UNIVERSIDADE ESTÁCIO DE SÁ
Especialização em Informática
Coordenação de Pós Graduação

Segurança Física de Redes de Computadores

Por
Eng. Leonardo Henrique Lima de Souza

Rio de Janeiro
Outubro de 2004

UNIVERSIDADE ESTÁCIO DE SÁ
Especialização em Informática
Coordenação de Pós Graduação

Segurança Física de Redes de Computadores

Por
Leonardo Henrique Lima de Souza
Engenheiro Eletricista - UERJ

Monografia entregue à Universidade Estácio de Sá, como requisito final para a obtenção do título de Especialista em Informática.

Rio de Janeiro
Outubro de 2004

Agradecimentos

A Kelly, que sempre me dá forças e encorajamento nos momentos difíceis.

Ao professor João Mendes, que atendeu a todas as minhas solicitações quando tive dúvidas.

A Deus, na certeza de que nossas conquistas são graças concedidas.

Sumário

Pág.

Resumo

Este trabalho objetivou introduzir aos profissionais da área de tecnologia da informação e áreas afins um estudo sobre os componentes pertinentes relacionados à segurança física de rede de computadores e seus centros de processamento de informação. O texto se divide em quatro capítulos, aos quais abordamos: a segurança da rede, segurança dos meios de armazenamento, plano de contingência e sala cofre. O seu conteúdo detalha aspectos construtivos da implantação de um centro de processamento de dados, as premissas que se deve ter, procedimentos de segurança, equipamentos de automação predial que devem fazer parte do escopo da construção e outros detalhes para a garantia da segurança física. O referencial teórico se baseou em livros, normas técnicas brasileiras e artigos de profissionais de segurança. Para o desenvolvimento de um plano de contingência de recursos de informática, o trabalho mostra um modelo e cita como deve se atribuir os diferentes tipos de responsabilidades da contingência dentro de uma empresa. O conceito de sala-cofre é discutido no último capítulo onde apresenta vários detalhes desse equipamento, seus benefícios e sobre a decisão de adotar essa tecnologia. A conclusão final apresentada é compatível com a idéia inicial de se obter conhecimento técnico sobre o assunto e deixa entender que é preciso estar sempre se atualizando para manter um bom nível de segurança.

Palavras chave: Segurança física. Plano de contingência. Centro de processamento de dados. Política de segurança.

Abstract

The aim of this work was introduce to the professionals of information technology area and similar areas, a study about the components related to physical security of computers network and its centers of information processing. The text has four chapters, to which approaches: the security of the network, security of the storage medias, plan of contingency and room-safe. Its content details constructive aspects about the implantation of a data processing center, the premises that must have, procedures of security, equipment of building automation that must be part of the purpose the construction, and other details for certify the physical security. The theoretical reference was based on books, brazilian technical norms and articles from security professionals. For develop a plan of contingency for computers resources, the text presents a sample and cites how the responsibilities must be shared inside a company. The room-safe concept is argued in the last chapter, where it presents some details of this equipment, its benefits and the decision to use this technology. The presented end conclusion is compatible with the initial idea of getting technician knowledge on the subject, and leaves to understand that is necessary to be always bringing up to date to keep a good level of security.

Keywords: Physical security. Plan of contingency. Data processing center. Security policy.

Introdução

A informação nos dias atuais é sem dúvida um dos ativos de maior importância no universo das organizações, conseqüentemente as medidas e regras para implementação de sua segurança têm sido intensivamente praticadas, tanto no que diz respeito à segurança lógica: implementada através de software, quanto à segurança física: relacionada a uma série de recursos, oriundos de outros campos da tecnologia, como por exemplo a automação predial e os sistemas de combate a incêndio, que se associam a informática para lhe garantir maior suporte.

Neste contexto enfocamos a segurança física das redes de computadores e dos Centros de Processamento de Dados (CPDs) que as servem, como um fator de vital importância para o desenvolvimento de qualquer empresa. Pois o sucesso de sua implantação, bem como a continuidade de seu funcionamento está diretamente ligada ao sucesso da organização.

A utilização das redes de computadores tem crescido de forma significativa nos últimos anos, criando uma relação direta de dependência entre as empresas e os recursos de informática. A conseqüência disso é o aumento da vulnerabilidade às ameaças de segurança. Somando-se a isto, vemos que muitos sistemas de informação não estão preparados para suportar tais ameaças, pois os fatores de segurança da informação não foram aplicados em sua totalidade a época de suas concepções

Sendo a segurança física um fator crucial para o bom funcionamento das redes, decidimos traçar um caminho no qual poderemos ampliar nossa visão em relação a esse assunto, e ao mesmo tempo contribuir para a rede de conhecimento dos profissionais da área, pois sabemos que muitos dos temas a serem abordados neste trabalho, não são comumente estudados no nível acadêmico nas faculdades ligadas a área de tecnologia da

informação. Com isso poderemos conhecer as aplicações dos sistemas de controle e estabelecer padrões de segurança física a altura das ameaças vigentes.

Temos portanto uma questão a responder: Como garantir segurança física eficaz para as redes de computadores e seus Centros de Processamento Dados?

Com ajuda das normas da Associação Brasileira de Normas Técnica (ABNT): NBR 17799 – "Tecnologia da Informação – Código de Prática para a gestão de segurança da informação" e NBR 11515 – "Critérios de segurança física relativos ao armazenamento de dados", em conjunto com as contribuições dos referenciais teóricos e práticos, pretendemos esclarecer os principais pontos relacionados a segurança física dos ambientes informatizados.

Para tanto, será necessário explorar os detalhes das instalações vislumbrando as medidas de controle que estão intimamente relacionadas, as quais podemos citar: o acesso e a monitoração do CPD, a segurança contra incêndio, o controle de temperatura e umidade, o aterramento e a alimentação elétrica. Sendo estes pontos marcantes para garantir (conforme afirma a norma NBR 17799):

1. a confidencialidade – acesso somente a pessoas autorizadas
2. a integridade – exatidão das informações
3. a disponibilidade – garantia de acesso sempre que necessário

Os desastres ocorridos recentemente com empresas de grande porte como Eletrobrás, Petrobrás e o Tribunal Regional do Trabalho no Rio de Janeiro, conforme temos notícia[1], além de causarem perdas materiais e paralisações nos sistemas, culminaram também em perda de dados, gastos elevados para as recuperações emergenciais, prejuízos a sociedade, imagem negativa para o público, aspectos jurídicos da paralisação e queda nas ações das companhias.

[1] Nos anexos A, B e C, estão as reportagens sobre a ocorrência de incêndios de acordo com a citação do texto.

Além disso, no que diz respeito aos serviços públicos prestados à população, seja na esfera federal, estadual ou municipal, a lei 4.150/62, em seu artigo 1º , determina que todos os órgãos públicos atendam as normas técnicas de segurança segundo a ABNT, conforme podemos comprovar no anexo D. Somando-se a isso, o novo Código Civil brasileiro impõe aos gestores da informação (Gerentes e Diretores) a solidariedade na reparação dos danos causados à sociedade e a terceiros, prejudicados em função de um ato ilícito[2], isto é, atribui diretamente a responsabilidade pela imperícia na gestão de segurança aos administradores dos sistemas de informação.

Em relação a localização do CPD,

> *O mais recomendável é a construção de um edifício exclusivo, localizado no centro de uma área exclusiva, acima do nível do solo, com as instalações sensíveis no centro do edifício e as áreas de apoio na periferia, seguindo o conceito das camadas concêntricas de segurança* (CARUSO & STEFFEN, 1999, p.210).

No entanto essa idealidade demanda recursos que estão além da capacidade da maioria das empresas, assim como, atinge um número relativamente pequeno de profissionais atuantes, por isso nosso estudo tenderá para a situação em que o CPD se localiza dentro da planta onde as empresas desenvolvem suas atividades, seja ela um prédio ou uma área comum, devendo ser a situação mais recomendável segundo CARUSO & STEFFEN objeto de um estudo mais profundo e mais amplo, o qual pretendemos desenvolver futuramente.

[2] Verificar o Anexo E

CAPÍTULO 1
Segurança Física dos Centros de Processamento de Dados (CPDs)

1.1 Breve histórico

A preocupação com a segurança física teve início dos anos 70, devido a atos de vandalismo praticados na Alemanha por estudantes que apontavam o processo de informatização das empresas como principal motivo de desemprego. Desde então a cultura da Segurança da Informação pelo mundo tem se tornado cada vez mais efetiva. No Brasil essa necessidade se consolidou nos anos 90, com a concepção das normas de segurança da informação editadas pela ABNT.

1.2 Considerações de projeto

O projeto e a implantação de um CPD devem contemplar uma série de características peculiares, ligadas à importância e a sensibilidade que lhe são atribuídas, com o objetivo de *"...prevenir perda, dano ou comprometimento dos ativos, e a interrupção das atividades do negócio"* (NBR ISSO/IEC 17799, 2001, p.15).

LOCALIZAÇÃO

Um centro de processamento de informações deve ser implantado em uma área livre de quaisquer fatores de risco. Dessa forma deve-se evitar sua proximidade com depósitos de materiais combustíveis, tubulações de água e esgoto ou outro tipo de líquido ou gás inflamável, antenas de telecomunicações e estações de energia elétrica. O local também deve estar acima do nível da rua para evitar inundações, ser livre de vibrações ou impactos, ser protegido de poluição atmosférica e ter acesso restrito.

ESTRUTURA FÍSICA

A estruturação física contempla os detalhes construtivos e arquitetônicos da instalação para se obter o nível adequado de segurança. Enumeramos abaixo os principais pontos a serem observados:

a) Piso, Teto e Paredes

O piso ideal a ser utilizado em uma instalação de CPD é do tipo piso elevado. Suas principais funções são: permitir a passagem de cabos de dados e alimentação elétrica, funcionar como "*plenum* de insuflamento" de ar-condicionado[3], permitir distribuição das várias linhas de comunicação, servir como meio para instalação de sistema de detecção e combate a incêndio e permitir fácil remanejamento das unidades, oferecendo maior flexibilidade na alteração do *layout*.

O piso elevado deve ter normalmente "*...de 0,2 m a 0,4 m de altura, e para o caso de equipamentos de grande porte, de 0,4 m a 0,6 m*" (CARUSO & STEFFEN, 1999, p.214). Essas características se estendem também aos aspectos construtivos do piso, que deve ser composto por placas removíveis e intercambiáveis com dimensões iguais. A estrutura metálica deve ser autoportante[4] reticulada e apoiada em suportes verticais ajustáveis. Devem ser previstas placas perfuradas ou grelhas para insuflamento do ar-condicionado, bem como o aterramento de toda a estrutura metálica do piso. As especificações de esforço devem estar de acordo com as cargas a serem colocadas em cima do piso, assim como ter previsão para expansões futuras. Materiais combustíveis devem ser evitados na sua composição.

[3] O nível do chão é utilizado para insuflamento do ar-condicionado, pois a tendência do ar frio é ficar abaixo do ar quente. Isso faz com que o ar frio insuflado percorra o ambiente até atingir o ponto retorno no teto da sala, tornando o sistema de refrigeração mais eficiente.

[4] "*Tem rigidez mecânica suficiente para sustentar-se com o apoio de uma só extremidade*". (FERREIRA, 1999, p. 236)

Tetos rebaixados devem ser evitados, dando-se preferência a instalações aparentes, no entanto, quando inaceitáveis, o teto deverá permitir: a passagem de cabos elétricos e de dados, instalação de grelhas para retorno do ar-condicionado e a instalação de sistema de detecção e combate a incêndio. A sua estrutura deve ser metálica e modular, sustentada por perfis metálicos e preparada para suportar o peso de luminárias, grelhas, sensores e outros acessórios. As placas devem ser removíveis e intercambiáveis, e feitas de materiais incombustíveis e não pulverizadores de partículas. O piso do andar superior ao da sala do CPD deve ser impermeabilizado, de forma evitar vazamentos.

As paredes devem ser de alvenaria ou concreto, e capazes de suportar impactos e furações caso a instalação necessite de algum acessório preso a elas. Deve também ser provida de uma porta corta fogo. Todo o conjunto deve garantir mínimo de 1 hora de resistência ao fogo a uma temperatura de até 1000^{o} C.

b) Iluminação e programação visual

Uma boa iluminação pode contribuir muito para a segurança e a produtividade de um CPD, portanto o projeto de iluminação do ambiente deve contemplar luminárias fluorescentes com índice de iluminamento não inferior a 500 lux medidos a 1 m do piso, utilizando uma central retificadora única e exclusiva para o sistema . Deve ser evitado o ofuscamento da visão, os pontos escuros (iluminação heterogênea) bem como o reflexo nas telas dos monitores de vídeo. O sistema de iluminação não deve interferir no funcionamento dos equipamentos presentes na sala.

O ambiente deve ser também composto por uma programação visual adequada que indique as tensões das tomadas, os espaços para passagem de cabos, a localização dos equipamentos de segurança, o caminho de saída e as portas.

c) Acabamento e mobiliário

O acabamento deve nortear todo o ambiente proporcionando limpeza e organização ao local, no entanto materiais combustíveis e de PVC devem ser evitados assim como carpetes e cortinas que podem acumular poeira. Adequando-se a esses aspectos, também deve ser enquadrado o mobiliário, que deve ser resistente para suportar o peso dos equipamentos, funcional no sentido de facilitar as instalações e as mudanças de *layout* e feito de metal ou outro material incombustível.

ENERGIA ELÉTRICA

A energia elétrica fornecida a um CPD deve ser estabilizada e ininterrupta, portanto recomenda-se que toda a alimentação seja fornecida por sistema *no-break*, que além de fornecer energia limpa para os equipamentos, atua também como fonte alternativa. Deve ser dimensionado para suportar 50% a mais da máxima carga a ser utilizada, devido aos picos de demanda. Deve ser modular para permitir expansões futuras.

O cabo de entrada da concessionária deve ser duplicado na subestação local, de forma que se tenha uma fonte alternativa caso a primeira falhe. Na subestação devem existir transformadores que isolem a instalação interna da externa. Uma forma de garantir energia independentemente das concessionárias é a instalação de um grupo gerador *diesel* que deverá entrar em operação toda vez que houver falta da alimentação externa.

Todo o sistema deve contar com um aterramento eficiente, de forma a garantir que correntes circulantes na malha de terra não retornem aos equipamentos, evitando choques acidentais e perdas de informação. Isto pode ser alcançado através do dimensionamento das cargas a serem ligadas e da passagem de uma malha de terra de acordo com as normalizações vigentes.

CABEAMENTO

"Convém que o cabeamento elétrico e de telecomunicações que transmite dados ou suporta serviços de informação seja protegido contra interceptação ou dano" (NBR ISSO/IEC 17799, 2001, p.16). A separação entre os cabos de dados e os cabos de elétrica, é a medida a ser tomada para prevenção de interferências. A proteção física dos cabos pode ser feita com uso de tubos conduítes e canaletas através do piso elevado. A identificação e a codificação do cabeamento são importantes nas manutenções e expansões do sistema.

CLIMATIZAÇÃO

Os CPDs são totalmente dependentes das instalações de climatização, em função das exigências de níveis de temperatura e umidade inerentes aos equipamentos que o compõe. Um sistema de condicionamento de ar destina-se a manter um ambiente isento de impurezas, bem como ao clima em condições ideais e estáveis. A pressão positiva deve ser mantida dentro do recinto, o que impede a entrada de fumaça e impurezas. Para se garantir a eficácia desse recurso, recomenda-se que se tenha um sistema exclusivo para essa área, e que se use filtros de materiais incombustíveis, sendo passível de manutenção e limpeza, e que possua controle automatizado, o que fará o sistema se regular automaticamente de acordo com parâmetros previamente determinados em projeto.

A temperatura e a umidade relativa ideais devem ficar em 22^{o} C e 55% respectivamente[5], isto pode ser alcançado com eficiência a partir da utilização de caixas de volume de ar variáveis (VAVs), que possuem controles PID (proporcional integral derivativo). Para manutenção de um ambiente limpo e seguro deve ser proibido fumar no recinto. Deve-se contar também com um sistema de controle que feche os *dampers* nas

[5] Caruso e Steffen afirmam que ± 10% para temperatura e ± 5% para umidade relativa são os limites tolerados, bem como variação máxima de 1^{o}C a cada 5 minutos para temperatura e de 45% a 55% em menos de 8 horas para umidade relativa.

tubulações de insuflamento de ar-condicionado quando nível alto de poluição (fumaça) for detectado, para tanto será necessária a instalação de sensores nas tubulações, assim como a automatização dos *dampers*.

CONTROLE DE ACESSO

"O acesso deve ser franqueado somente a pessoas que precisem entrar nos recintos dos ambientes de informações em virtude da necessidade funcional" (CARUSO & STEFFEN, 1999, p.227). Para tanto o ambiente do CPD deve ser classificado como de alto risco[6], e deve contar com um sistema de controle de acesso eletrônico, de preferência com mais de um nível de segurança, como por exemplo, crachá de identificação e senha de acesso. Identificações biométricas como digitais e íris são recomendadas.

Esse sistema deve ser operado por pessoal de alta confiança, e deve prover funções qualitativas extremamente confiáveis, bem como relatórios de registro de acessos e eventos nos ambientes controlados. Sensores de porta devem ser instalados para garantir monitoração do funcionamento. Em casos extremos recomenda-se um posto de vigilância permanente na entrada do CPD, provido por pessoal treinado adequadamente.

PROTEÇÃO CONTRA INCÊNDIO

As recomendações presentes neste documento até agora se referiram a informação como foco principal, e em segundo plano aos equipamentos. No caso da proteção contra incêndio, as vidas humanas passam também a compor esse conjunto, tornando a especificação da segurança mais complexa e ao mesmo tempo mais importante. De modo a qualificar esse segmento, podemos dividi-lo em: detecção, combate e proteção passiva.

[6] Têm características específicas, sendo seu funcionamento vital para a sobrevivência da organização.

Os sistemas de detecção de incêndio têm evoluído muito nos últimos anos, oferecendo aos projetistas uma gama enorme de produtos para diferentes aplicações. Para o caso de uma área sensível como um CPD, é recomendável utilizar detectores de fumaça do tipo iônico, pois possuem tempo de resposta menor, em conjunto com detectores inteligentes ópticos de fumaça, pois podem funcionar por mais tempo em condições de sujeira. É aconselhável também o uso de detectores de câmara de aspiração, pela precisão em diagnosticar um incêndio através da análise do ar com raios *laser* em uma câmara fechada. Os detectores devem ser instalados no piso elevado, no ambiente e no teto rebaixado (se for o caso), obedecendo-se as distâncias regulamentadas na norma NBR 9441, editada pela ABNT, referente a sistemas de detecção e alarme de incêndio. Todas as peças devem ser ligadas por laços tipo "classe A"[7], a uma central de alarmes, onde se pode monitorar os níveis de poluição de cada uma. As sinalizações com sirenes e *strobes*[8] também são muito importantes para indicar a presença do sinistro e direcionar às saídas.

O combate ao incêndio pode ser automático, através da composição do sistema de detecção em conjunto com a liberação automatizada de gases para a extinção do fogo, ou manual com a liberação do gás extintor por um comando, ou ainda com a utilização de extintores de CO_2, que devem ser alocados em número adequado dentro do recinto. Extintores de água ou pó químico, a princípio não são recomendados, pois podem danificar os equipamentos.

Atualmente, a extinção automatizada de fogo em CPDs é feita com a utilização do gás FM200, que dimensionado corretamente, de acordo com o volume da sala, é eficaz e não é tóxico para as pessoas, ao contrário do gás carbônico que é letal. Este porém, foi largamente usado no passado, e ainda está presente em boa parte das instalações. Além

[7] Tipo de ligação em que existe um circuito fechado ligando os detectores à central de alarmes, aumentando a segurança do sistema

[8] Lâmpada especial tipo *flash,* para sistemas de incêndio. A luz emitida transpõe-se à fumaça.

disso o CO_2, quando liberado, provoca mudança brusca na temperatura do ambiente, podendo ser prejudicial também aos equipamentos. Por essas razões se tornou um recurso inconveniente nas novas instalações.

A proteção passiva contra incêndio é feita através de enchimentos nas paredes dos recintos com materiais isolantes, geralmente fibra de cerâmica, fibra de silício ou lã de rocha. Normas internacionais recomendam que as paredes suportem no mínimo a temperatura 1260^{o} C por uma hora. Outro recurso importante são as tintas intumescentes[9], que aplicadas as estruturas metálicas formam um conjunto impeditivo de propagação de fogo. As massas corta-fogo são indicadas para cobertura de cabos elétricos e de dados.

MONITORAÇÃO DO AMBIENTE

Para monitorar o ambiente do CPD, é recomendável a instalação de um circuito fechado de TV, que irá manter vigilância constante tanto no interior da sala quanto em seu perímetro externo, podendo ser configurado para indicar alarmes em caso de invasão devido ao recurso de detecção de movimento. As imagens devem ser gravadas e armazenadas para o caso de consulta posterior. O tempo de retenção ficará a cargo dos administradores da segurança.

1.3 Procedimentos Operacionais

"*O principal esforço administrativo dentro de qualquer organização é o estabelecimento de padrões de execução de atividades e de comportamento de seres humanos*" (CARUSO & STEFFEN, 1999, p.259). Porém, as rotinas podem significar riscos à medida que os procedimentos se tornam mecânicos e repetitivos. Neste sentido,

[9] Pintura que se parece com um *"coating"* e que oferece resistência ao fogo em estruturas metálicas. Na presença do fogo, a película de tinta intumesce formando uma camada isolante que protege o perfil metálico.

convém lançar mão de recursos como, rodízio de pessoal, cursos de reciclagem, e até mesmo mudanças superficiais nos procedimentos, com objetivo de manter atentas as equipes responsáveis.

Controle de Acesso de Pessoas e Materiais

O acesso de pessoas previamente autorizadas às dependências do CPD foi descrito na secção anterior, porém existe a situação de serviços esporádicos de funcionários terceirizados, bem como visitação de pessoal externo. Nesses casos devem ser registradas informações como: nome, procedência, motivo da entrada, organização à qual está ligado, número de documento de identidade, data e hora de entrada e saída, nome do responsável que autorizou e assinatura da pessoa em livro de registros. Caso portem algum objeto, este deve ser registrado e analisado com cautela, pois no caso de ímãs, materiais explosivos e mídias virgens, figuram em ameaças ao sigilo e a integridade das informações.

Procedimentos de Emergência

Todo o aparato tecnológico dimensionado para situações de emergência pouco ou nada pode fazer se as pessoas envolvidas não forem conscientizadas a respeito dos riscos. Este fato dá origem a necessidade de se ter uma política de segurança interiorizada na cultura dos colaboradores, sendo estabelecida regras claras e objetivas a serem seguidas.

O detalhamento dos procedimentos deve levar em consideração situações como: incêndio, falta de energia, tempestades e raios, assaltos , invasões, terremotos, etc. Enfim, todas as situações que podem significar riscos para o funcionamento do CPD.

TESTES E SIMULADOS

Os colaboradores envolvidos em torno de um ambiente sensível devem estar sempre preparados para situações de emergência, os testes e simulados assim como cursos de reciclagem, ajudam a mantê-los atentos e atualizados aos procedimentos padrões, amenizando o risco de imperícias e negligências quando solicitados. Quanto aos equipamentos, estes devem sofrer manutenções preventivas constantes, efetuando-se testes periódicos de funcionamento, além disso é importante haver uma equipe preparada para reparos, com peças sobressalentes à disposição, isto contribui para que a estrutura esteja sempre em funcionamento.

CAPÍTULO 2
Segurança física dos meios de armazenamento

2.1 Introdução

Os meios de armazenamento estão sujeitos a uma série de riscos que podem afetar a sua integridade. Podemos citar por exemplo a exposição a campo magnético, a calor, à umidade, a impacto mecânico e à poeira, como os principais agentes que compõem a lista dos causadores de destruição física de informações, levando-se em conta todos os tipos de meios de armazenamento existentes. Não obstante, o transporte, a deterioração natural e falta de testes periódicos das mídias gravadas, figuram como pontos chaves para definição de procedimentos seguros para evitar a perda de informações.

2.2 Fatores de Risco

CAMPO MAGNÉTICO

Os campos magnéticos são gerados ao redor de um condutor, quando este é percorrido por uma corrente elétrica. Um campo com intensidade de 4.000 A/m é fatal para qualquer mídia magnética, de acordo com Caruso (1999, pág.276). A uma distância de 10 mm, essa intensidade decai para 250 A, o que nos parece uma situação improvável em um ambiente de armazenamento de mídia, entretanto recomenda-se uma distância de segurança bem maior.

A exposição às antenas de telecomunicações que emitem ondas eletromagnéticas também deve ser evitada, pois pode danificar o conteúdo das mídias.

DECOMPOSIÇÃO QUÍMICA

Os componentes plásticos usados na fabricação das mídias são susceptíveis a decomposição química quando submetidos ao calor excessivo e aos poluentes atmosféricos. Essa deterioração compromete a qualidade do que está gravado, assim como regravações futuras.

CHOQUES MECÂNICOS

Os choques mecânicos podem causar danos aos conteúdos das mídias, portanto deve-se ter cuidado e cautela no seu manuseio.

2.3 Instalações

Assim como em um ambiente de CPD, a sala para guarda dos meios de armazenamento deve ter características peculiares para garantia da integridade das informações. O lugar deve ser provido de sistema de climatização ambiente, seguindo os valores discriminados nas tabelas 1 e 2. *"Para situações freqüentes, tais como operação (uso), transporte, manutenção ou outro manuseio de rotina as variações temporárias das condições ambientais devem ser contidas dentro de limites aceitáveis específicos"* (NBR 11515, 1990, p.3). Além disso o ambiente deve contar com paredes com resistência contra fogo, instalações elétricas adequadas, proteção contra raios, aterramento e iluminação de emergência.

Um recurso largamente utilizado nas empresas e por este trabalho também recomendado são os diversos tipos de cofres para mídias. Esses equipamentos são dimensionados para suportar impactos, fogo e tentativa de furto, recomenda-se entretanto certificados de laboratório independente, no sentido de assegurar os limites estabelecidos na especificação técnica.

2.4 Segurança Operacional

Todo esquema montado para guarda de informações deve contar com procedimentos operacionais específicos, a fim de assegurar a sua eficácia.

DOCUMENTAÇÃO

"O registro é uma medida indispensável para um controle adequado de todos os meios de armazenamento disponíveis e de sua localização" (CARUSO & STEFFEN, 1999, p.278). Entretanto recomenda-se a identificação de todas as mídias armazenadas com etiquetas visuais. As alterações feitas em programas também devem ser documentadas e guardadas para o suporte posterior.

PROCEDIMENTOS OPERACIONAIS

As cópias efetuadas devem ser testadas ao longo do tempo, respeitando-se a vida útil das mídias e o número máximo de regravações estabelecidas pelo fabricante, pois existem vários registros de perda de informação por falta de cuidado com esses itens.

No recinto de armazenamento deve ser proibida a entrada de alimentos para evitar acidentes. Este é um local de uso esporádico, isto é, somente quando houver necessidade, portanto o trabalho permanente deve ser proibido, de acordo com Caruso (1999, pág. 279). Mas para o caso de anormalidades, algumas diretrizes devem ser elaboradas no sentido de se ter ações imediatas, para amenizar os possíveis danos.

Os procedimentos de recuperação devem ser estabelecidos pela equipe responsável, este documento procura prever todas as situações possíveis orientando sobre as medidas a serem tomadas e ainda rotas alternativas para o caso de imprevistos.

Por fim recomendamos algumas práticas a serem seguidas em relação a utilização de mídias para armazenamento de informações, a citar: testes de aceitação em mídias

novas; as fitas devem ser guardadas na posição vertical; a caixa da fita só deve ser aberta na sala de operação; para transporte de mídias, deve ser usada caixa apropriada bem como seguir os limites de temperatura impostos nas tabelas 1 e 2; após constantes sacudidas, as fitas devem ser rebobinadas para recuperarem a tensão; a mídia dos disquetes nunca deve ser tocada.

Tabela 1 – Condições normais para discos rígidos e fitas

Situação	Temperatura	Umidade relativa	Partículas no ar máx. por m^3
Condições Ideais - mín. / máx. - variação (±)	+17° C / + 23° C máx 2 por hora	+45% / 55% máx. 5 por 24h	< 5µm: o mínimo > 5µm: isento
Limites normais - Transporte (mín. / máx.) - Operação (mín. / máx.) - variação (±)	+5° C / + 32° C (A) +16° C / + 32° C máx. 10° C por hora	20% / 60% 20% / 60% máx. 5 por 24h	< 5µm: 30.000 > 5µm: 01
Limites de emergência	+ 75° C	85%	(B)

(A) Fita virgem pode ser exposta +48° C.
(B) Fita – Contaminação por partículas pode ser resolvida por processo de saneamento, desde que haja corrosão (fuligem, ácido).

Fonte: (NBR 11515, 1990, pág. 3)

Tabela 2 – Condições normais para discos flexíveis

Situação	Temperatura	Umidade relativa	Partículas no ar máx. por m^3 (M=milhão)
Condições Ideais - mín. / máx. - variação (±)	+17° C / + 23° C máx 2 por hora	+45% / 55% máx. 5 por 24h	< 5µm: 30.000 > 5µm: 01
Limites normais - Arquivo (mín./máx.) - Transporte - Operação (mín./máx.) - variação (±) -	+4° C / + 51,5° C -40° C / + 51,5° C +10° C / + 51,5° C máx. 20° C	8% / 65% 8% / 65% 30% / 65% Sem restrição	> 0,3µm: 540 M > 0,5µm: 85 M > 1µm: 8 M > 5µm: 25.000
Limites de emergência	+ 55° C	85%	(A)

(A) Fita – Contaminação por partículas pode ser resolvida por processo de saneamento, desde que não haja corrosão (fuligem, ácido)

Fonte: (NBR 11515, 1990, pág. 4)

CAPÍTULO 3
Plano de contingência

3.1 Objetivo

Um plano de contingência estabelece uma série de procedimentos padronizados, com o objetivo de amenizar os impactos causados por um desastre, em que toda a segurança implementada não conseguiu evitar. Parece-nos evidente que uma organização interrompe boa parte de suas atividades, quando um desastre acontece em seu ambiente de processamento de informações, espera-se portanto, que a equipe responsável já tenha em seu escopo de serviços as devidas ações a serem tomadas mediante tal situação. Entretanto os esforços a se despenderem, bem como os custos envolvidos para implementação de um plano de contingência, devem estar de acordo com as necessidades vitais de cada área da organização, as quais, deverão previamente definir seus serviços essenciais para que sejam inseridos no escopo de recursos que serão restaurados no menor tempo possível.

> *É importante que as conseqüências de desastres, falhas de segurança e perda de serviços sejam analisadas. Recomenda-se que os planos de contingência sejam desenvolvidos e implementados para garantir que os processos do negócio possam ser recuperados dentro da requerida escala de tempo. É importante que tais planos sejam mantidos e testados de forma a se tornarem parte integrante de todos os outros processos gerenciais.* (NBR ISO/IEC 17799, 2001, p.45)

Vale ressaltar que a efetivação de um plano de contingência a um custo justificado, está atrelada a idéia de serviços informatizados essenciais, os quais devem estar instituídos nas atribuições dos responsáveis de cada área da organização, visando principalmente àqueles recursos que a organização depende para sobreviver. Neste ponto o conhecimento específico das áreas e o trabalho em equipe são vitais, portanto os preciosismos e os

exageros devem ser evitados, em prol da otimização do consumo de verbas, tempo e pessoal para execução dos processos.

3.2 Conceituação

Para um entendimento conceitual de um plano de contingência, listamos a frente os itens considerados importantes na visão de vários autores sobre o assunto, os quais definem parâmetros e premissas a serem seguidas, porém em alguns casos suas idéias não chegam a divergir mas se complementam, dando margem à criação de meios próprios na resolução dos problemas por cada profissional da área, e da pluralidade de idéias para esse nível de segurança. Por esse motivo entendemos que seguir a linha de um determinado autor pode significar uma incompleta adequação do que se propõe, às características da organização. Além disso no início dos trabalhos, está-se diante de questões subjetivas, as quais a concretização dependerá de um consenso entre as partes envolvidas. Portanto além de um estudo preliminar do que se entende por plano de contingência, deve-se também considerar as particularidades internas e o nível de contingência que se almeja.

Uma forma interessante e padronizada de se chegar a um plano ideal, considerando os riscos, os custos e o restante dos pontos de análise, é a utilização de guias padronizados, onde se pode enquadrar todas as implicações pertinentes, e lançá-las em um modelo onde, segundo os fabricantes, estão previstas todas as situações possíveis, ficando a cargo do operador a responsabilidade e inserir as informações. Um bom exemplo desse tipo de programa é o "*BCP Generator*" que pode ser encontrado na página: "http://www.disasterrecoveryworld.com".

Para iniciar os trabalhos, recomenda-se:

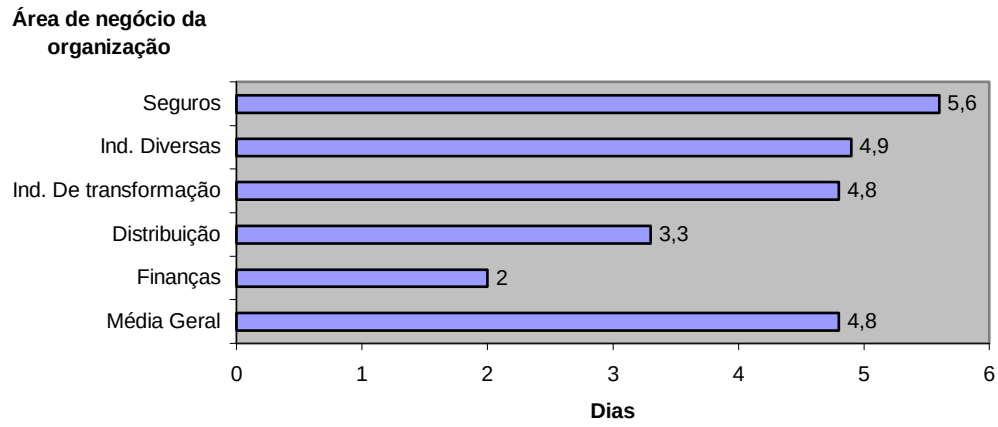
a. definir o grau de criticidade dos serviços computadorizados, isto é, pontuar e classificar cada serviço administrativo de modo a perceber sua importância para a área de negócios.

b. definir as prioridades dos serviços, caracterizando a importância que determinados aplicativos têm para o fluxo organizacional.

c. definir o período crítico, que pode ser entendido como o tempo máximo que uma área pode funcionar sem o auxílio de determinada aplicação.

Para um referencial corporativo, sugerimos analisar o gráfico 1, em que se pode observar um estudo feito pela Universidade de *Minnesota*, sobre o tempo médio que funções essenciais se mantém após um desastre.

Gráfico 1 - Período médio de tempo durante o qual as funções essenciais das organizações se mantém após um desastre no CPD (por atividade). Estudo da Universiade de Minnesota



Fonte: (CARUSO & STEFFEN, 1999, p.290)

O tempo necessário para o retorno das atividades dependerá do grau do problema que ocasionou a parada, portanto os responsáveis das áreas envolvidas deverão tomar ciência do ocorrido e serem informados sobre a previsão de tempo de indisponibilidade.

3.3 Modelo de um plano de contingência

O modelo apresentado a seguir é representado por um resumo do que propõem Caruso & Steffen em “Segurança de informática e de informações – 1999” no seu apêndice “D”.

DEFINIÇÃO DOS GRUPOS ENVOLVIDOS NO PLANO DE CONTINGÊNCIA:

a. Coordenação – coordenação geral do plano de contingência;
b. Áreas de negócios – coordenação dos aspectos relacionados à área de negócios;
c. Administrativo – coordenação de todas as atividades de apoio administrativo;
d. Aplicativos – coordenação do ferramental necessário para o processamento de aplicativos durante a contingência;
e. *Hardware* – coordenação dos equipamentos necessários para a contingência;
f. *Software* – coordenação das exigências relacionadas com *software* básico e de apoio;
g. Operação – coordenação da operacionalização do plano de contingência;
h. Comunicações – coordenação e execução de procedimentos necessários para operacionalização da estrutura de comunicações na contingência;
i. Microinformática – coordenação e execução da estrutura de microinformática.

PLANO DE AÇÃO

a. Controles a serem mantidos – descrição de todos os controles a serem mantidos com relação equipamentos, softwares, infra-estrutura e documentação;

b. Procedimentos de retorno - descrição de todos os controles a serem restaurados com relação a equipamentos, softwares, infra-estrutura e documentação;

OPERACIONALIZAÇÃO DO PLANO

Nesta parte estabelecemos as informações referentes a recursos humanos e de maquinário necessário para as ações do plano de contingência. Também definimos os responsáveis por manter e atualiza-lo.

a. Manuais de contingência – definição dos procedimentos de contingência, especificando os responsáveis por manter as atualizações, descrição dos equipamentos e *softwares* necessários;
b. Relação de pessoal – relação geral de todas as pessoas envolvidas com suas funções específicas. Neste documento devem constar dados como: nome, endereço, telefone e as atividades relacionadas ao plano de contingência;
c. Relação de equipamentos e *softwares* – relação de todos os equipamentos e *softwares* inseridos no plano e contingência. Na parte de *hardware* podemos citar: gabinetes, microcomputadores, discos, fitas, impressoras, equipamentos de telecomunicações e etc. Quanto aos *softwares* destacam-se os sistemas operacionais de rede e de estações de trabalhos, aplicativos de comunicação e aplicativos de apoio.

CAPÍTULO 4
O estado da arte: Sala cofre

4.1 Introdução

Neste capítulo trataremos da apresentação de um recurso cada vez mais evidente nas empresas que zelam pela segurança de seus dados. As metas e premissas de segurança física da informação chegaram em um nível tal de exigência, que - em muitos casos - foi necessário se dar um passo a frente do que se produzia até então. Tendo como base todo o conhecimento adquirido anteriormente com as normalizações e modelos construtivos de ambientes para processamento de informações, foi inserido no mercado a alguns anos atrás o conceito de sala-cofre.

Este equipamento de segurança conta com um aparato tecnológico altamente desenvolvido, com o principal objetivo de salvaguardar fisicamente tudo que dentro dele estiver. A casca metálica envoltória do sistema propicia isolamento contra pulsos eletromagnéticos e de rádio-freqüência. Além disso como se tratam de módulos montados de forma a atender especificações de cada empresa, a sala-cofre pode também ter seu tamanho modificado, dentro de determinados limites, bem como ser transportada para outros lugares, graças ao conceito de modularidade. O investidor que despender recursos nesse empreendimento pode transferir a localização do seu patrimônio, utilizando os mesmos benefícios que tinha antes (o que não ocorre com o modelo tradicional de construção de CPDs). Nesse aspecto não se recomenda efetuar qualquer mudança sem antes consultar o fabricante dos equipamentos, pois se trata de algo muito específico, o que incorre na necessidade de contratação de empresas certificadas para exercerem tal função.

Este fato deve ser observado também no momento da aquisição do sistema, pois conforme o desenvolvimento da tecnologia, mais os fabricantes estão trabalhando com a certificação de parceiros, para que tenham garantias de condições na implantação de seus sistemas.

As paredes de concreto e alvenaria que compõe o modelo tradicional de construção de CPDs acumulam umidade cristalizada desde a sua construção, em caso de altas temperaturas essa umidade se despende das paredes passando sobre a forma de vapor para o ambiente[10], o que pode danificar componentes eletrônicos e mídias[11]. Uma sala-cofre delimita um local totalmente estanque para o resto do ambiente, não apresentando transferência de umidade para sua área interna. Isso inclui a exposição a altas temperaturas, pressão de gases corrosivos e água.

4.2 Aspectos gerais

A sala-cofre é composta por duas camadas envoltórias, uma camada externa refratária capaz de suportar temperaturas de até 1000^{o} C, e uma célula interna hermética, estanque a gases e líquidos. Um modelo didático sobre esse conceito pode ser verificado na figura 1.

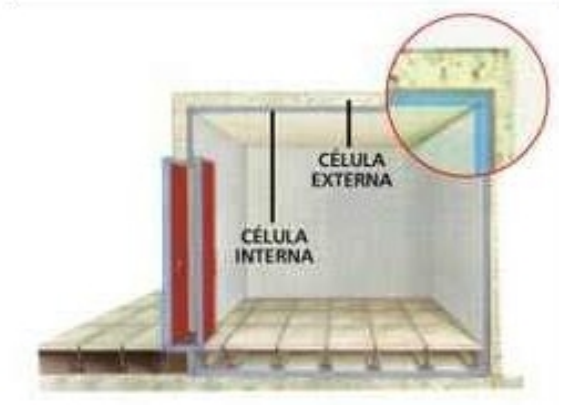


Figura 1- Modelo didático sobre as camadas da sala-cofre.

[10] De acordo com a norma NBR 11515/1990 a umidade relativa do ar limite para armazenamento de mídias é de 85%.
[11] Segundo Aceco TI, 100^{o} C são suficientes para liberar água cristalizada do concreto.

A câmara externa tem função de isolar termicamente e proporcionar resistência mecânica à estrutura. Alguns projetistas fazem uso de uma estrutura de concreto e alvenaria para compor esta camada, podendo-se também aproveitar os tetos e paredes existentes, desde que estejam dentro dos padrões de projeto. Existe também a solução modular, onde a câmara externa é parte integrante de um conjunto metálico que compõe toda a sala, portanto o fabricante fornece a estrutura completa de forma a atender os padrões de projeto.

A camada interna é composta por elementos pré-fabricados em chapas de aço com 3 cm de espessura, conforme afirma Brasiliano (2001, pág 4). As chapas ou painéis são montados internamente de modo que exista um vão entre a camada externa e a interna. Os dois conjuntos são montados de forma independente, embora estejam fixados um ao outro por pontos de solda. Esses pontos de fixação possuem flexibilidade para não prejudicar a estanqueidade do sistema no caso de deformações.

O acesso à sala-cofre é feito através de duas portas subseqüentes: a primeira é refratária integrada à câmara externa e abre para fora, a segunda é uma porta estanque integrada a câmara interna e abre para dentro. O estado normal das portas é fechado, sendo os comandos de abertura enviados através de um sistema eletrônico de controle de acesso. O nível de segurança desse sistema, pode ser de um simples crachá de identificação, passando por autenticação com códigos numéricos podendo chegar até a identificação biométrica, onde se verificam as digitais dos dedos, a retina, a voz e a íris.

O sistema que gerencia a abertura das portas também pode ser acionado para travá-las em caso de invasões à empresa, no entanto as requisições de saída, isto é, pessoas que estão dentro da sala podem abrir as portas normalmente, pois se assim não fosse, a vida humana estaria em perigo.

Para um nível de segurança maior é recomendado que a sala-cofre tenha um sistema de detecção de incêndio, bem como um sistema de combate, com a utilização de descarga de gás supressor de combustão. Esse gás não deve ser tóxico ao ser humano, sendo sua descarga fruto da decisão que o sistema automático deve tomar ao se identificar com precisão a incidência de combustão dentro do ambiente. Além disso, deve ser acionado um alarme avisando a ocorrência do sinistro aos empregados responsáveis pelas ações imediatas.

O cabeamento elétrico e de dados que chega à sala-cofre deve ser totalmente estruturado e passar por quadros de blindagem modular que permitam o isolamento do ambiente interno. É também recomendável a cobertura de todos os cabos e tubulações com massa do tipo corta-fogo[12] para evitar propagação de incêndio pelos seus leitos. Esses cabos trafegam pelo piso elevado da sala, que possui uma estrutura preparada para recebê-los de acordo com as normas internacionais de cabeamento estruturado.

4.3 Aplicações

A salas-cofre são recomendadas para abrigar equipamentos que possam trabalhar sem intervenção humana, conforme afirma Brasiliano (2001, pág 4). As principais aplicações do conceito são voltadas para servidores de rede, discos e fitotecas robotizadas, equipamentos de comunicação e outros itens de funcionamento crítico.

Geralmente o que tem se visto nas grandes empresas é a adoção de se construir um "*datacenter* "[13] e dentro dele abrigar a sala-cofre. Isto eleva o grau de segurança dos serviços informatizados, porém o custo de implantação de uma sala-cofre ainda é muito

[12] Massa especial para cabos e tubulações, com o principal objetivo de isolamento térmico.

[13] *Datacenter* é um termo atual utilizado pelo mercado que significa um grande CPD, com recursos tecnológicos e com capacidade para crescimento. Por causa do alto investimento para sua implantação, um novo ramo de negócio surgiu, onde a empresa dona do *datacenter* aluga serviços para outras empresas, garantindo segurança e disponibilidade de funcionamento.

alto, bem como os equipamentos que a compõe e os serviços de profissionais especializados. Em todo caso vale a ressalva de que todo o investimento despendido, dependerá de quão valorosas são as informações que se deseja guardar.

Conclusão

Tivemos ao longo deste trabalho a inserção de vários conceitos técnicos voltados para a segurança física da informação. Não obstante os casos exclusos, certamente o grau de profundidade que se chegou foi demais adequado para o propósito que tínhamos inicialmente. Em nosso entendimento, a meta que se definiu de estabelecer padrões de segurança e conhecer mais sobre as diferentes disciplinas que a envolvem, foi atingida por completo. Sabemos porém que observações podem chegar a citar as omissões que tivemos, no entanto em nossa visão os pontos abordados englobam os mais importantes temas de interesse nesse assunto.

Foi de extrema importância a utilização das referências bibliográficas, pois a fusão dos seus conteúdos nos proporcionou uma pluralidade de idéias que se autocompletavam ao longo do texto, enriquecendo-o de forma significante.

Descobrimos também que o assunto que abordamos ainda tem muito a se desenvolver sobre a forma de literatura, pois tivemos dificuldades para reunir o material adequado para trabalhar. Além disso percebi que algumas passagens escritas à cerca de somente cinco anos atrás, já não valem mais. Portanto para quem leu esse trabalho não espere que aqui estejam informações totalmente duradouras, pois o avanço da tecnologia e as novas necessidades certamente o tornarão muito em breve parcialmente obsoleto.

Quanto a isso a conclusão que tenho é que apesar de ter chegado onde desejava, o esforço para se manter a segurança física é um trabalho contínuo de atualização e implementação de tecnologias, que só cessará quando não houver mais ameaças.

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799 - Tecnologia da Informação:** Código de Prática para a gestão de segurança da informação. Rio de Janeiro: ABNT, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 11515 - Critérios de segurança física relativos ao armazenamento de dados**. Rio de Janeiro: ABNT, 1990.

CARUSO, Carlos A. A.; STTEFEN, Flávio Deny. **Segurança em Informática e de Informações**. 2ª ed. rev. e ampl. São Paulo: Senac, 1999.

CASTRO NETO, Jaime Spinola. **Edifícios de alta tecnologia.** São Paulo: Carthago & Forte, 1994.

MARTE, Cláudio Luiz. **Automação Predial**: A inteligência distribuída nas edificações. São Paulo: Carthago & Forte: 1995.

FERREIRA, Aurélio B. de Holanda. **Novo Aurélio Século XXI**: o dicionário da língua portuguesa. 3ª ed. Rio de Janeiro: Nova Fronteira, 1999.

LUBIANCO, Júlio. Incêndio destrói parte do prédio da Petrobrás. **JB Online**, Rio de Janeiro: 20 maio 2004. Disponível em: <www.jb.com.br>. Acesso em: 28 set. 2004.

Prejuízo de R$ 3 milhões. **JB Online**, Rio de Janeiro: 27 fev. 2004. Disponível em: <www.jb.com.br>. Acesso em: 28 set. 2004.

PETRAGLIA, Marcela. Incêndio no Ministério do Trabalho. **JB Online**, Rio de Janeiro: 09 fev. 2002. Disponível em: <www.jb.com.br>. Acesso em: 28 set. 2004.

ACECO. **Segurança para ambientes de TI**. Disponível em <http://www.aceco.com.br/acecoti/seguranca/seguranca.html>. Acesso em: 30 set. 2004.

BRASILIANO, Antônio C. R. **Conceito de segurança em áreas computacionais – CPD.** Disponível em <www.brasiliano.com.br>. Acesso em: 6 ago. 2004

SCUA**. A Norma Brasileira para a Gestão da Segurança da Informação (ISO/IEC 17799).** Disponível em <www.scua.com.br>. Acesso em: 10 ago. 2004

ANTUNES, Edson. **Planejamento de Contingência e Continuidade de Negócios.** Disponível em <www.modulo.com.br>. Acesso em: 10 out. 2004.

SOUZA, Renato Bernardes. **Proteção passiva contra incêndios.** Disponível em <www.unifrax.com.br>. Acesso em: 12 out. 2004.

Anexo A

Publicado em.: 20/05/2004.....Fonte..: JORNAL DO BRASIL
Página.....: 018.....Edição.: 01
Autor: Júlio Lubianco

Incêndio destrói parte do prédio da Petrobrás

Parte da laje do último andar desabou de madrugada. Não houve feridos.

Um incêndio destruiu, na madrugada de ontem, 650 metros quadrados do 26º andar do prédio sede da Petrobrás, na Avenida República do Chile, no Centro. O fogo foi controlado pelos bombeiros e não houve vítimas. **No local, funcionava a central de telecomunicações do edifício, que foi danificada**. Parte da laje do prédio desabou devido à dilatação provocada pelo fogo.

Funcionários sentiram cheiro de fumaça e borracha queimada e alertaram a brigada de incêndio interna da empresa, que iniciou o combate às chamas. Bombeiros de quatro quartéis foram chamados e controlaram a situação em pouco mais de duas horas. Eles precisaram entrar no prédio, pois a escada Magirus não chegava até o fogo, no último andar.

Segundo o coronel Roni Azevedo, o trabalho foi feito com relativa facilidade devido ao bem estruturado sistema de prevenção do prédio, que conta com sensores de fumaça e uma brigada de incêndio. Depois de extinto o fogo, o trabalho de rescaldo, para evitar novos focos, se estendeu até o início da manhã.

Mais de 3 mil pessoas trabalhavam no local, mas apenas alguns funcionários da limpeza, segurança e manutenção estavam no prédio durante o incêndio. Por precaução, a empresa suspendeu o expediente. Com o prédio interditado, os funcionários que chegavam para trabalhar eram orientados para voltar no dia seguinte.

No início da noite, a empresa divulgou nota informando que as causas do incêndio ainda não são conhecidas. Uma comissão formada por funcionários, Conselho Regional de Engenharia e Arquitetura (Crea-RJ) e Sindipetro-RJ vai investigar as causas do incidente.

Pela manhã, todos os telefones do prédio estavam fora de operação, já que o fogo atingiu exatamente a central de telecomunicações do prédio. Uma reunião da diretoria com investidores e analistas, para apresentação do planejamento estratégico anual, foi transferida para o prédio da BR Distribuidora, no Maracanã. Durante o dia, técnicos e peritos do Corpo de Bombeiros e da Defesa Civil fizeram uma inspeção para tentar identificar as possíveis causas do fogo. Foi mantida a interdição dos três últimos andares e liberado o restante do edifício. O Instituo de Criminalística Carlos Éboli vai divulgar o laudo da perícia em 30 dias.

O Sindicato dos Profissionais da Petrobrás divulgou nota defendendo a realização de concursos públicos para ocupar postos de trabalho terceirizados. De acordo com o sindicato, a terceirização aumenta o risco de problemas, e outros focos de incêndio no mesmo edifício já foram controlados por profissionais que conhecem bem o local. O sindicato alega que um funcionário que não conheça detalhadamente o ambiente de trabalho não tem condições de atuar com a mesma eficiência.

Anexo B

Publicado em.: 27/02/2004.....Fonte..: JORNAL DO BRASIL
Página.....: 026.....Edição.: 01
Autor: não divulgado

Prejuízo de R$ 3 milhões

O incêndio na sede da Eletrobrás deverá causar **um prejuízo de R$ 2 a R$ 3 milhões para a estatal**, que será coberto pelo seguro. Essas são as estimativas preliminares do presidente em exercício e diretor financeiro interino da companhia, José Drumond Saraiva.

O executivo explicou que, além do seguro predial, com a Porto Seguro, no valor de R$ 23 milhões, a Eletrobrás tinha seguro próprio de até R$ 11,5 milhões, com a Marítima Seguradora, para cobrir equipamentos no local. **Apesar de admitir perda de informações importantes para a empresa**, Saraiva explicou que grande parte dos documentos estava digitalizada na rede de computadores e foi salva quando o primeiro foco de incêndio foi apagado e a equipe de informática da estatal pôde entrar no prédio.

Vamos contabilizar perdas nos nossos ativos de conhecimento, mas isso não afeta o funcionamento da empresa - explicou.

Saraiva não quis especular sobre a causa do incêndio mas desconsiderou a possibilidade de uma ação criminosa. Mesmo assim, a estatal solicitou ao Conselho Regional de Engenharia, Arquitetura e Agronomia do Rio de Janeiro (Crea-RJ) ajuda nas investigações.

Ao todo, cerca de 900 funcionários e prestadores de serviços da Eletrobrás trabalhavam no prédio - outros 250 ligados à Sul América Capitalização.

A Eletrobrás é a maior companhia do setor elétrico brasileiro e tem um valor de mercado (soma do preço de todas as ações) de R$ 18 bilhões. Segundo estimativas de analistas, o faturamento da estatal no ano passado deve ser de R$ 18 bilhões, com lucro líquido de R$ 2 bilhões.

A empresa é uma holding, que controla as maiores geradoras de energia do país, que são Chesf, Furnas e Eletronorte. Além disso, a companhia controla a Eletronuclear, que administra as usinas nucleares de Angra 1 e 2.

Anexo C

Publicado em.: 09/02/2002.....Fonte..: JORNAL DO BRASIL
Página.....: 13.....Edição.: 1ª
Autor: MARCELA PETRAGLIA

Incêndio no Ministério do Trabalho

Um incêndio destruiu no início da noite de ontem os quatro últimos andares da antiga sede do Ministério do Trabalho, na Rua da Imprensa, Centro do Rio, onde hoje funciona o Tribunal Regional do Trabalho (TRT). **Pelo menos 30 mil processos judiciais foram queimados** em gabinetes de juízes localizados no 11º andar, de onde as chamas se alastraram, a partir das 18h, até o 12º pavimento, destruindo as instalações da Delegacia Regional do Trabalho e salas do TRT no 13º pavimento. Na cobertura, no 14º andar, foi atingido o gabinete do ministro do Trabalho, Francisco Dornelles, que viajou para o Rio tão logo soube do incêndio. Às 22h o fogo continuava alto e ameaçava o 10º andar.

Havia pelo menos sete pessoas no prédio quando o fogo começou. Os bombeiros demoraram 20 minutos para chegar ao local. Helicópteros foram acionados e houve dificuldade para obter água: seis hidrantes não funcionaram e o coronel bombeiro Paulo Ramos atribuiu a falha ao incidente provocado por um gambá em uma elevatória da Cedae, na quarta-feira . Carros-pipa da prefeitura também foram usados. Os bombeiros ainda enfrentaram o mau estado das mangueiras, repletas de fissuras. Não houve vítimas graves, mas no terraço do 14º andar estavam o segurança Laerte Oliveira, que feriu a mão esquerda ao quebrar uma vidraça de saída de emergência, e uma funcionária identificada apenas como Iolanda, que trabalhava no 12º andar e desceu até o 10º andar para desligar computadores.Ambos foram resgatados do prédio por cordas.

Ainda não há informações sobre a origem do fogo no prédio, construído em 1940, no governo Getúlio Vargas. Caberá à Polícia Federal investigar. **"É um prejuízo incomensurável. Meu carnaval acabou. Não sei o que farei para fazer o tribunal funcionar na quinta-feira",** alarmou-se a presidente do TRT, a juíza Ana Maria Cossermelli. A área em torno do edifício foi isolada, pois pedaços de vidros e esquadrilhas das janelas começaram a despencar. Segundo o juiz Luiz Carlos de Brito, de 70 anos, aposentado, os processos destruídos poderão ser retomados, com a colaboração das partes, que deverão ceder novamente cópias dos documentos necessários. **"É uma tragédia", lamentou o magistrado, que trabalhou 15 anos no prédio onde funcionam 43 varas trabalhistas, com 10 mil processos tramitando em cada uma.**

Anexo D

Lei nº 4.150/62:
"Art. 1º

Nos serviços públicos concedidos pelo Governo Federal, assim como nos de natureza estadual e municipal por ele subvencionados ou executados em regime de convênio, nas obras e serviços executados, dirigidos ou fiscalizados por quaisquer repartições federais ou órgãos paraestatais, em todas as compras de materiais por eles feitas, bem como nos respectivos editais de concorrência, contratos ajustes e pedidos de preços será obrigatória a exigência e aplicação dos requisitos mínimos de qualidade, utilidade, resistência e segurança usualmente chamados 'normas técnicas' e elaboradas pela Associação Brasileira de Normas Técnicas, nesta lei mencionada pela sua sigla 'ABNT'." (grifou-se)

Anexo E

Alguns artigos do Novo código civil

- Art. 186: “Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”

- Art. 187: “Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes”

- Art. 927: “Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo.”

– Par. único: “Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.”