Gestão da Tecnologia da Informação

Auditoria e Segurança da Informação

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Semana 07
Aula 13/14
Segurança Física

19/10

Francisco José Tosi

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Física:

"a segurança física desempenha um papel tão importante quanto à segurança lógica, porque é a base para a proteção de qualquer investimento feito por uma organização. Investir em diferentes aspectos da segurança sem observar suas devidas prioridades pode ocasionar uma perda de todos os recursos investidos em virtude de uma falha nos sistemas mais vulneráveis"

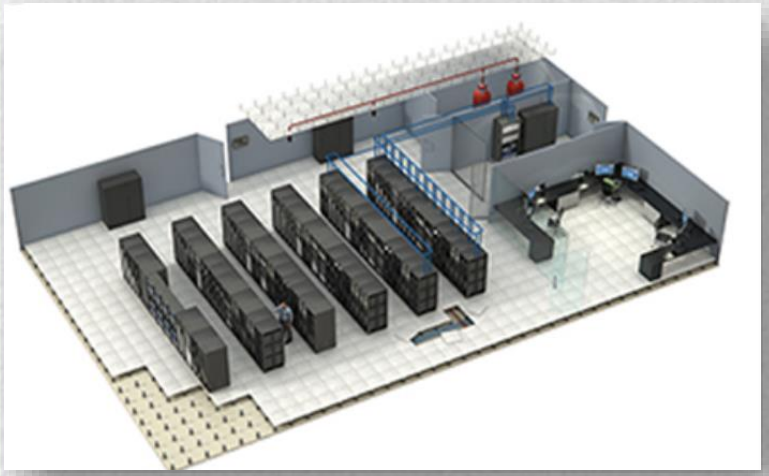
Ferreira e Araújo (2008, p. 123) Appud Gross

Auditoria e Segurança da Informação

Segurança Física:

ASPECTOS GERAIS DA SEGURANÇA FÍSICA

Os acessos as dependências da organização, sejam áreas de trabalho ou ambientes severos devem ser controlados.



Os sistemas de segurança devem ser implementados para garantir que em todos os locais da organização o acesso seja realizado apenas por profissionais autorizados

Quanto maior for a sensibilidade do local, maiores serão os investimentos em recursos de segurança para serem capazes de impedir o acesso não autorizado

Gross, 2013, p. 76

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Física:

ASPECTOS GERAIS DA SEGURANÇA FÍSICA

- ✓ As áreas e os ambientes físicos da organização devem ter acesso restrito para visitantes e outras pessoas que não trabalham no local no dia a dia.
- ✓ Os visitantes devem estar sempre acompanhados de alguém da organização.
- ✓ Todas as pessoas no ambiente da organização devem estar identificadas com crachás, e qualquer colaborador deve poder questionar pessoas sem identificação.

Gross, 2013, p. 76

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Física:

ASPECTOS GERAIS DA SEGURANÇA FÍSICA

Uma barreira corresponde a qualquer obstáculo colocado para prevenir um ataque:

física (cerca elétrica, parede);

lógica (processo de logon para acesso a uma rede);

combinação de ambas (autenticação de indivíduos por dispositivo biométrico para concessão de acesso, catraca eletrônica, porta aberta por cartão magnético).

Gross, 2013, p. 76

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Física:

ASPECTOS GERAIS DA SEGURANÇA FÍSICA

Perímetro de Segurança, "quaisquer elementos que estabeleçam uma barreira ao acesso indevido". Uma melhor definição para perímetro de segurança seria o contorno ou linha delimitadora de uma área ou região separada de outros espaços físicos ou lógicos por um conjunto qualquer de barreiras.

ISSO 17799 Appud Gross

- ✓ Sala Cofre;
- ✓ Roleta de controle de acesso físico;
- ✓ *Token*;

Auditoria e Segurança da Informação

Segurança Física:

SITUAÇÕES COMUNS DA SEGURANÇA FÍSICA

- ✓ Roubo de insumos (tais como fitas, disquetes etc.) e de partes de microcomputadores (memórias, discos etc.).
- ✓ Acesso de pessoas não autorizadas aos relatórios com dados estratégicos da empresa, ainda que dentro do setor de Tecnologia da Informação;
- ✓ Roubo de dados armazenados em arquivos magnéticos (fitas, disquetes etc.) ou ópticos (CD-ROM, CR-RW etc.) com conteúdo de interesse da empresa (lista de clientes, arquivos de senhas etc.).;
- ✓ Sabotagem em equipamentos e arquivos de dados

A forma de minimizar tais problemas é o rígido controle de acesso às áreas sensíveis da empresa

adoção de cartões magnéticos e bloqueios de portas tem-se mostrado eficiente contra acesso não autorizado

Gross, 2013, p. 77

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Física:

Recomendações Sobre Projetos

O ambiente de processamento de informações, deve ser localizado em uma área livre de quaisquer fatores de risco.

"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, apud Gross

Gross, 2013, p. 78

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Física:

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

A segurança de qualquer organização acarreta procedimentos operacionais padronizados para as inúmeras atividades exercidas

Necessário estabelecer padrões de procedimentos de segurança para as seguintes áreas

EDUCAÇÃO METODISTA

Gross, 2013, p. 80

Auditoria e Segurança da Informação

Segurança Física:

Procedimentos Operacionais

- ✓ Controle de acesso;
- ✓ Prevenção e combate a incêndios;
- ✓ Controle do fornecimento de energia;
- ✓ Controle das condições ambientais;
- ✓ Entrada e saída de equipamentos, materiais e produtos;
- ✓ Segurança dos meios de armazenamento.

Gross, 2013, p. 79

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Física:

Nos Meios de Armazenamentos

Mídias levadas para fora das instalações devem sujeitar-se a procedimentos de proteção e normas para que não permaneçam desprotegidas em áreas públicas

Os meios de armazenamento estão sujeitos a uma série de agentes de risco, que podem afetar o conteúdo dos mesmos

Gross, 2013, p. 80

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Ambiental:

A adequada proteção do ambiente e dos ativos físicos de informação, tanto como no caso do ambiente lógico, exige a combinação de medidas preventivas, detectivas e reativas

As proibições de fumar, tomar café, fazer refeições e outras regras de comportamento devem ser rigorosamente implementadas em todo lugar onde existir mídia magnética.

Gross, 2013, p. 81

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Ambiental:

Rede Elétrica

- ✓ A rede elétrica deve ser sempre estabilizada e dimensionada por profissionais especializados, sendo em seu planejamento, considerada a carga necessária.
- ✓ A manutenção deve ser tratada em procedimentos específicos, considerando a segurança contra incêndios.
- ✓ A fiação para o CPD deve ser única e independente para evitar a penetração de ruídos.
- ✓ Para cada ativo considerado crítico, principalmente os de processamento de dados, deve haver fornecimento de energia de forma alternativa, independente das concessionárias de energia.
- ✓ Para as situações de contingência deve-se fazer o uso de geradores de energia.

Gross, 2013, p. 83

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Ambiental:

Energia alternativa

Deve-se ter muita preocupação com *no-breaks* e geradores.

Assim, é importante que seja assegurado um fornecimento constante e contínuo de energia elétrica, à prova de falhas

fase de projeto devem ser previstos os locais e espaço suficiente para abrigar os equipamentos de geração e condicionamento de energia elétrica

Gross, 2013, p. 83

Auditoria e Segurança da Informação

Segurança Ambiental:

Localização

A escolha da localização correta é, provavelmente, a medida isolada mais importante que se pode tomar na fase de projeto

as instalações de processamento de informações, como qualquer outra instalação sensível, devem ser alojadas em edifício isolado ou em recinto isolado do resto do edifício por paredes divisórias corta-fogo

Gross, 2013, p. 84

EDUCAÇÃO METODISTA

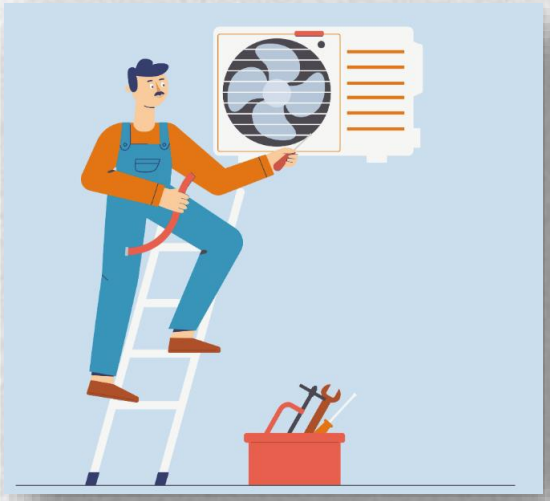
Auditoria e Segurança da Informação

Segurança Ambiental:

Climatização

é muito importante que se pense desde o início nas instalações de climatização de ambiente.

utilização de equipamento de ar-condicionado exige planejamento e em muitas ocasiões, a realização de obras, envolvendo especialistas de TI e engenharia



- ✓ Avaliação da capacidade mínima requerida para os equipamentos que serão armazenados neste ambiente.
- ✓ Itens de segurança contra incêndios.
- ✓ Aspectos de contingência.
- ✓ Avaliação das opções de manutenção.

Gross, 2013, p. 85

Auditoria e Segurança da Informação

Segurança Ambiental:

Climatização

- ✓ Na implantação de uma instalação para ambientes de informações, o sistema central de condicionamento de ar é vital ao seu pleno funcionamento.

- ✓ Devido à necessidade do controle das condições ambientais e de confiabilidade para o sistema de condicionamento de ar, é recomendável a instalação de condicionadores do tipo compacto (*self-contained*) ou de central de água gelada.

- ✓ conveniente que a água de condensação, gerada pelo sistema de climatização, seja canalizada diretamente para um dreno capaz de suportar o volume máximo de água condensada pelo ar-condicionado, com uma folga de pelo menos 50%.

Gross, 2013, p. 85

Auditoria e Segurança da Informação

Segurança Ambiental:

Prevenção e combate a Incêndio

As instalações de um ambiente de informações, de acordo com Caruso e Steffen (1999, p. 220), devem ser projetadas de maneira que reduzam ao mínimo o risco de fogo na edificação ou em qualquer equipamento, dispositivo ou material que sirva para gerar ou propagar fogo.

quanto mais críticos forem os equipamentos para o negócio, mais investimentos em recursos devem ser efetuados, com um técnico de segurança avaliando a necessidade da utilização dos seguintes recursos:

- ✓ Uso de equipamentos para extinção automática.
- ✓ Uso de portas corta-fogo.
- ✓ Uso de alarmes de incêndio e detectores de fumaça.

Gross, 2013, p. 85

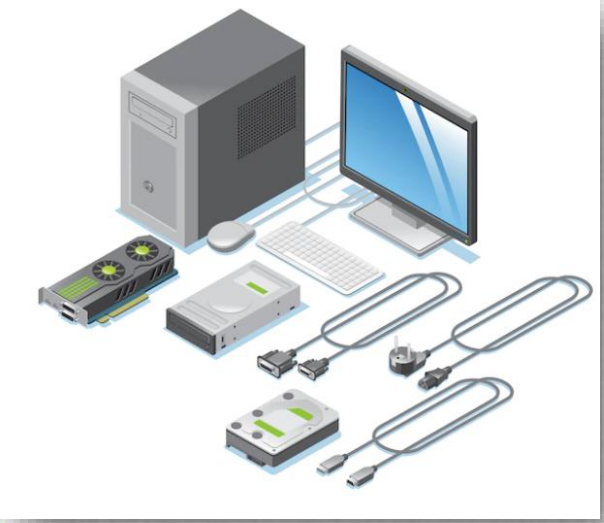
EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Ambiental:

Instalação, proteção e manutenção de equipamentos

A instalação de qualquer tipo de equipamento relacionado à TI deve ser precedida de uma avaliação do ambiente para reduzir o grau de exposição e acessos desnecessários, sabotagem, espionagem etc.



- ✓ Roubo
- ✓ Fogo
- ✓ Explosivos
- ✓ Fumaça
- ✓ Água
- ✓ Poeira
- ✓ Vibração
- ✓ Efeitos Químicos

Gross, 2013, p. 88

Auditoria e Segurança da Informação

Segurança Ambiental:

Instalação, proteção e manutenção de equipamentos

A adequada manutenção dos equipamentos é necessária para a garantia de sua integridade e disponibilidade.

A ISO 17799 (item 7.2.4) recomenda

a realização de manutenções de acordo com as especificações e os intervalos indicados pelo fabricante

uso de pessoal qualificado para a execução dos reparos, registro de falhas suspeitas e das manutenções corretivas e preventivas realizadas, controles apropriados para o envio de equipamentos para manutenções fora da organização

Gross, 2013, p. 88

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Ambiental:

Descarte de Equipamentos

Controles específicos devem ser implementados para evitar vazamento de informações, remoção não autorizada de propriedade e furto de equipamentos

- ✓ verificação da eliminação segura de informações sensíveis e de software licenciado de discos rígidos antes de sua transferência ou descarte
- ✓ inspeção de equipamentos retirados e devolvidos à organização e transporte de equipamentos portáteis em viagens sempre que possível como bagagem de mão e dentro de receptáculos que disfarcem seu conteúdo

Gross, 2013, p. 89

Auditoria e Segurança da Informação

Segurança Ambiental:

Proteção de Documento em Papel

Devem existir procedimentos que verifiquem os aspectos:

- ✓ Cópia;
- ✓ Armazenamento;
- ✓ Transmissão pelo correio ou *fax;*
- ✓ Descarte seguro*;*

Gross, 2013, p. 89

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação

Segurança Ambiental:

Proteção de Documento em Papel

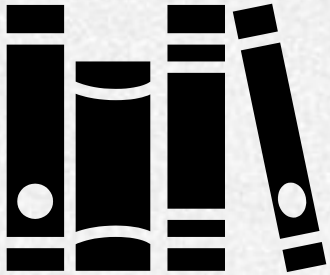
Caso a organização dependa de documentos em papel para cumprir sua missão e alcançar seus objetivos:

- ✓ Uso de rótulos para identificar documentos que requerem tratamento confidencial
- ✓ Política de armazenamento de papéis que assegure a guarda em local protegido (de preferência em cofre ou arquivo resistente a fogo) de papéis com informações confidenciais ou críticas para o negócio
- ✓ Procedimentos especiais para a impressão e transmissão via fax de documentos confidenciais (incluindo supervisão da impressora durante o processo de impressão e proteção contra discagem incorreta ou uso de números errados guardados na memória do aparelho de *fax*).
- ✓ Recepção e envio controlado de correspondência sigilosa.

Gross, 2013, p. 90

EDUCAÇÃO METODISTA

Auditoria e Segurança da Informação



Dias Claudia; Segurança e Auditoria da tecnologia da informação Claudia Dias Indaial : Editora Axcel Books, 2000

Gross, Christian Meinecke; Segurança em tecnologia da informação / Christian Meinecke Gross; Jan Charles Gross. Indaial : Uniasselvi, 2013.

Hintzbergen, Julie; Fundamentos de Segurança da Informação: Com base nas normas ISO 27001 e na ISO 27002 / Julie Hintzbergen, Kees Hintzbergen, André Smulders, Hans Baars; Tradução Alan Sá – Rio de Janeiro : Brasport, 2015

Imoniana, Joshua Onome; Auditoria de Sistemas de Informação / Joshua Onome Imoniana; 2. ed. – 2. reimpr; S;ao Paulo : Atlas, 2010

Lyra, Maurício Rocha; Governança da Segurança da Informação / Edição do Autor, 2015

Sêmola, Marcos; Gestão da Tecnologia da Informação: visão executiva da segurança da informação : aplicada a Security Officer / Marcos Sêmola e Módulo Security Solutions S.A. Rio de Janeiro : Elsevier, 2003 – 10ª reimpressão

Silva, Michel Bernardo Fernandes da, Cibersegurança uma visão panorâmica sobre segurança da informação na internet / Michel Bernardo Fernandes da silva. – Rio de Janeiro : Freitas Bastos, 2023.

EDUCAÇÃO METODISTA