UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança da Informação
# Aula 4 – Segurança Física e Lógica

Prof. Dr. Eng. Fred Sauer

fsauer@gmail.com

http://www.fredsauer.com.br

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Definições

- Segurança Física:
  - Realizada para evitar/dificultar as falhas nos equipamentos e instalações.
    - Ex: problema com equipamentos ativos, furtos, acidentes, etc.

Proteção dos ATIVOS

- Segurança Lógica:
  - Realizada para evitar/dificultar o uso inadequado de dados, programas e sistemas.
    - Ex: invasões hacker, roubo de dados.

Proteção da INFORMAÇÃO

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física

- Abrange todo o ambiente onde os sistemas de informação estão instalados:
  - prédio
  - portas de acesso
  - trancas
  - piso
  - salas
  - computadores
- Requer ajuda da engenharia civil e elétrica
- A norma NBR ISO/IEC 27002:2014 divide a área de segurança física da seguinte forma:
  - Áreas de segurança
  - Segurança dos equipamentos

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física ISO 27002

- Áreas (perímetros) de segurança
- Objetivo: Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização
  - Perímetro da segurança física
  - Controles de entrada física
  - Segurança em escritórios, salas e instalações
  - Proteção contra ameaças externas e do meio ambiente
  - Trabalhando em áreas seguras
  - Acesso do público, áreas de entrega e de carregamento

# Segurança Física ISO 27002

- Segurança dos equipamentos
- Objetivo: Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.
  - Instalação e proteção de equipamentos
  - Utilidades (fornecimento de energia e/ou outros ativos de serviço)
  - Segurança do cabeamento
  - Manutenção de equipamentos
  - Segurança de equipamentos fora das instalações
  - Reutilização e alienação segura de equipamentos
  - Remoção de propriedade

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
# Segurança Externa e de entrada

- Proteção da instalação onde os equipamentos estão localizados, contra:
  - entrada de pessoas não autorizadas
  - catástrofes ambientais
- O prédio deve ter paredes sólidas e número restrito de entradas e saídas
- Evitar baixadas onde a água possa se acumular → enchentes
- Evitar áreas muito abertas → descargas atmosféricas
- Em qualquer lugar, usar para-raios
- Usar muros externos e manter a área limpa → queimadas

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física

## Segurança Externa e de entrada

- Controle de acesso físico nas entradas e saídas:
  - travas
  - alarmes
  - grades
  - vigilante humano
  - vigilância eletrônica
  - portas com senha
  - cartão de acesso
  - registros de entrada e saída de pessoas e objetos
- Funcionários que trabalham na instituição devem ser identificados com crachás com foto
- Visitantes devem usar crachás diferenciados por setor visitado
- Todos funcionários devem ser responsáveis pela fiscalização

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
## Segurança da Sala de Equipamentos

- Agrega todo o centro da rede e os serviços que nela operam.
- Entrada somente de pessoal que trabalha na sala.
- Registro de todo o pessoal que entra e sai.
- A sala deve ser trancada ao sair.
- Deve fornecer acesso remoto aos equipamentos.
- O conteúdo da sala não deve ser visível externamente.
- Além do acesso indevido, a sala deve ser protegida contra:
  - vandalismo
  - fogo
  - interferências eletromagnéticas
  - fumaça
  - gases corrosivos
  - poeira

# Segurança Física

## Segurança da Sala de Equipamentos

- Uso de salas-cofre

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
# Segurança dos equipamentos

- Evitar o acesso físico aos equipamentos
  - acesso ao interior da máquina (hardware)
  - acesso utilizando dispositivos de entrada e saída (console)
- Proteger o setup do BIOS
- Tornar inativos botões de setup e liga/desliga no gabinete
  - colocar senha no BIOS
  - inicialização apenas pelo disco rígido

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
# Segurança do ambiente

- Geralmente o fornecimento de energia é de responsabilidade da concessionária, e pode apresentar:
  - variação de tensão
  - interrupção do fornecimento

- Para garantir a **disponibilidade** da informação é preciso garantir o fornecimento constante de energia e que ela esteja dentro da tensão recomendada
  - *Nobreak*
  - Gerador

- Refrigeração

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
# Segurança do ambiente

- Norma TIA 942
  - Define padrões de disponibilidade e redundância de equipamentos.
  - 4 níveis de confiabilidade (TIERs)

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
# Segurança do ambiente

- TIER-1
  - Sem redundância de equipamentos e infraestrutura de distribuição (caminho único não redundante).
  - Disponibilidade >= 99,671 % (29hs de indisponibilidade/ano)

- TIER-2
  - Atende TIER-1
  - Redundância de infraestrutura suficiente para atingir disponibilidade >= 99,741% (22hs de indisponibilidade/ano)

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
# Segurança do ambiente

- TIER-3
  - Atende ao TIER-2
  - Todos os equipamentos de TI com alimentação redundante e 100% compatíveis com a arquitetura do local.
  - Caminhos múltiplos de distribuição atendendo aos equipamentos de TI.
  - Disponibilidade >= 99,982% (94 mins de indisponibilidade/ano)

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Física
# Segurança do ambiente

- TIER-4
  - Atende ao TIER-3
  - Equipamentos de refrigeração/ventilação/aquecimento (HVAC) redundante e com alimentação redundante.
  - Infraestrutura tolerante a falhas, armazenamento e distribuição de energia elétrica redundante.
  - Disponibilidade >= 99,995% (26 mins de indisponibilidade/ano)

# Segurança Física
# Segurança do ambiente

**No-Break (UPS)**

- Alimenta os equipamentos até o gerador estar disponível.
- Utiliza baterias.
- Autonomia limitada.

# Segurança Física
# Segurança do ambiente

**Banco de baterias**

- Alimentam o no-break.

- Sobre baterias, lembre-se:
  - São caras.
  - Vida útil limitada.
  - Devem ser monitoradas.
  - Descarte ecológico.

# Segurança Física
# Segurança do ambiente

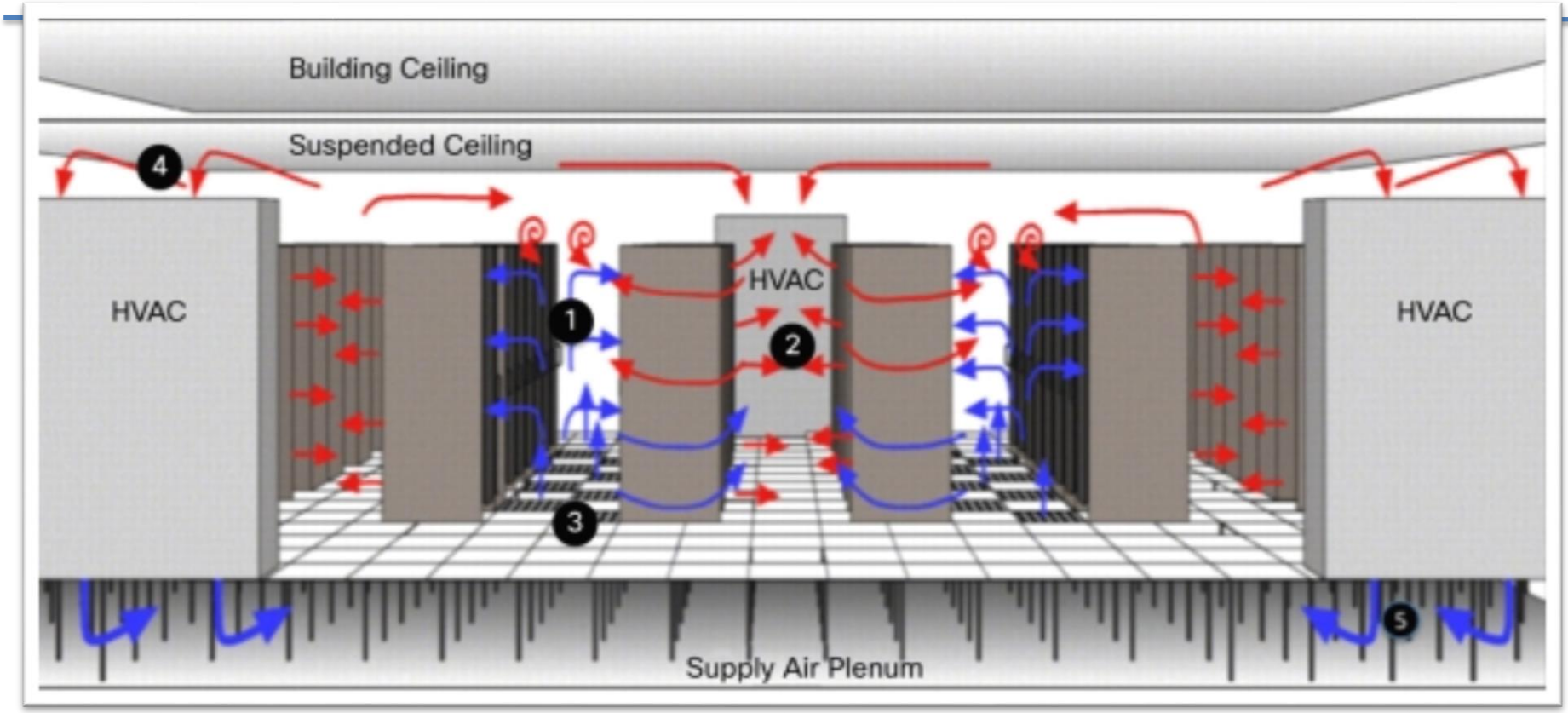
**Gerador**

- Diesel
- Gás natural

- Requer manutenção constante.

- Partida
  - Manual
  - Automática.
- Local de instalação:
  - Exaustão de gases.
  - Ruído.
  - Abastecimento.
  - Armazenamento de combustível.

# Segurança Física
# Segurança do ambiente




- Fluxo de ar em um *datacenter*.

# Segurança Física
# Segurança do ambiente

- Combate a incêndios

➢ Detecção
  - Sensores de fumaça convencionais.
  - *Very early smoke detection apparatus* (VESDA)
    - Detecção por aspiração (dutos que percorrem a área).
  - Botão de acionamento manual.

➢ Combate
  - Extintores convencionais.
  - Chave para desligamento de emergência.
  - Dispersão de gases
    - Água pode apagar um incêndio, mas não é conveniente num datacenter (sprinklers).
    - Gases extintores como NOVEC 1230, FM-200, FE-25 e INERGEN

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

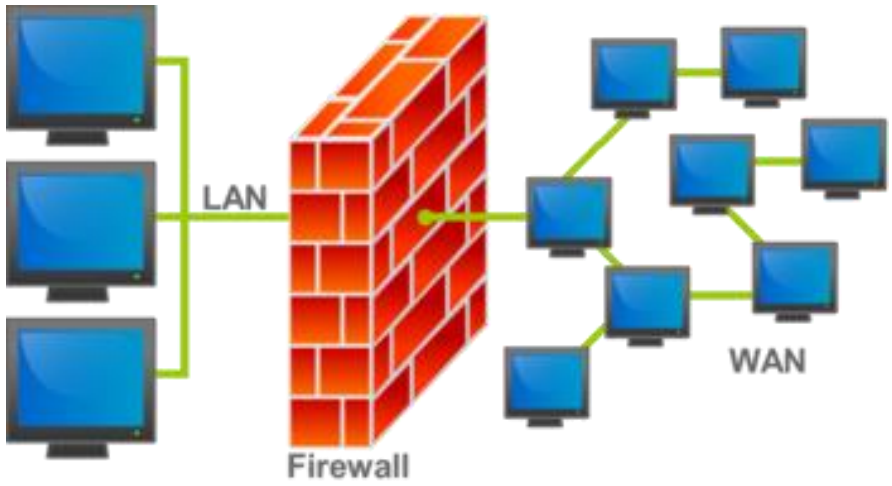
# Segurança Lógica

- Compreende os mecanismos de proteção baseados em software
  - senhas
  - listas de controle de acesso
  - criptografia
  - firewall
  - sistemas de detecção de intrusão
  - redes virtuais privadas

# Segurança Lógica
# Firewall

- Referência às portas corta-fogo responsáveis por evitar que um incêndio em uma parte do prédio se espalhe facilmente pelo prédio inteiro

- Na Informática: previne que os perigos da Internet (ou de qualquer rede não confiável) se espalhem para dentro de sua rede interna



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Lógica
# Firewall

- Um firewall deve sempre ser instalado em um ponto de entrada/saída de sua rede interna.
- Este ponto de entrada/saída deve ser único.
- O firewall é capaz de controlar os acessos de e para a sua rede.
- Objetivos específicos de um firewall:
  - restringe a entrada a um ponto cuidadosamente controlado.
  - previne que atacantes cheguem perto de suas defesas mais internas.
  - restringe a saída a um ponto cuidadosamente controlado.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Lógica
# Firewall

- O firewall pode estar em:
  - computadores
  - roteadores
  - configuração de redes
  - software específico

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Lógica
# Detectores de intrusão

- IDS – (*Intrusion Detection Systems*): responsáveis por analisar o comportamento de uma rede ou sistema em busca de tentativas de invasão
  - HIDS – (*Host IDS*):
    - monitora um host específico
  - NIDS – (*Network IDS*):
    - monitora uma segmento de rede
- Um IDS utiliza dois métodos distintos:
  - detecção por assinaturas
  - detecção por comportamento

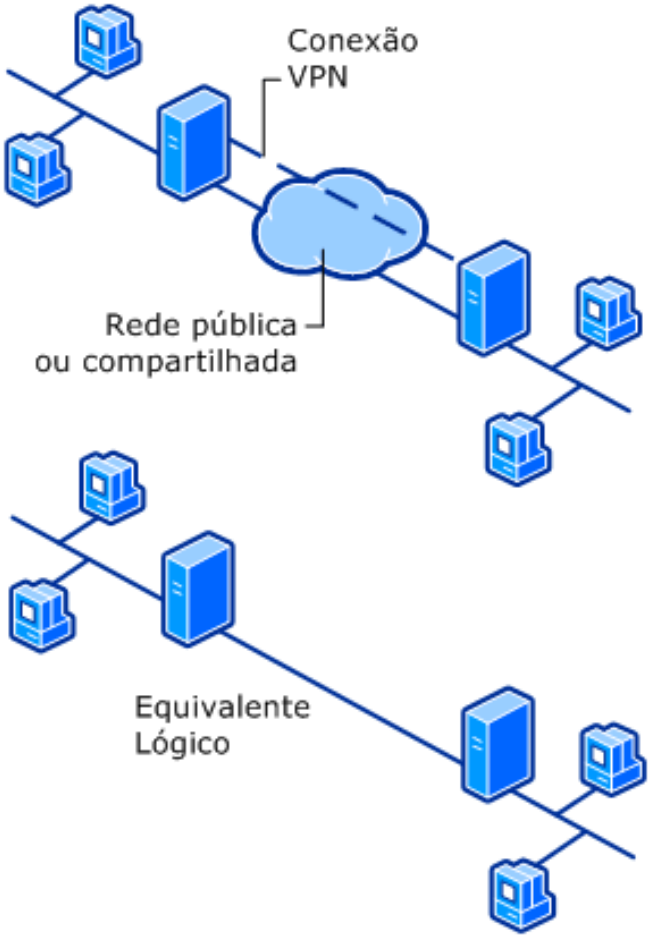
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Lógica
# Detectores de intrusão

- Detecção por assinaturas:
  - semelhante às assinaturas de antivírus associam um ataque a um determinado conjunto de pacotes ou chamadas de sistema
  - não só detecta o ataque como também o identifica
  - exige atualizações frequentes do fabricante
- Detecção por comportamento:
  - observa o comportamento da rede em um período normal, e o compara com o comportamento atual da rede
  - diferença significativa entre os comportamentos, o IDS assume que um ataque está em andamento
  - utiliza métodos estatísticos ou inteligência artificial
  - detecta ataques desconhecidos
  - não sabe informar qual ataque está em andamento

# Segurança Lógica
# VPN (Virtual Private Networks)

- VPN – (Virtual Private Networks):
  - Forma barata de interligar duas redes privadas (Intranet) através da Internet.
  - Permite usar uma rede não confiável de forma segura.
  - Exemplos:
    - Ligação entre dois firewalls ou entre dois servidores de VPN para interligar duas redes inteiras
    - Ligação entre uma estação na Internet e serviços localizados dentro da rede interna (Intranet)



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Propriedades das conexões VPN

- **Encapsulamento**
  - Contém informações de roteamento que permitem que os dados atravessem a rede de tráfego.
- **Autenticação**
  - Autenticação no nível do usuário.
  - Autenticação no nível do computador.
  - Autenticação da origem dos dados e integridade dos dados.
- **Criptografia de dados**
  - Garante a confidencialidade dos dados que atravessam a rede de tráfego pública ou compartilhada.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança Lógica
# VPN (Virtual Private Networks)

- VPN emprega criptografia em cada pacote trafegado
  - A criptografia deve ser rápida o suficiente para não comprometer o desempenho entre as redes.
  - A criptografia deve ser segura o suficiente para impedir a quebra de confidencialidade.
- Para cada pacote trafegado é verificado
  - A integridade (CRC ou Hash – será visto posteriormente).
  - A autenticidade: pacotes carregam assinaturas/senhas para garantir a veracidade da fonte emissora.
- Exemplos de protocolos de encapsulamento empregados
  - IPSec (RFC 3193)
  - L2TP (RFC 2661/ RFC 3193)
  - PPTP (RFC 2637)
  - SSTP

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Fixação

- Ao instalar um dispositivo biométrico na porta do datacenter, é segurança ___FÍSICA___. Ao instalar um antivírus, é segurança ___LÓGICA___.
- Os datacenter são classificados em TIERS, quanto MENOR o Tier, ___MENOR___ a sua resistência a incidentes.
- Um IDS que usa um arquivo com trechos de malwares conhecidos opera por ___ASSINATURAS___. O que se baseia no comportamento do programa suspeito opera por _____.
- Uma VPN é um recurso barato que oferece ___ENCAPSULAMENTO___, ___CRIPTOGRAFIA___ e ___AUTENTICAÇÃO___.