Prime

ISF – CONTROLES FÍSICOS DA SEGURANÇA DA INFORMAÇÃO

Segurança Física

Segurança física faz parte da segurança da informação, porque todos os ativos da empresa devem ser fisicamente protegidos

A fim de detectar qualquer invasão, a segurança física usa vários tipos de sensores, como:

Detecção passiva por infravermelho: Detectam mudanças de temperatura a uma dada distância do sensor (Detecção de Intrusão).

Câmeras: Gravam imagens que podem ser posteriormente visualizadas. Alguns softwares inteligentes permitem que verificações automáticas sejam realizadas.

Detecção de vibração: Detectar passos.

Sensores de quebra de vidro: Detectam quando uma janela foi quebrada.

Contatos magnéticos: Detectam quando uma porta ou janela é aberta.

Medidas de Segurança Física

- Segurança Física emprega uma combinação de medidas organizacionais, estruturais e eletrônicas;
- Medidas de Segurança Física precisam ser planejadas e coordenadas de forma coerente.

Exemplos:

- Proteção dos equipamentos através do controle de temperatura (ar condicionado, umidade);
- Cabos devem ser instalados de tal forma que evitem interferências. A interferência ocorre quando os cabos captam ruídos e estática de cabos de energia que estão próximos;
- A exclusão de Informação Confidencial na mídia de armazenamento quando uma pessoa deixa a organização.

Medidas de Segurança Física

Anéis de Proteção:

- A área ao redor do prédio;
- O edifício;
- O espaço de trabalho;
- Os objetos.

Alarmes:

- Sensores;
- Monitoramento;
- Proteção contra incêndio;
- **Planos:**
- Plano de Emergência;
- Plano de Contingência.

Controle: Perímetros de Segurança Física

Objetivo:

Evitar acesso físico não autorizado, danos e interferência nas informações da organização e outros ativos associados.

Como proteger o perímetro fisicamente?

- Criando uma ou mais barreiras físicas ao redor das instalações;
- Pode ser um escritório com chave ou várias salas cercadas por uma barreira.

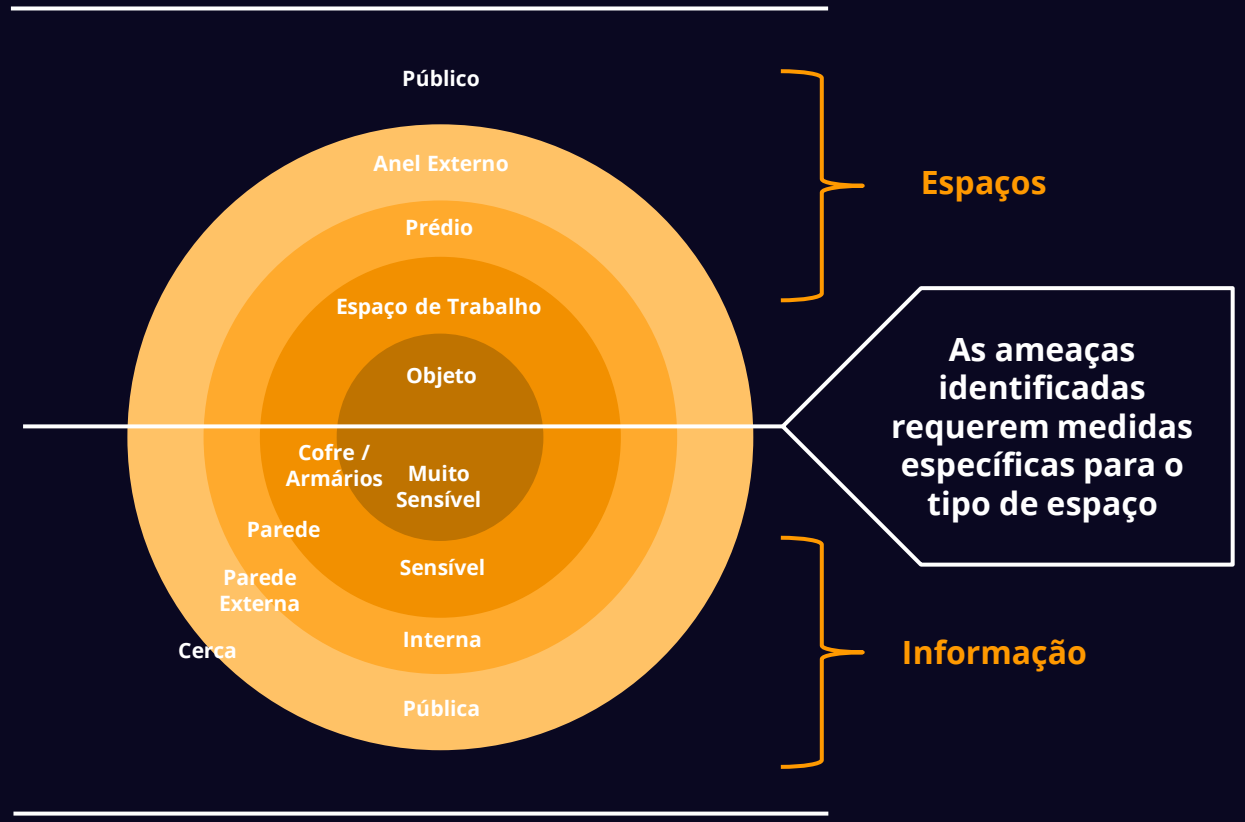
Controle: Perímetros de Segurança Física

Quais diretrizes seguir ao definir os perímetros?

- Perímetros de segurança;
- Localização e resistência de cada um dos perímetros;
- Todos de acordo com os requisitos de segurança da informação;
- Ter perímetros fisicamente sólidos para um edifício ou local;
- Garantir que não haja lacunas ou áreas de arrombamento;
- Cobrir áreas externas, paredes, janelas, portas, tetos e pavimentos;
- Manter áreas adequadamente protegidas contra acesso não autorizado com mecanismos de controle (por exemplo, barras, alarmes, fechaduras);
- Considerar o nível do solo e pontos de ventilação;
- Alarmar, monitorar e testar todas as portas corta-fogo.

ISO 27001

Perímetros de Proteção



Anel Externo

Construções

Acessos Físicos

Uma análise de riscos determina o nível de medidas necessárias, exemplo:

Empresa Privada:

Acesso mais restritivo
- Indústria Química;
- Mas e um shopping?

Empresa Pública:

Acesso mais liberado
- Biblioteca Pública;
- Mas e a Secretaria da Fazenda?

Tudo depende não só do tipo da organização, mas do que se quer proteger.

Controle: Entrada Física

Objetivo:

Garantir que ocorra apenas o acesso físico autorizado às informações da organização e outros ativos associados.

O que considerar na entrada física?

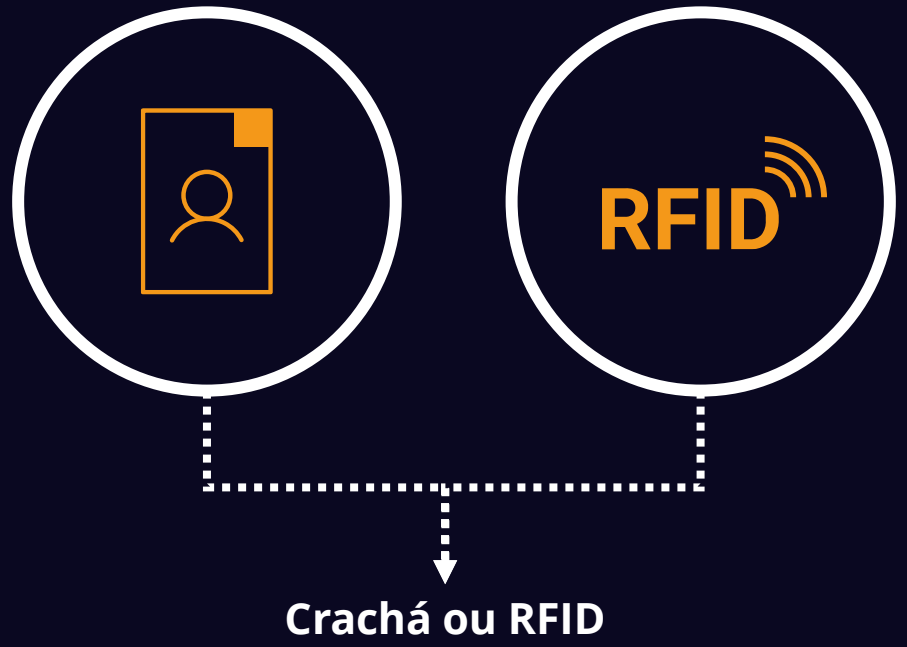
- Se possível, isolar as instalações de processamento de informações;
- Restringir o acesso a locais e edifícios apenas a pessoal autorizado;
- Monitorar o log ou trilha de auditoria de todos os acessos;
- Usar mecanismos de autenticação como cartões de acesso, biometria ou autenticação de dois fatores;
- Instalação de área de recepção monitorada;
- Inspecionar e examinar pertences pessoais dos interessados na entrada e saída;
- Exigir algum tipo de identificação visível e notificar perda e roubo;
- Proteger outros pontos de entrada, como saídas de emergência;
- Processo de gerenciamento de chaves.

Gestão de Acesso

Gerenciamento de acesso eletrônico

Recomendação

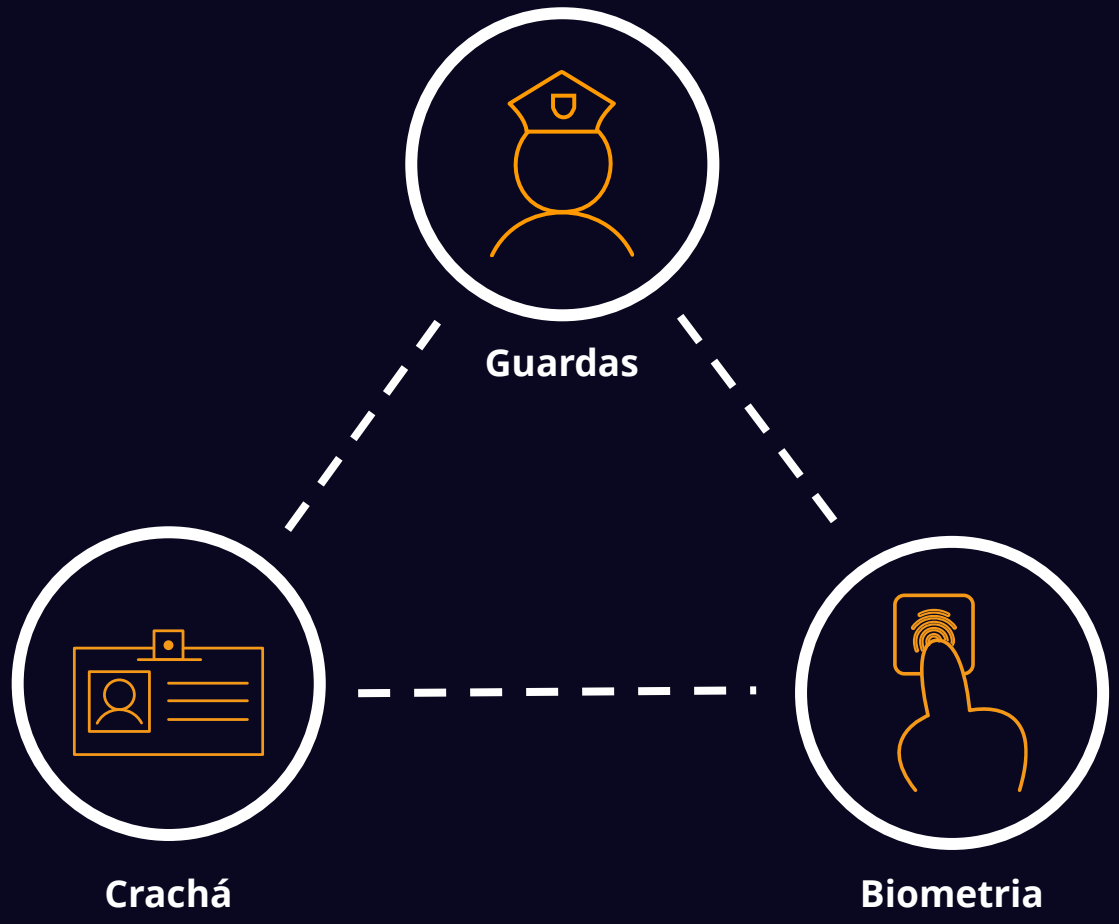
- Colocar uma foto no cartão;
- Não coloque o nome da empresa ou logotipo;
- Exija que funcionários e visitantes usem o crachá em um lugar visível;



- Algo que você saiba, por exemplo, um código ou uma senha.
- Algo que você possui, por exemplo, um cartão ou outro dispositivo;
- Algo que seja parte de você (biometria), tal como uma impressão digital ou uma varredura de íris.

Gestão de Acesso

Medidas adicionais



Controle: Protegendo Escritórios, Salas e Instalações

Objetivo:

Evitar o acesso físico não autorizado, danos e interferências nas informações da organização e outros ativos associados em escritórios, salas e instalações.

Como manter protegidos ativos corporativos importantes?

- Manter pessoas não autorizadas fora do local onde esses ativos se encontram;
- Controles de acesso;
- Não adianta apenas “esconder” esses locais, devemos aplicar outras medidas, como:
  - ✓ Não informar o propósito desses locais;
  - ✓ Reduzir qualquer informação essencial ao mínimo necessário.

Controle: Protegendo Escritórios, Salas e Instalações

Exemplos

- Se processar informação confidencial, garantir que não seja possível espionar de fora;
- Se for uma sala de reuniões, assegurar que nenhuma das conversas sejam audíveis;
- Garantir que ninguém possa olhar para dentro da sala;
- Proteger a sala de qualquer radiação eletromagnética, caso a informação seja processada eletronicamente.

Controle: Monitoramento de Segurança Física

Objetivo:

Monitorar continuamente o acesso físico não autorizado.

Do que é composto um Sistema de Vigilância?

- Guardas;
- Alarmes de intrusão;
- Sistemas de monitoramento de vídeo, como circuito fechado de televisão;
- Software de gerenciamento de informações da segurança física;
- Gerenciado internamente ou por um provedor de serviços.

Controle: Monitoramento de Segurança Física

Considerações

- Instalar um sistema de monitoramento de vídeo, como circuito fechado;
- Registrar o acesso a áreas sensíveis dentro e fora das instalações;
- Testar periodicamente o contato, o som ou detectores de movimento;
- Instalar alarmes para cobrir todas as portas externas e janelas acessíveis;
- O projeto dos sistemas de monitoramento deve ser mantido em sigilo;
- Sistemas de monitoramento devem ser protegidos contra acesso não autorizado;
- O sistema de acionamento de alarme deve ser de fácil acesso;
- Considerar as leis para gravação e monitoramento.

Monitoramento de Alarmes

Detecção de Intrusão: Método passivo com infravermelho, onde movimentos aparentes são detectados quando há um objeto com temperatura.

Câmeras

Detecção de vibração

Sensores de quebra de vidro

Contatos magnéticos

Controle: Proteção Contra Ameaças Físicas e Ambientais

Objetivo:

Prevenir ou reduzir as consequências de eventos originados de ameaças físicas e ambientais.

O que considerar deste controle?

- As avaliações de risco para identificar as consequências potenciais de ameaças;
- As salvaguardas necessárias que devem ser implementadas;

Controle: Proteção Contra Ameaças Físicas e Ambientais

O que considerar neste controle?

- As mudanças nas ameaças que devem ser monitoradas, como:
  - ✓ Inundação ou alagamento, terremoto, tsunami ou desbarrancamento;
  - ✓ Incêndio, explosão, choque elétrico;
  - ✓ Agitação civil, pandemia, surtos, greve, guerra ou terrorismo;
  - ✓ Lixo tóxico, emissões ambientais;
  - ✓ Outros desastres naturais ou desastres causados por seres humanos.
- A localização e a construção das instalações físicas devem levar em conta;
- Cofres ou outras formas de armazenamento podem proteger as informações contra desastres como incêndio, terremoto, inundação ou explosão.

Controle: Trabalhando em Áreas Seguras

Objetivo:

Proteger as informações de áreas seguras.

O que seriam essas áreas seguras?

- Cada espaço de trabalho pode ter a sua própria área segura;
- Por exemplo, em uma prefeitura, podemos entrar nas áreas públicas do edifício, mas os escritórios não são acessíveis para todos;
- Em um banco, não podemos ultrapassar os balcões de atendimento.

Controle: Trabalhando em Áreas Seguras

Considerações

- As medidas de segurança se aplicam a todo o pessoal que trabalha nessas áreas;
- Evitar o trabalho não supervisionado em áreas seguras;
- Monitorar atividades que ferem a segurança e atividades maliciosas;
- Trancar fisicamente e inspecionar periodicamente as áreas seguras vazias;
- Não permitir equipamentos fotográficos, de vídeo, de áudio ou outros equipamentos de gravação;
- Controlar adequadamente o transporte e uso de equipamentos de usuários;
- Afixar procedimentos de emergência de forma facilmente visível ou acessível.

OBRIGADO

ISF – CONTROLES FÍSICOS DA SEGURANÇA DA INFORMAÇÃO