Prime

CCS-A

Segurança Física

O Valor da Segurança Física

- Sem segurança física, os outros controles podem ser ignorados por hackers.
- Todos os sistemas críticos devem ser colocados em um lugar seguro (sala de servidores):

Monitore quem sai e entra da sala.

Insira os equipamentos em um rack.

Tranque os racks.

Trave ou tranque a tampa no chassi/blade.

Considere as questões de segurança em torno do edifício.

Preocupações com a Instalação

Observe a taxa de criminalidade da área do local.

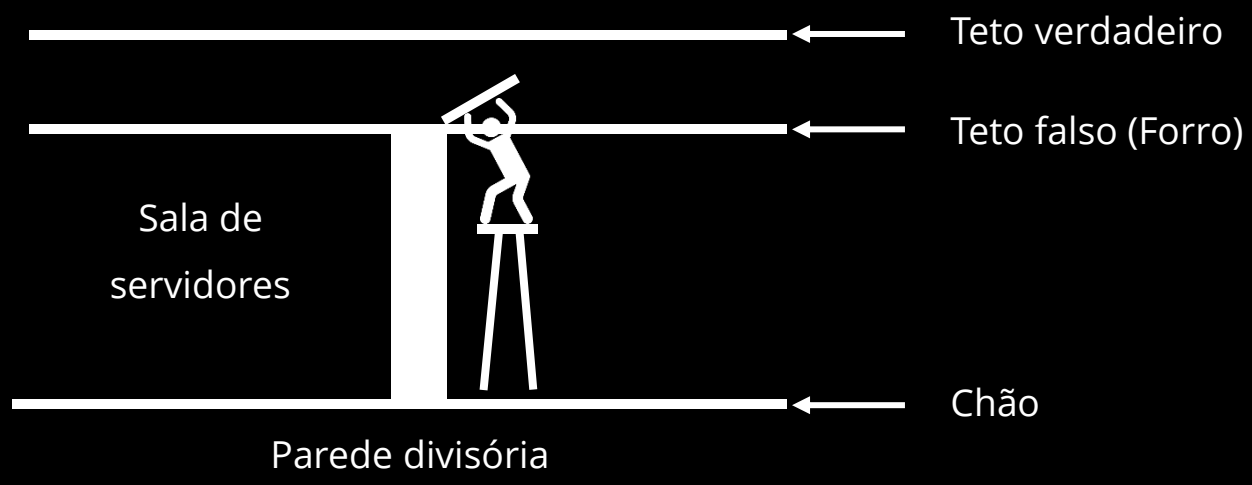
Preocupe-se com inundações ou desastres naturais.

Veja o tempo para serviços de emergência, ambulância, bombeiros, polícia etc.

Iluminação e Janelas

- Instalação de luz de emergência com fonte de alimentação de backup.
- Mantenha baterias para fontes de emergência para ajudar na evacuação do prédio.
- Iluminação externa para prevenir atividades não autorizadas.
- Avalie a utilização de janelas para fácil observação.
- Invista em janelas com telas de arame ou barras.
  - Proteja contra o ataque ***shoulder surfing***.
  - Suficiente para visualizar, mas não o que digitam.

Portas e Paredes



Exemplo de Sensores (inclusive nos dutos):

- Sensor de circuito fechado;
- Tapete de sensor de pressão;
- Sensor de proximidade;
- Sensor fotoelétrico do transmissor para o receptor.

- Utilize porta com barras antipânico com dobradiças seguras.

Preocupações de Segurança

Componentes de segurança física que adicionam segurança:

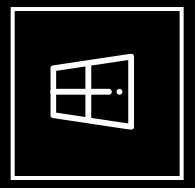
- Sinais, como saídas de emergência;
- Rota de fuga, em caso de incêndio;
- Planos de fuga bem comunicados;
- Simulações;
- Controles de testes de extintores, alarmes etc.

Controles de Acesso Físico

Um hacker pode ignorar a segurança de um sistema se puder acessar fisicamente um sistema.

A maioria dos hackers que ignoram a segurança do SO inicializa o ataque a partir de um CD ou USB.

Garanta o controle do acesso físico aos ativos para evitar que seja atacado.



A segurança física é importante para impedir acessos não autorizados a sistemas e redes.

Fencing e Pessoal

- Primeira linha de defesa em segurança física: Perímetro das instalações.
- Controle quem tem acesso à propriedade, mesmo antes de chegar ao prédio.
- Dois métodos:
  - Cercas;
  - Guardas.

Cerca de Perímetro

Força qualquer pessoa a acessar uma instalação pelos portões principais.

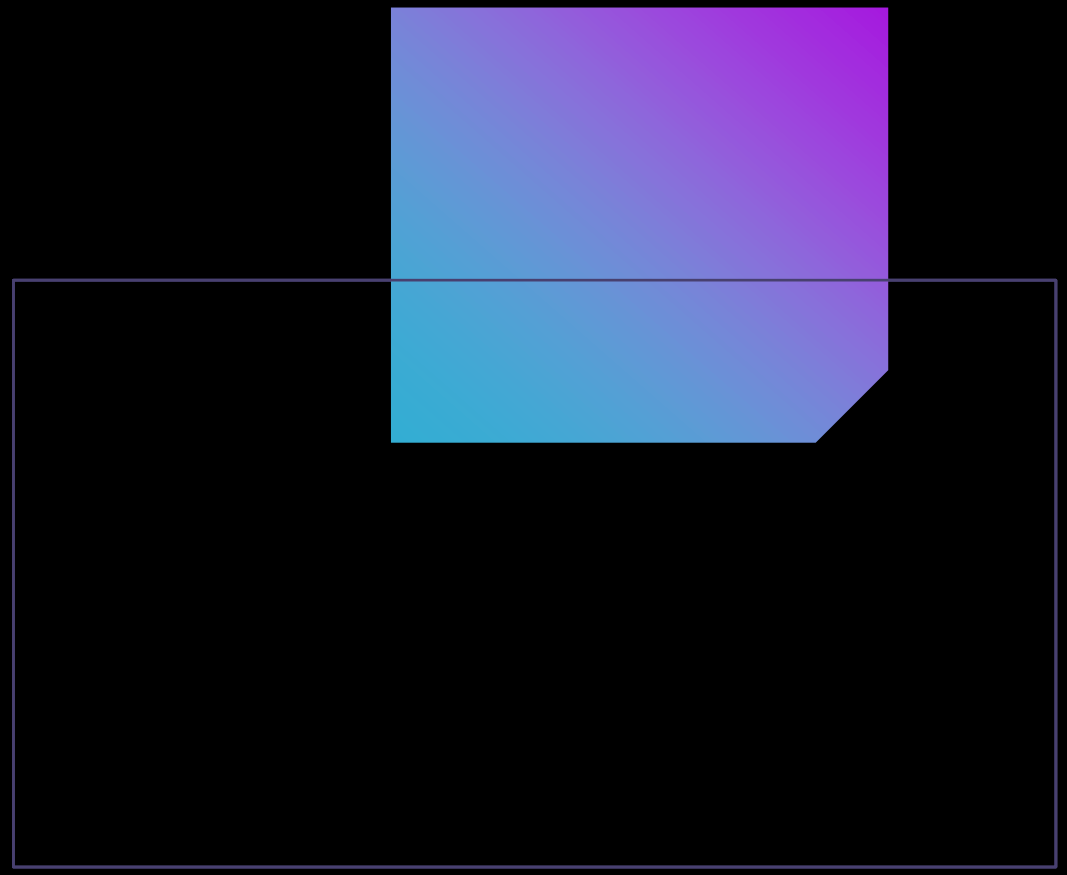
Intruso casual = Uso de uma cerca de 1m de altura.

Alpinista casual = Uso de uma cerca de 1,5 a 2m.

Intruso determinado = Uso de uma cerca de 2,5m, mais três linhas de arame farpado no topo, inclinadas em um ângulo de 45 graus para fora do edifício.

Guardas

- Com uma cerca de perímetro, é preciso de guardas que vigiem quem entra e sai.
- No portão, verificar se um visitante é esperado.
- Dentro, exibir o crachá de identificação de funcionário.
- Na saída, o guarda do portão deve garantir que nenhum equipamento foi roubado.
- Adicionar guardas tem a vantagem de verificar uma atividade anormal.
- Dependendo do nível de segurança, é preciso posicionar guardas em toda a instalação.



Robôs Sentinelas e Recepção

- Manter guardas 24x7 pode ser caro.

Robôs podem:

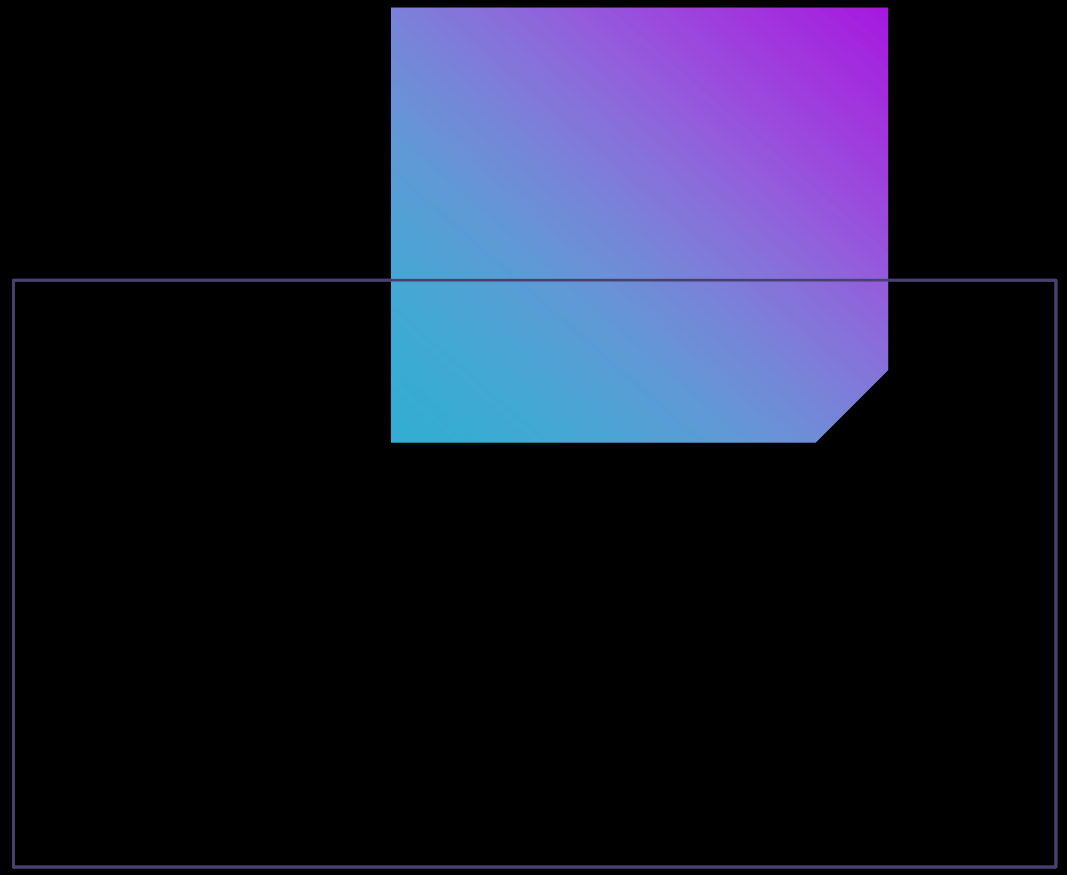
- Patrulhar as instalações e capturar vídeo, mesmo vazios;
- Detectar movimentos que podem enviar notificações para algum telefone.

Na recepção:

- Obrigatoriedade de check-in anterior;
- Espera para que a pessoa do contato busque-a;
- Inserção de um crachá de visitante.

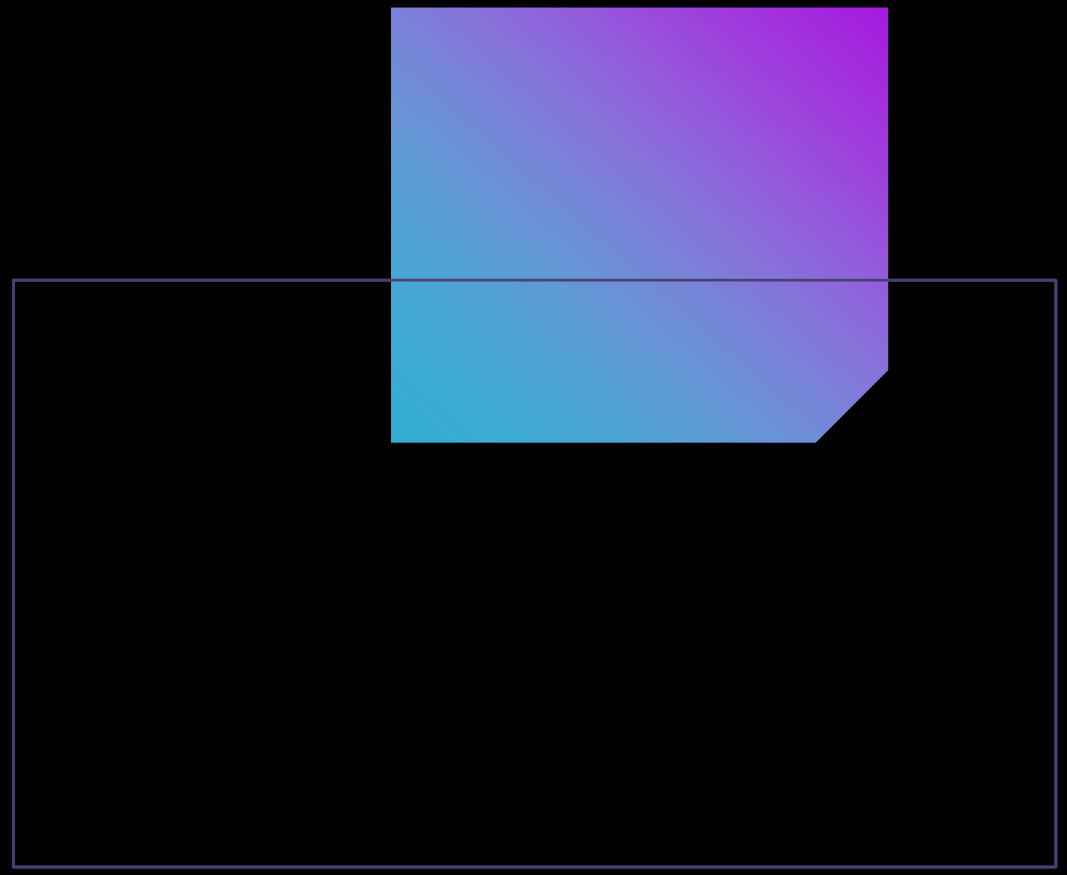
Integridade/Controle de Duas Pessoas (TPI)

- Aplica-se o princípio de Separação de Funções.
- Duas pessoas presentes em um determinado acesso.
- Cada pessoa valida se os procedimentos de segurança estão sendo seguidos.
- Exemplo para acesso ao visitante:
  - A primeira pessoa **inicia o processo de verificação e cadastro de um visitante.**
  - A segunda **controla o acesso à porta.**



Fechadura e Cadeados

- Portas são suscetíveis a arrombamento com chave micha (*Lock-picking tools*).
- A maioria das empresas usa **sistemas de travamento eletrônico.**
- Com uma **fechadura eletrônica,** os funcionários acessam as salas via token.
  - Também são conhecidas como **fechaduras de cifra.**
- Áreas trancadas podem ser acessadas via **biometria**.
- Tipo diferente de trava: **Trava de cabo nos desktops.**



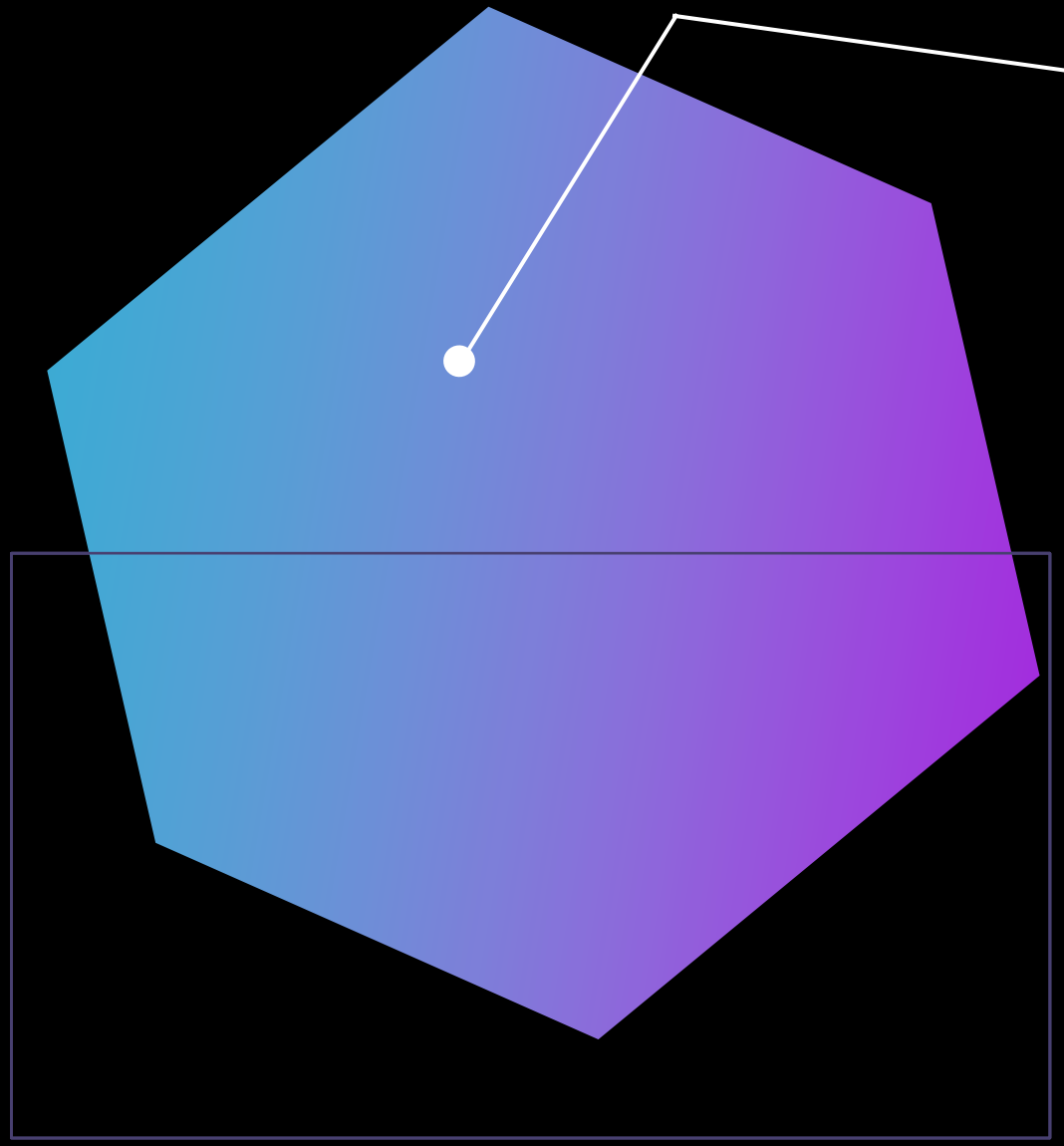
Crachás de Identificação

Crachás de identificação com **nome e foto**.

- Diferencia o visitante do funcionário.
- Os funcionários também são obrigados a usar em local visível.
- Pode haver RFID no crachá para registrar os movimentos.
- Uma tarja magnética pode servir para abrir portas.
- Pode conter um certificado digital para controlar o acesso a sistemas e recursos.

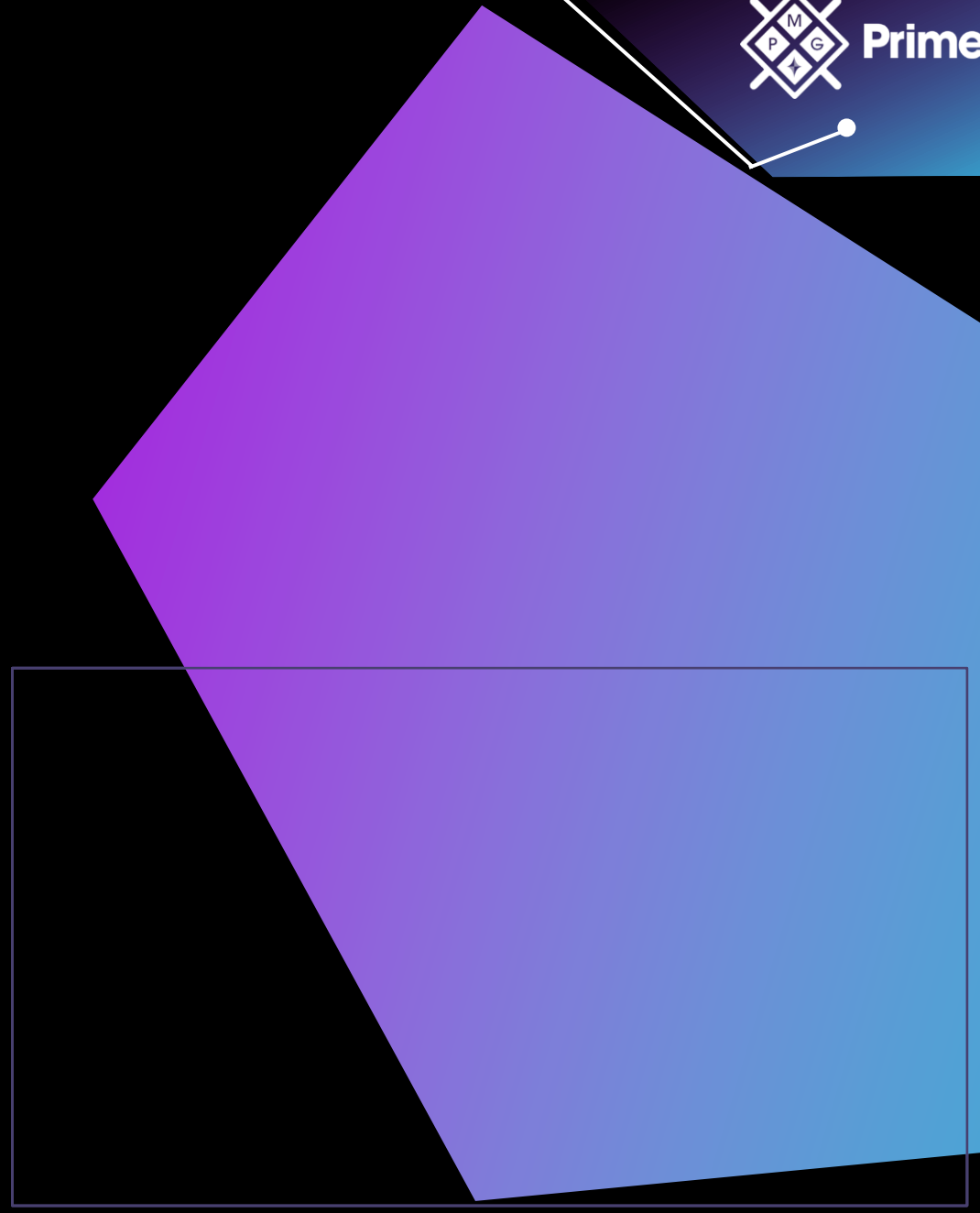
Tokens Físicos e Leitores de Proximidade

- Token físico - Colocado em um chaveiro (Key fobs) do funcionário e carregado o tempo todo.
  - Podem receber tokens que contêm códigos de acesso.
- Leitor de proximidade - Lê o código de acesso de um token ou cartão.
  - Dois tipos principais de leitores:
    - Ativados pelo usuário com a digitação de um código ou a passagem do cartão no leitor;
    - De proximidade com detecção automática.



Armadilhas (*Mantrap*)

- Área entre duas portas, com a segunda porta não abrindo até que a primeira esteja fechada.
- Evita o *piggybacking* e o *tailgating*.
  - Piggybacking – Quando um invasor entra em uma instalação atrás de um membro do time, com o conhecimento desse mesmo membro.
  - Tailgating – O mesmo ato, mas sem o conhecimento do membro do time.
- A área da armadilha pode ter uma janela segura, com o monitoramento de um segurança.
- Armadilhas giram em forma de C.



Áreas Seguras

- Áreas seguras comuns usadas pelas organizações:
  - Entreferro;
  - Cofre;
  - Armários/Gabinetes seguros;
  - Sub-rede rastreada (zona desmilitarizada).

Áreas Seguras

- Vários outros controles de segurança podem ser implementados:


Sinalização;


Alarmes;


Travas de cabo;


Filtros de tela;

Gerenciamento de chaves e logs;


Barricadas;


Biometria;


Distribuição de cabos protegida;


Camuflagem industrial.

Bloqueador de Dados USB

- Risco: um usuário de smartphone pode conectar seu dispositivo móvel a qualquer dispositivo para carregá-lo.

Se a estação for maliciosa, ela roubará os dados ou infectará o smartphone.

- Bloqueador de dados USB - Importante para a segurança.

Impede o acesso do smartphone, criando uma barreira entre a estação e o smartphone.

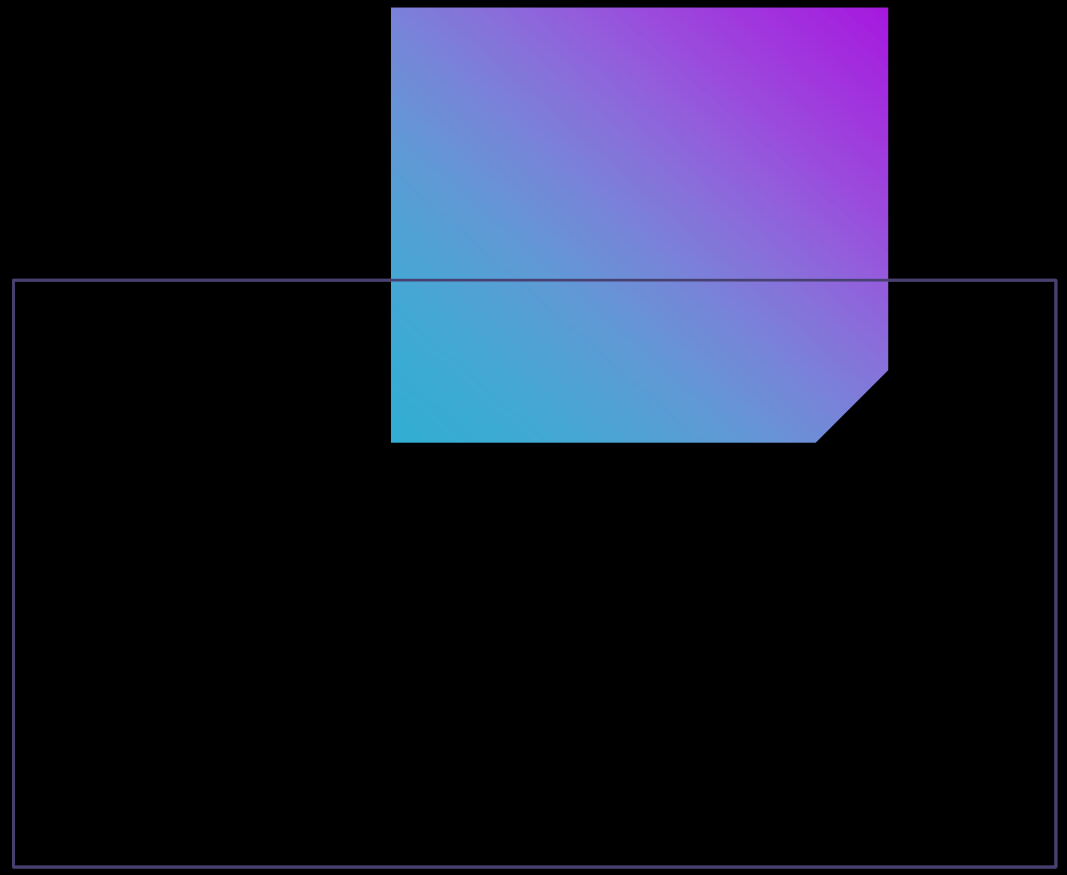
Destruição Segura de Dados

- É preciso garantir que alguém não tenha acesso aos dados armazenados após desativá-los ou descartá-los.
- Algumas opções para descarte de dados são:

Queimar;	Destruir;
Despolpar;	Pulverizar;
Desmagnetizar;	Limpar;
Enxugar;	Soluções de terceiros.

Listas e Logs de Acesso Físico

- Quando uma lista de acesso é criada, o sistema nega todo acesso à instalação, exceto se um código for fornecido.
- Os controles de acesso permitem:
  - Acesso a uma área;
  - Registro de quem obteve acesso.
- É preciso manter registros de visitantes na entrada, como:
  - Nome;
  - Empresa;
  - Número de telefone;
  - Propósito da visita;
  - Pessoa de contato.



Vídeo Vigilância

- A segurança física lida com a implementação de circuito fechado de televisão (CCTV).
- Os sistemas de monitoramento atuais são avançados porque agora é possível se conectar à câmera pela Internet.
- Opções populares para monitoramento de vídeo:


Câmeras falsas;


Câmeras ocultas;


Câmeras de visão noturna;


Câmeras sem fio;


Reconhecimento/detecção de movimento;


Detecção de objetos.

Drones e Tipos de Sensores

- Drones são ferramentas comuns de monitoramento.
- Controlados remotamente e gravam imagens de cima.
- Tipos de sensores:
  - Detecção de movimento;
  - Leitor de proximidade;
  - Cartões;
  - Temperatura;
  - Detecção de umidade.

Entendendo o HVAC

- HVAC - Sistema para fornecer ou reduzir o calor, a umidade e o ar externo.
- Ajuda os sistemas de computador a funcionar de forma otimizada.
- Níveis de umidade devem estar entre 40 e 60%.

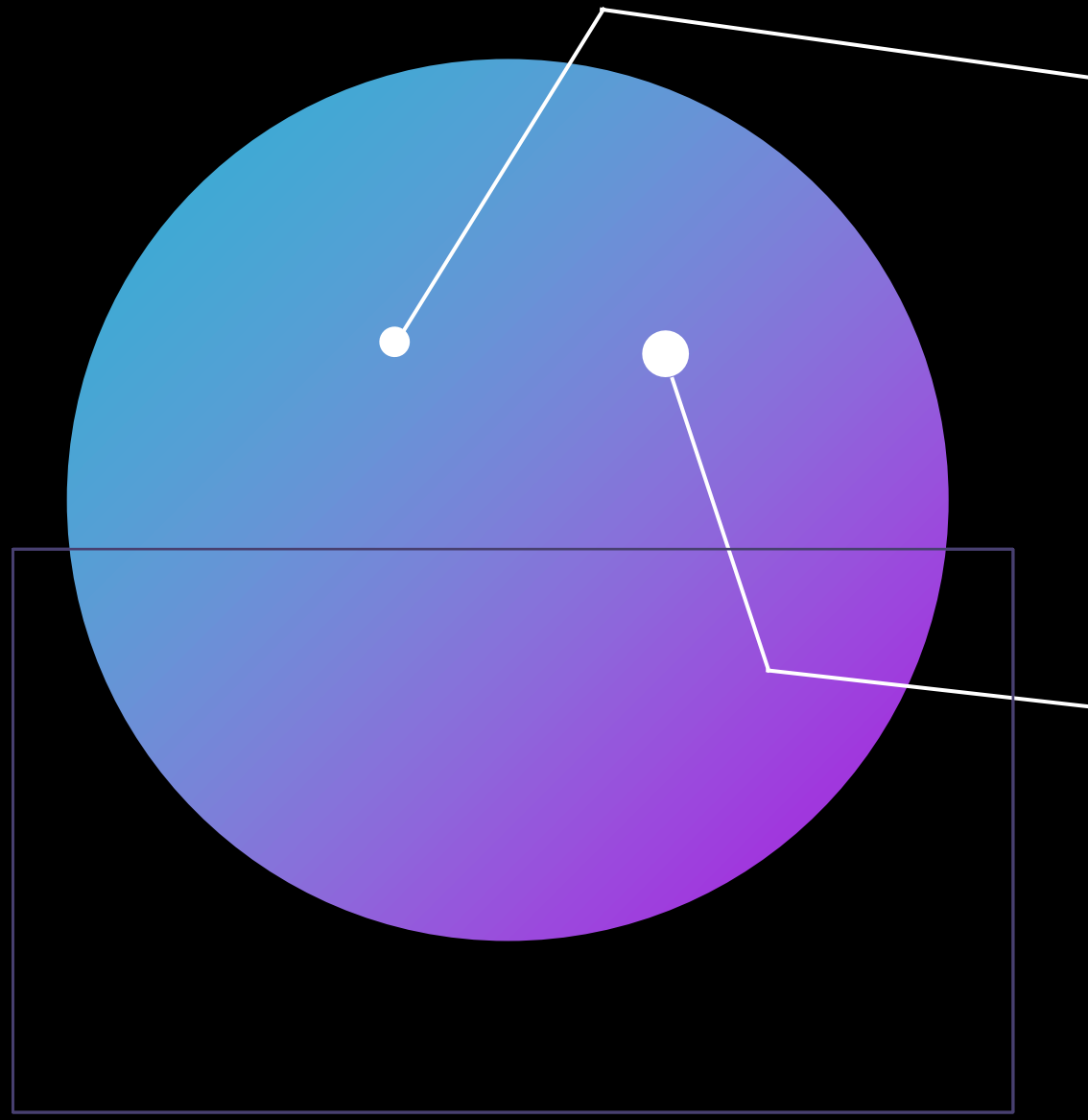
<40%	Abaixo de 40% - Descarga eletrostática.
>60%	Acima de 60% - Prejudica os componentes do computador.

- Alguns componentes de HVAC incluem:

	Monitoramento ambiental;
	Corredores quentes e frios;
	Controles de temperatura e umidade.

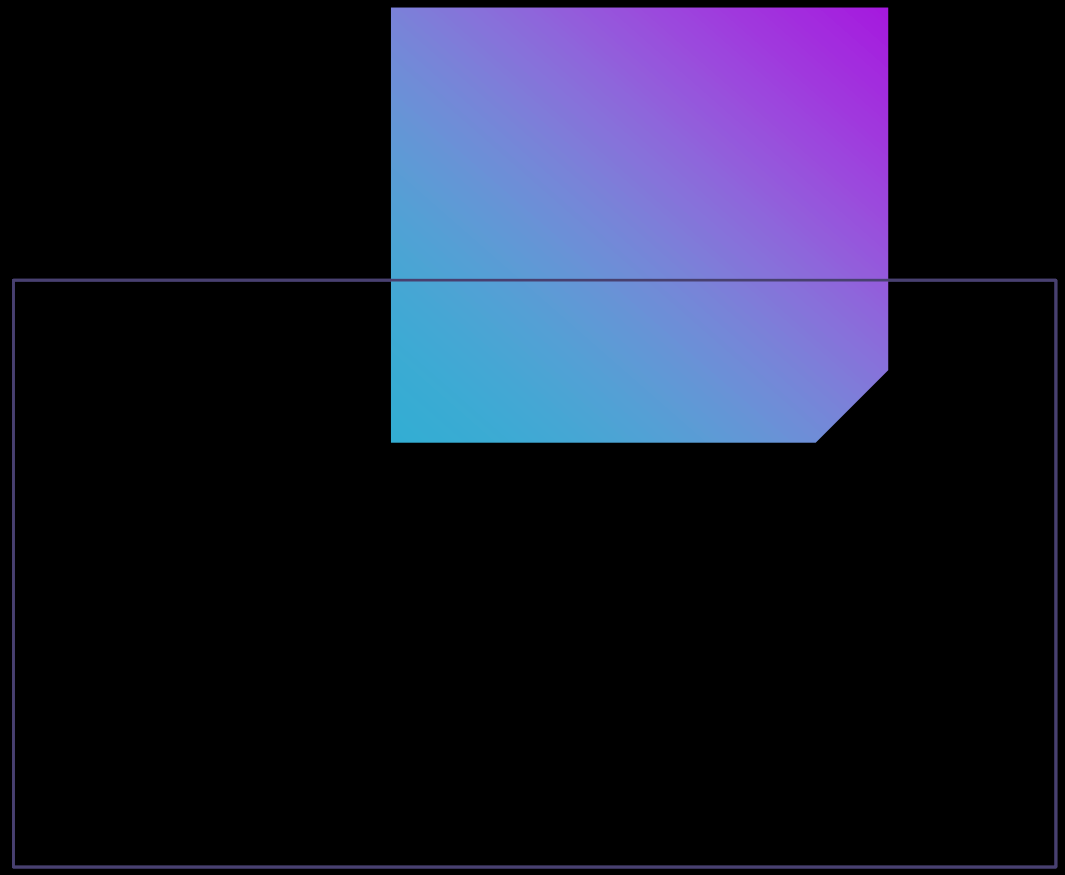
Blindagem

- É preciso garantir que as informações não sejam recebidas por pessoas não autorizadas por meio de emanações.
- Emanações - Emissões de sinais elétricos de componentes do computador.
  - Emissões podem ser interceptadas e analisadas por receptores.
- A blindagem impede que o sinal viaje para fora de uma determinada área.
- Ambiente blindado – TEMPEST
- É possível implementar a proteção contra interferência eletromagnética (EMI).



Contenção do Fogo

- Configure o dispositivo de detecção para fazer uma chamada para o corpo de bombeiros.
- Desligue o HVAC da solução de detecção de incêndio.
- Tipos de incêndios:
  - Classe A - Combustíveis comuns;
  - Classe B - Incêndios líquidos;
  - Classe C – Queima de componentes e equipamentos elétricos;
  - Classe D – Queima de metais combustíveis.



OBRIGADO!

SEGURANÇA FÍSICA