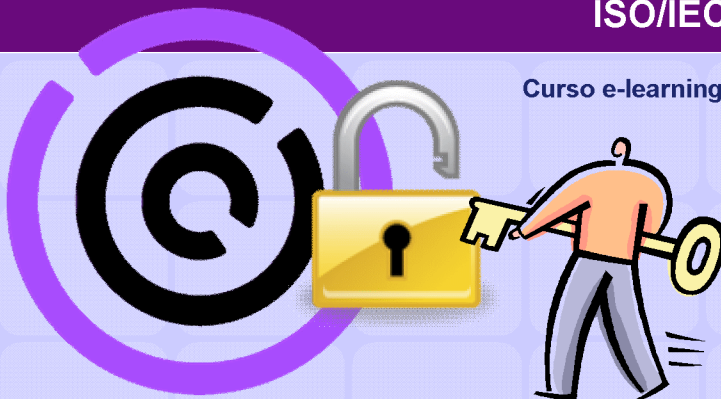


## Fundamentos da Segurança da Informação com base na **ISO/IEC 27002**

Curso e-learning completo



Preparatório para o exame EXIN ISO 27002 Foundation

Todos os direitos de cópia reservados. Não é permitida a distribuição física ou eletrônica deste material sem a permissão expressa do autor.

### Módulo 5



## Medidas Físicas

**Este módulo cobre:**

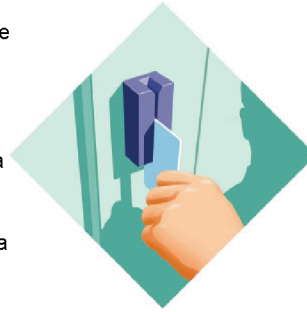
- Segurança física, proteções, alarmes e proteção contra fogo

## Medidas físicas

A análise de risco estabelece um pacote de medidas de controle para a organização reduzir ou eliminar o risco de falta de disponibilidade, integridade ou confidencialidade e as medidas físicas fazem parte deste pacote, em conjunto com medidas técnicas e organizacionais.

### Exemplos de medidas físicas:

- Organizações que tem funções públicas como bibliotecas, fóruns, prefeituras que utilizam controle de acesso
- Organizações privadas que estabelecem áreas restritas devido a necessidade de proteger conhecimento, como novas descobertas ou próximos lançamentos, como é o caso da indústria farmacêutica e de informática
- Áreas com recursos de processamento de informações que mantêm perímetros de segurança
- Proteção de equipamentos por dispositivos de segurança como correntes para que não sejam roubados



## Segurança física

Segurança física é mais antiga que a segurança da informação, basta lembrar que na idade média castelos eram construídos para impedir o acesso de invasores.

O mundo da segurança física emprega uma combinação de medidas eletrônicas e estruturais, por isso as medidas físicas devem ser planejadas e coordenadas da mesma forma. Por exemplo, a instalação de câmeras de segurança deve ser realizada onde elas (as câmeras) são realmente necessárias, e ao mesmo tempo a organização deve ser capaz de assistir e analisar o que está ocorrendo ou já ocorreu.

Não se deve esquecer de aplicar medidas físicas em locais temporários utilizados para casos de emergência.

### Equipamentos

Medidas de segurança física incluem a proteção de equipamentos contra efeitos do clima (ar condicionado, controle de umidade, etc), o uso de extintores de incêndio e o fornecimento de energia estável, sem picos (utilização de filtros).

### Cabeamento

Cabos devem ser instalados de forma a não ocorrer interferências, como ruídos ou estática devido a outros cabos instalados na mesma canaleta, por exemplo, chiados que ouvimos no telefone quando nos aproximamos de outros equipamentos como rádios, transformadores, motores etc.

Dutos de cabos também devem ser protegidos. Salas com servidores devem ser separadas de fontes de energia e sempre que possível é importante ter mais de uma fonte de energia para um grupo de servidores.

## Segurança física

### Mídia de armazenamento

- As pessoas devem ser treinadas para lidar com as diversas mídias de armazenamento, por exemplo, apagar informações confidenciais armazenadas quando o profissional sai da organização. O armazenamento de informações não inclui apenas pendrives ou HD's, muitas impressoras podem armazenar informações no seu disco rígido. Documentos podem ser armazenados temporariamente em impressoras e podem ser recuperados.
- Também é possível armazenar uma grande quantidade de informações em equipamentos móveis como telefones, cartões de memória, pendrives, agendas, notebooks etc. É importante que sempre que um empregado deixe a empresa ele devolva todos os equipamentos, e a informação contida neles seja apagada. Também deve haver procedimentos para o caso de perda ou roubo de equipamentos.



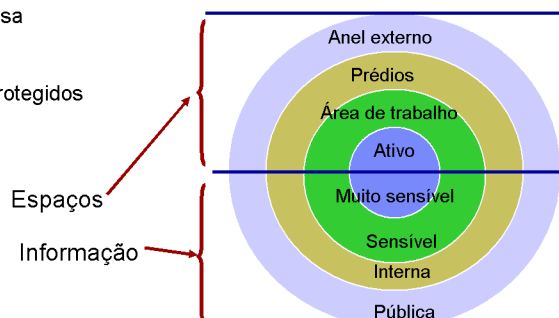
## Anéis de proteção

Todos os ativos do negócio tem um certo valor e dependendo de qual seja este valor e das ameaças e riscos para estes ativos, medidas de proteção devem ser tomadas. Medidas de proteção físicas devem ser tomadas para proteger informação de fogo, ladrões, vandalismo, sabotagem, acesso não autorizado, acidentes e desastres naturais.

### Mas onde se iniciam as medidas de segurança?

Medidas de segurança não devem ser iniciadas nas estações ou locais de trabalho, mas fora da empresa. O acesso aos ativos da empresa deve ser difícil ou impossível, devemos pensar em termos de uma série de perímetros:

- Área em volta da empresa
- Acesso aos edifícios
- Área de trabalho
- Ativos que devem ser protegidos



## Anéis de proteção

### Anel externo

- O anel externo que rodeia a empresa pode ser protegido por barreiras naturais ou pela arquitetura da empresa. Barreiras naturais podem ser, por exemplo, vegetação ou um rio. Exemplos de barreiras de arquitetura podem ser cercas, arame farpado, paredes, muros etc.
- O anel externo deve permitir acesso de pessoas autorizadas, portanto, devem ser instaladas barreiras para verificação eletrônica ou pessoal.
- A área entre o anel externo e a organização pode ser supervisionada por vigilantes (guardas) ou por serviços auxiliares, como manobristas no caso de estacionamentos. Câmeras de vigilância também podem ser utilizadas.

### O prédio

- Há situações onde não existe um anel externo. Neste caso, medidas estruturais, como janelas e portas são importantes. O ideal é que estas medidas sejam concebidas antes da construção, uma vez que modificações em prédios antigos podem ser caras.
- As medidas estruturais devem atender à regulamentos e legislações e existem diversas alternativas como vidros blindados, portas de aço, etc. Essas medidas devem estar de acordo com as necessidades de proteção da organização.
- Além de trancas podemos usar meios eletrônicos de acesso com sistemas de cartão e senha. Equipamentos biométricos ainda não são comuns, mas já se encontra controle de acesso pela digital. O acesso poderia ainda ser liberado por leitura da retina, do rosto, da voz, da mão, etc.
- Características biométricas podem ser divididas em 2 grandes grupos: 1) físico relacionado a forma do corpo e 2) comportamental relacionado ao comportamento das pessoas. Na proteção de edifícios deve ser dada especial atenção ao telhado e as paredes, câmeras podem ajudar nesta vigilância.

## Anéis de proteção: área externa e prédio / Gestão de acesso

Existem várias opções disponíveis no mercado para gestão de acesso a um negócio.

### Gestão eletrônica de acesso:

Muitas organizações estão usando o sistema de passes com wireless RFID (Identificação por Rádio Frequência). Este é um sistema muito utilizado atualmente, mas tem se discutido a possibilidade de clonagem.

Além dos passes RFID existem vários outros passes que não podem ser clonados, mas algumas medidas complementares são recomendadas:

1. Colocar uma foto no passe
2. Não colocar o nome da empresa ou o logo no passe
3. Solicitar aos funcionários que usem o passe visivelmente

Para salas especiais, além do passe de acesso, medidas adicionais de segurança podem ser usadas:

1. Alguma informação só do conhecimento da pessoa como um código PIN
2. Alguma coisa que você tem, como, por exemplo, um segundo passe
3. Alguma coisa que faça parte da pessoa, como uma característica biométrica

### Guardas de segurança

Esta medida pode ser suplementada junto com outras medidas de segurança, como câmeras e sensores com um sistema de alarme acoplado

## Anéis de proteção: espaço de trabalho

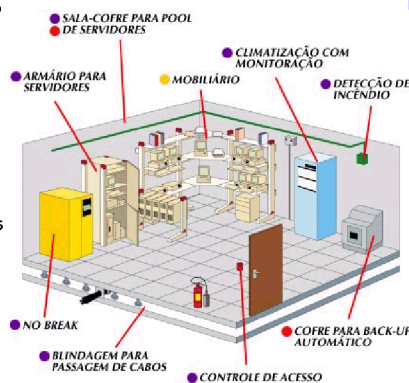
Cada espaço de trabalho pode ter sua função particular e poderia ser objeto de medidas específicas de proteção, por exemplo, um prédio público pode ter áreas públicas onde se pode entrar livremente e áreas restritas não acessíveis ao público.

### Detecção de intrusos

O sistema mais utilizado para detecção de intrusos são os sensores de infravermelho (radiação eletromagnética) que identificam o calor emitido pelos corpos e podem identificar os movimentos, e isso ocorrendo acionam um alarme.

### Salas especiais

É recomendado que uma organização estabeleça salas especiais e áreas para fornecedores retirar e entregar mercadorias de forma que eles não tenham acesso aos ativos do negócio e informações, da mesma forma que tem os empregados da empresa. A restrição de acesso é uma medida preventiva e há um grande número de áreas especiais que veremos a partir do próximo slide.



© Todos os direitos reservados. Material exclusivo dos sites [www.conexto.com.br](http://www.conexto.com.br) e [www.texames.com.br](http://www.texames.com.br). Se você identificar que alguém está usando nosso material para outro fim, denuncie para nós pelo telefone (11) 3522-6380.

Slide 9

## Anéis de proteção: espaço de trabalho - salas especiais

### Armazenamento de materiais sensíveis

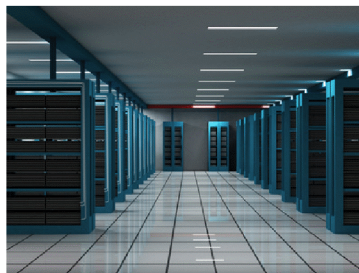
Materiais sensíveis podem ser informações ou produtos caros como medicamentos e produtos que utilizam metais preciosos etc. O acesso a estas áreas deve ser verificado, preferencialmente incluindo estas áreas no controle de acesso das dependências.

### Sala de servidores

Salas de servidores e de rede merecem tratamento especial em relação a medidas físicas de segurança, porque elas contêm equipamentos sensíveis que são vulneráveis a umidade e ao calor, e, se houver uma falha de energia, eles podem parar de funcionar.

Uma das grandes ameaças a sala de servidores é o fogo. Além de requisitos específicos na estrutura do ambiente, estas salas devem ter requisitos especiais de acesso.

Mídias e fitas de backup não devem ser armazenados nas salas de rede, a fim de garantir sua integridade em caso de desastre.



© Todos os direitos reservados. Material exclusivo dos sites [www.conexto.com.br](http://www.conexto.com.br) e [www.texames.com.br](http://www.texames.com.br). Se você identificar que alguém está usando nosso material para outro fim, denuncie para nós pelo telefone (11) 3522-6380.

Slide 10

## Anéis de proteção: espaço de trabalho Salas especiais – sala de servidores

### Refrigeração

Nas salas de servidores o ar deve ser resfriado e o calor produzido pelos equipamentos deve ser retirado do ambiente. O ar também precisa ser desumidificado e filtrado.

Um problema que costuma ocorrer é que, com o tempo, realiza-se a instalação de mais equipamentos, do que aqueles que foram considerados no projeto da sala, e, o ar condicionado e a desumidificação não dão conta do novo nível de exigência..



### Energia de emergência

É importante ter mais de uma fonte de energia (gerador de emergência) para os servidores e a rede, pode-se ter além disso outros recursos de proteção como baterias e baterias de backup (UPS - Uninterruptible Power Supply), filtros, absorvedores para picos de energia e regulagem para quedas de energia.



© Todos os direitos reservados. Material exclusivo dos sites [www.comexto.com.br](http://www.comexto.com.br) e [www.texames.com.br](http://www.texames.com.br) e fim, denuncie para nós pelo telefone (11) 3522-6380.

Slide 11

## Anéis de proteção: espaço de trabalho Salas especiais – Sala de servidores

### Umidade

O ar da sala dos servidores deve ser desumidificado e também deve-se garantir que canos de água e centrais de aquecimentos não sejam instalados nas salas de servidores.

### Fogo

Fogo é uma das grandes ameaças para salas especiais, como sala de servidores ou de rede. Aqui algumas medidas são aplicáveis:

- Detectores de fumaça
- Extintores de incêndio
- Não utilização de material inflamável
- Backups armazenados em outros locais
- Uso de cabos resistentes ao fogo



© Todos os direitos reservados. Material exclusivo dos sites [www.comexto.com.br](http://www.comexto.com.br) e [www.texames.com.br](http://www.texames.com.br) e fim, denuncie para nós pelo telefone (11) 3522-6380.

Slide 12



## Anéis de proteção: O objeto

O objeto é a parte mais sensível a ser protegida, o anel interno. Várias opções existem para armazenamento e proteção de material sensível:

### Armários

Armários servem para armazenar coisas e podem ser trancados, a chave não deve ficar facilmente acessível, mas não são particularmente resistentes contra fogo e podem ser facilmente abertos.

Existem armários de segurança ou resistentes ao fogo, eles existem em várias classes que indicam o grau de proteção ao fogo. Nesses armários podemos armazenar fitas de backup e se houver um incêndio as fitas poderão ser recuperadas.

Armários resistentes ao fogo muitas vezes podem ser uma sala inteira, podem ter uma grande variedade de fechaduras e de proteções contra invasão.



## Alarmes

### Sensores

Segurança física pode usar uma grande variedade de sensores, os mais comuns são:

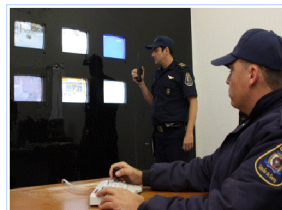
- Detectores infravermelhos, normalmente usados em áreas internas e detectam mudanças de temperatura a certa distância do sensor
- Câmeras, registram imagens que podem ser vistas posteriormente
- Sensores de vibração
- Sensores de detecção de quebra de vidros
- Contatos magnéticos: detectam quando portas ou janelas são abertas



### Monitoramento do alarme

Os sensores devem ser conectados a um sistema de monitoramento de invasão, o qual pode, automaticamente, contatar um centro de emergência, por exemplo, uma empresa de segurança.

Um registro de todos os alarmes ocorridos deve ser realizado para que um processo de investigação documentado seja mantido.



## Proteção contra incêndio

Proteção contra incêndio tem regulamentações compulsórias, requisitos que devem ser atendidos obrigatoriamente.

Incêndios podem começar por várias causas: curto circuitos, ação humana, falha de equipamento, aquecedores com defeito etc. Para ocorrer um incêndio é necessário 3 componentes: material inflamável, oxigênio e temperatura de ignição; este é chamado o triângulo do fogo. Para combater um incêndio devemos usar agentes extintores que atuem em uma das 3 causas anteriores.

O fogo causa os seguintes danos: calor, fumaça, resíduos dos agentes extintores e materiais queimados.

### Sinalização

Para indicar a presença de fogo são utilizados normalmente alarmes de fumaça que são conectados a um sistema de controle de incêndio. Os alarmes e o sistema devem ser verificados regularmente.



### Agentes para extinção de incêndio

O fogo pode ser causado por eletricidade, substâncias químicas ou líquidos inflamáveis. Os agentes extintores de incêndio são: gases inertes (um gás que não reage com o oxigênio), por exemplo: dióxido de carbono, argônio (gás nobre), etc; espuma (a base de água – não adequada para eletricidade); pó (adequado para eletricidade, mas causa dano nos metais); água (não adequada para eletricidade; areia (adequada para óleo).