução da instalação física e no controlo da execução dos trabalhos.

3.2.Planeamento do projecto das instalações. Rede Pert

A ausência de planeamento conduz sempre, qualquer que seja o sector de actividade, a situações de impasse e de incongruência cuja resolução custa bastante tempo e dinheiro.

A instalação de um Centro de Informática deve igualmente ser objecto de um cuidadoso planeamento.

A colaboração de um especialista em segurança física de Centros de Informática é indispensável para a coordenação das várias fases do projecto.

No entanto, o papel dos gestores e dos informáticos é vital. Serão eles quem definirá o grau de importância que a informática tem na vida da empresa ou organismo.

As medidas de segurança física a implementar vão ser função da exigências de "inexpugnabilidade" que

os responsáveis da empresa ou organismo definirem.

No tocante à execução do projecto de instalações, o recurso a uma rede Pert é de uma importância primordial, pois ela permitirá o acompanhamento das diversas actividades, desde os estudos iniciais até aos trabalhos de execução.

A rede Pert que no final se apresenta representa um projecto típico: um organismo (ou empresa) que a informatiza e, enquanto decorre a construção das futuras instalações, tem que efectuar a adaptação de instalações provisórias para o Centro de Informática.

Esta adaptação é pertinente, pois que o tempo que decorre entre o projecto de instalações e a entrega da obra não é inferior, regra geral, a cinco anos.

As actividades encontram-se detalhadas no quadro que antecede a figura da rede propriamente dita. Nesta, o projecto de adaptação das instalações provisórias encontra-se a tracejado para maior realce.

Finalmente, no quadro 4 encontram-se detalhadas as várias fases em que o especialista em segurança de Centros de Informática deve intervir.

4 - CONSIDERAÇÕES FINAIS

A segurança deve constituir um motivo de preocupação imperiosa e imediata, para qualquer organismo ou empresa que recorra a meios automáticos para o tratamento da informação.

Queria deixar, como corolário de tudo o que foi dito um conjunto de normas essenciais:

- A Direcção deve definir muito claramente o que deve ser protegido e contra que riscos deve o Sistema informático ser seguro

- Com base nessa definição, e antes mesmo da instalação do Centro de Informática, devem ser examinados todos os pontos críticos do sistema. Com base nessa análise, deve ser elaborado um plano de Segurança, sensato e eficaz.

- Um plano de segurança, não é conseguido por acaso. É necessária uma definição clara dos objectivos, seguida de uma planificação detalhada e, evidentemente, de um estudo económico que determine, para o caso concreto, a razão ideal entre o custo do sistema de segurança e o custo dos riscos potenciais que ele pretende eliminar, ou reduzir.

- Se para certo tipo de riscos, a probabilidade do seu aparecimento se torna facilmente estimável (por ex. incêndio ou corte de corrente) para outros pode tornar-se bastante difícil (por ex. fraude ou sabotagem). Torna-se, no entanto, importante quantificar essas probabilidades em termos de perdas monetárias, por forma a possibilitar a avaliação, a comparação e a afectação de prioridades mas medidas de segurança a implementar.

- O plano de Segurança deve contemplar o pessoal que trabalha no Centro, pois ele desempenha um papel extremamente importante na manutenção da segurança. É necessário motivá-lo e treiná-lo, por forma a dotá-lo de uma capacidade efectiva de avaliação de situações difíceis, e de uma reacção imediata, controlada e metódica.

- É necessário ter consciência de que, mesmo utilizando medidas de segurança e técnicas de controlo aperfeiçoadas não se conseguem reduzir os riscos para além de um certo limite.

- O risco residual deve ser transferido para uma companhia de Seguros.

- O plano de segurança deve ter em linha de conta os fenómenos imprevisíveis, por forma a reduzir-se ao mínimo a desarticulação das operações em caso de acidente

- As tarefas a realizar, em caso de acidente, devem estar claramente definidas, terem uma ordem de execução e serem muito treinadas.

- Após a elaboração do plano de segurança, a direcção do Centro de Informática deve pôr em acção um

mecanismo de auditoria interna que verifique o cumprimento e a eficácia do plano no dia-a-dia, e que promova a sua constante adaptação.

- O plano de segurança deve ser dinâmico, acompanhando a evolução do Centro e das técnicas de segurança.