Segurança Física e Lógica do Ambiente

Isledna Rodrigues

Antes de começar...

- Segurança física dos ativos é uma combinação de medidas de prevenção, detecção e reação.
- A ISO 17.799 é a principal norma de segurança em ambientes físicos.

CONCEITOS DA ISO 17.799

- Barreira de segurança: quaisquer medidas preventivas que impeçam ataques aos ativos da informação.
  - Físicas: muros, cercas trancas
  - Lógicas: senhas de logon

CONCEITOS DA ISO 17.799

- Perímetro de Segurança: contorno ou linha imaginária que delimita uma área ou região separada de outros espaços físicos por um conjunto qualquer de barreiras.
  - Ex: Prédios, geradores, cofres, etc.

Controles de Entrada Física

- Data e hora dos visitantes sejam registradas.
- Acesso restrito a áreas que processam ou armazenam informações sensíveis.
- Todos devem possuir identificação visível.
- Acesso a terceiros deve ser autorizado e monitorado.
- Direitos de acesso devem ser atualizados em intervalos regulares.

Segurança em Escritórios, Salas e Instalações

- As instalações-chave sejam localizadas de maneira a evitar o acesso ao público.
- Edifícios discretos que dêem a menor indicação possível de sua finalidade, fora ou dentro do edifício.
- Lista de funcionários e guias telefônicos internos devem ficar fora do acesso público.

Proteção contra ameaças externas e do meio Ambiente

- Materiais perigosos ou combustíveis devem ser armazenado distantes da área de segurança. Isso inclui material de papelaria.
- Equipamentos para contingência e mídia de backup fiquem a uma distância segura.
- Equipamentos para detecção e combate a incêndio sejam providenciados e posicionados corretamente.

Trabalhando em Áreas Seguras

- Pessoal só deve ter conhecimento das áreas seguras e trabalho nela realizado se for necessário.
- Seja evitado o trabalho não-supervisionado em áreas seguras.
- Áreas seguras não ocupadas sejam fisicamente trancadas e periodicamente verificadas.
- Não seja permitido equipamentos de gravação e filmagem.

Acesso do Público, áreas de entrega e carregamento

- Acesso restrito ao pessoal identificado e autorizado.
- Edifício deve permitir que entregadores possam descarregar sem ter acesso a outras áreas.
- Portas protegidas quando não houver entregas
- Materiais entregues devem ser inspecionados.
- Remessas entregues segregadas das remessas que saem.
- Materiais entregues devem ser registrado.

Segurança de Equipamentos

O objetivo é impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.

Instalação e Proteção do Equipamentos

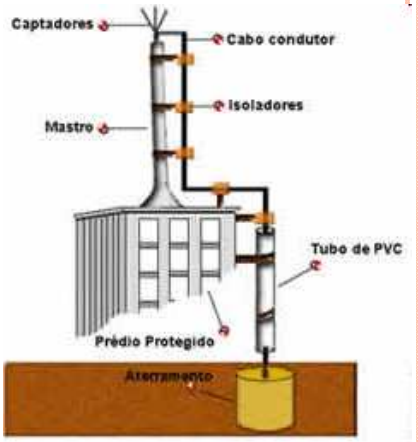
- Instalações de processamento de informações sensíveis posicionadas de forma que o ângulo de visão seja restrito.
- Sejam adotados controles para minimizar:
  - Furtos
  - Incêndios, Explosivos, Fumaça
  - Água, poeira, efeitos químicos
  - Radiação eletromagnética.

Instalação e Proteção do Equipamentos

- Diretrizes quanto a comer, beber e fumar nas proximidades das instalações.
- Condições ambientais para manter temperatura e umidade sejam controladas.

Instalação e Proteção do Equipamentos

- Edifícios e todas as linhas de entrada de forma tenham proteção contra raios.

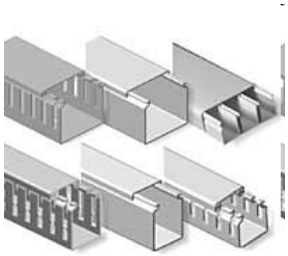
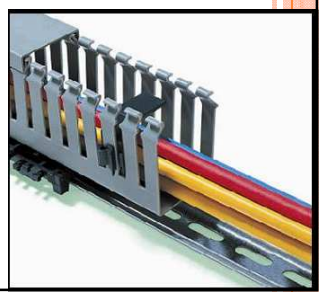


Instalação e Proteção do Equipamentos

- Em ambientes industriais outros equipamentos como membrana para teclado podem ser utilizados.

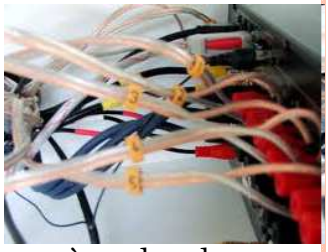
Segurança do Cabeamento

- Linhas de energia e telecomunicações que entram nas instalações devem ser subterrâneas ou ficar abaixo do piso.
- Cabeamento de rede protegido contra interceptação ou danos. Ex: uso conduites e canaletas.

Segurança do Cabeamento

- Cabos de energia separados/isolados dos cabos de comunicações.
- Usar marcações nos cabos.
- Para sistemas críticos:
  - Fibra-óptica
  - Blindagem dos cabos
  - Acesso controlado a painéis de conexões e às salas de cabos.
  - Varreduras técnicas e inspeções físicas para detectar a presença de dispositivos não autorizados.



Manutenção dos Equipamentos

- Manutenção realizada nos intervalos recomendados pelo fornecedor.
- Manutenção realizada por pessoal autorizado.
- Sejam mantidos registros de todas as falhas, suspeitas e operações de manutenção preventiva e corretiva.

Segurança de Equipamento fora das Dependências da Organização

- Não devem ficar sem supervisão em locais públicos.
- Computadores de mão devem ser carregados como bagagem de mão e disfarçados.
- Observada recomendações do fabricante.
- Controles para trabalho fora de casa:
  - Arquivos trancáveis
  - Política de "mesa limpa"
  - Comunicação segura com o escritório.

Remoção de Propriedade

- Equipamentos, informações ou software não sejam retirados sem autorização prévia.
- Funcionários, fornecedores e terceiros que possuam autorização sejam claramente identificados.
- Limites de tempo para retirada e devolução controladas.
- Registro da retirada ou devolução.

Controles contra Códigos Maliciosos

- Política formal para proibição de software não autorizado.
- Política formal para importação de arquivos.

Controles contra Códigos Maliciosos

- Instalar e atualizar regularmente software de detecção e remoção de códigos maliciosos.
  - Verificar antes de usar um arquivo.
  - Verificar antes de usar arquivos do correio.
  - Verificação em páginas WEB.

Controles contra Códigos Maliciosos

- Definir procedimentos de gerenciamento e responsabilidades para proteção, treinamento, reporte e recuperação a códigos maliciosos.
- Preparar planos de continuidade do negócio.
- Verificar regularmente novidades sobre códigos maliciosos.
- Implementar procedimentos para verificação da informações sobre códigos maliciosos.

Cópias de Segurança

- Definição do nível necessário de cópias de segurança.
- Produção de registros completos e exatos das cópias de segurança e procedimentos de restauração.
- A extensão (completa ou parcial) e a frequência das cópias reflita os requisitos da organização.

Cópias de Segurança

- Deve ser dado um nível apropriado de proteção física e ambiental das informações das cópias de segurança.
- Devem ser armazenadas em local distante.
- Devem ser testadas regularmente.
- Procedimentos de recuperação sejam verificados e testados regularmente.
- Podem ser protegidas através de encriptação.

MANUSEIO DE MÍDIAS

- Destruir mídias que não serão mais utilizadas.
- Manter registro de autorizações para remoção de mídias.
- Guardada de forma segura de acordo com especificações do fabricante.
- Duplicidade de mídias para informações que precisam durar muito tempo.
- Unidades de mídias removíveis habilitadas apenas se houver necessidade do negócio.

MANUSEIO DE MÍDIAS

- Pode haver serviços para implementar descarte seguro de papel, equipamentos e mídias magnéticas.

MENSAGENS ELETRÔNICAS

- Proteção contra acesso não autorizado, modificação ou negação de serviço.
- Assegurar que o endereçamento e o transporte da mensagem estejam corretos.
- Requisitos de assinaturas eletrônicas.
- Níveis mais altos de autenticação para acesso a partir de redes públicas.

EXERCÍCIOS

1) O "Teclado Virtual" é um mecanismo que na segurança de dados digitados através de páginas da web, comumente utilizado em sites de instituições bancárias. O "Teclado Virtual" é um importante agente no combate a um spyware, conhecido como:

(A) Adware
(B) Verme
(C) Key-logger
(D) Hijacker
(E) Sniffer

EXERCÍCIOS

2) O que chamamos de Engenharia Social?

3) Explique o que podemos fazer para evitar o sequestro de dados remotamente.

4) Quais os riscos, detalhadamente, de se acessar um site bancário usando uma rede e um PC públicos (LAN house)?

ENTREGA 1

Pesquisar sobre ferramentas, dispositivos e processos que poderiam ser utilizados para segurança nos laboratórios da UAST considerando os conceitos vistos em sala sobre engenharia social, segurança física e lógica.

REFERÊNCIAS

- LYRA, M. Segurança e Auditoria de Sistemas de Informação. Ed. Ciência Moderna. 2008.
- ABNT NBR ISO/IEC 17799:2005