1.Áreas seguras

Segurança física é a parte da segurança da informação, pois todos os ativos do negócio também devem ser fisicamente protegidos. Segurança física é mais antiga do que a segurança da informação.

Tradicionalmente, a segurança física é provida por gerentes de serviços gerais e técnicos que utilizam seus próprios métodos e técnicas para estabelecer a segurança física. Em muitas organizações, a coordenação entre os encarregados da segurança física e da segurança da informação é de grande importância. O mundo da segurança física emprega uma combinação de medidas organizacionais, estruturais e eletrônicas. Medidas físicas precisam ser planejadas e coordenadas de forma coerente.

Por exemplo, câmeras de segurança somente serão realmente efetivas se medidas estruturais forem tomadas e se houver uma cuidadosa reflexão quanto ao seu propósito e localização. O efeito de dissuasão de câmeras externas pode ser significativo, especialmente em locais no centro de cidades. O que muitas vezes se esquece é que as medidas físicas também se aplicam a locais temporários.

A fim de detectar qualquer invasão, a segurança física usa vários tipos de sensores. Os mais comuns são:

- **Detecção passiva por infravermelho:** São normalmente usados internamente e detectam mudanças de temperatura a uma dada distância do sensor
- **Câmeras:** Gravam imagens que podem ser posteriormente visualizadas. Alguns softwares inteligentes permitem que verificações automáticas sejam realizadas
- **Detecção de vibração:** Detectam vibrações
- **Sensores de quebra de vidro:** Detectam quando uma janela foi quebrada
- **Contatos magnéticos:** Detectam quando uma porta ou janela é aberta.

Além da capacidade de detectar quaisquer intrusões, o acompanhamento da detecção é fundamental para reduzir qualquer dano mínimo. Portanto, os sensores devem ser conectados a um sistema de detecção de intrusos e devem ser bem monitorados. Existem alguns sistemas que podem até mesmo entrar em contato automaticamente com um centro de emergência de um terceiro, como uma empresa de segurança responsável pelo monitoramento. Em qualquer caso, sempre que um alarme for desligado, a causa deve ser investigada.

1.1 Anéis de proteção

Todos os ativos de negócio representam certo valor e, dependendo desse valor, bem como as ameaças e riscos a esses ativos, medidas específicas devem ser tomadas. medidas de segurança física são tomadas para proteger a informação de incêndio, furto, vandalismo, sabotagem, acesso não autorizado, acidentes e desastres naturais.

A segurança física começa na estação ou no local de trabalho, mas fora das instalações do negócio. Deve-se impossibilitar que qualquer pessoa acesse facilmente os ativos que devem ser protegidos. Isso pode ser ilustrado de forma simples e clara ao pensarmos em termos de uma série de anéis:

- **O anel externo:** área em torno das instalações
- **O prédio:** o acesso às instalações
- **O local de trabalho:** as salas das instalações, também conhecido como "anel interno"
- **O objeto:** o ativo que deve ser protegido

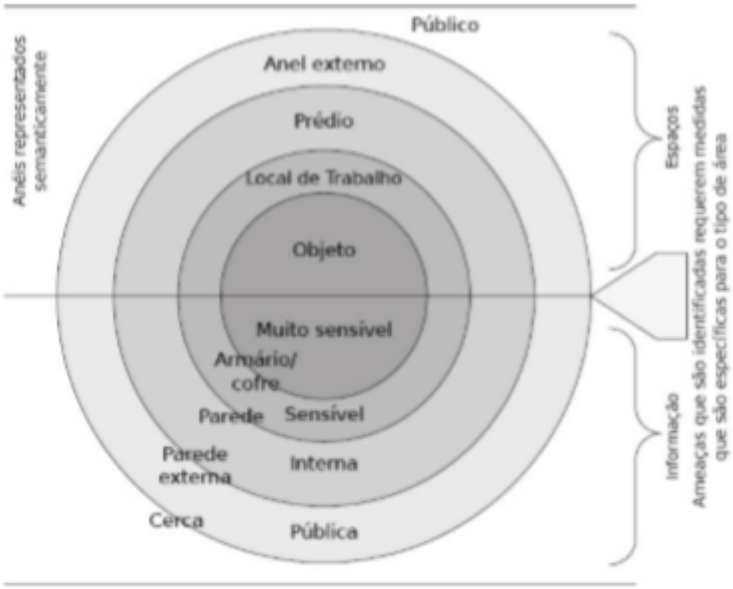

Figura 11.1. Anéis de proteção.

O anel externo que circunda as instalações comerciais pode ser protegido por barreiras naturais e arquitetônicas. Barreiras naturais podem ser um bom exemplo de barreira. O anel externo também deve permitir o acesso de pessoas autorizadas, de modo que as barreiras devem sempre empregar uma verificação pessoal/eletrônica.

Existem situações em que não há um anel externo. Nesses casos, medidas arquitetônicas como janelas, portas e outros tipos de aberturas são importantes. É, naturalmente, melhor que as medidas de segurança sejam integradas enquanto as instalações estão sendo construídas, já que modificar um edificação existente pode ser muito caro. Medidas arquitetônicas também estão sujeitas a regulamentações estritas. Existem várias maneiras de tornar seguras as aberturas nas instalações, como por exemplo, o uso de vidro resistente à quebra.

1.2 Controles de entrada física

A área entre o anel externo e as instalações do negócio (anel interno) pode ser usada para vigilância por um guarda de segurança e para serviços auxiliares, tais como estacionamento. Tais áreas devem ser iluminadas apropriadamente, e, possivelmente, vigilância por câmeras. Ao proteger o prédio, também deve ser dada atenção ao telhado e às paredes. Câmeras de vigilância podem ajudar nisso.

Há diversas opções disponíveis para gerenciar o acesso às instalações do negócio:

1.2.1 Guardas de segurança

O uso de guardas é a medida de segurança física mais cara. Essa medida pode ser suplementada por medidas mais baratas, tais como sensores e câmeras que podem ser monitoradas remotamente. Nesse caso, deve haver sempre um procedimento de acompanhamento se um alarme disparar. É melhor que o pessoal da segurança também verifique pessoalmente o acesso daqueles que entram no edifício. Dessa forma, é mais difícil usar credenciais falsas.

1.2.2 Gerenciamento do acesso eletrônico

Além das fechaduras tradicionais, nos últimos anos tem sido crescente o uso de meios eletrônicos para controlar o acesso a edifícios. Isso inclui sistemas de cartão e fechaduras de código. Muitas organizações usam sistemas com acesso sem fio por RFID. Esses são atualmente, os sistemas mais usados, mas são também assunto de muita discussão, uma vez que suas informações são colhidas, copiadas e imitadas. Para além do RFID, existem outros tipos de controle de acesso que não podem ser penetrados.

Ao usar controles de acesso, algumas medidas organizacionais complementares são recomendadas:

- Uma credencial só deve ter um proprietário, caso contrário não será possível determinar quem acessou o edifício.
- Não coloque o nome da empresa ou logotipo na credencial, use um estilo neutro.
- Se alguém encontrar a credencial, seu propósito não deve ser óbvio. Os funcionários devem ser obrigados a usar a credencial de forma visível. Isso também deve se aplicar aos visitantes, para que a segurança e os funcionários possam detectar e abordar qualquer pessoa que não esteja usando uma credencial.
- Todas as credenciais também devem exibir uma data de validade legível para os humanos.
- Certifique-se de que é estabelecido um sistema em que as pessoas que não têm uma credencial são escoltadas pela equipe de segurança.

- Para salas especiais, medidas de autenticação vigorosas também podem ser usadas. Além das credenciais de acesso, medidas de segurança adicionais são tomadas, tais como: algo que você saiba, algo que você possui e algo que seja parte de você

1.4 Protegendo escritórios, salas e instalações

Uma forma de proteger ativos corporativos importantes é manter pessoas não autorizadas fora do local onde esses ativos se encontram. Além dos controles de acesso descritos antes, é bom tornar mais difícil para invasores encontrarem esses locais. É importante compreender que apenas "esconder" esses locais não é o suficiente. Quando os locais são usados para processar informação confidencial, é importante garantir que não seja possível espionar de fora. Dependendo do tipo de informação e de como ela é processada, há diferentes formas de alcançar isso. Outra medida é garantir que ninguém possa olhar para dentro da sala.

1.5 Protegendo contra ameaças externas e ambientes

Deve haver medidas de proteção física no local para proteger contra quaisquer ameaças externas, tais como incêndio, inundação, explosões e afins. É prudente obter aconselhamento especializado sobre o assunto.

1.6 Trabalhando em áreas seguras

Cada espaço de trabalho pode ter sua própria função específica e, portanto, estar junto às suas próprias medidas de segurança. Por exemplo, em um prédio público, como uma prefeitura, podemos entrar nas áreas públicas do edifício, mas os escritórios não são acessíveis para todos.

1.7 Áreas de carregamento e entrega

É recomendado que uma organização crie salas e áreas especiais para que os fornecedores peguem e entregam mercadorias, de forma que eles não tenham acesso aos mesmos ativos e informações de negócios que os empregados da empresa. A restrição de acesso é uma medida preventiva.

2.Equipamentos

Segurança física inclui a proteção dos equipamentos através do controle de clima, do uso de extintores de incêndio especiais e da provisão de energia limpa, referindo-se à prevenção de picos e quedas na fonte de alimentação e ao fato de que a fonte de alimentação é filtrada.

2.1 Localização e proteção do equipamento

Em salas localizadas no térreo e outras salas especiais, vários tipos de detecção de intrusão podem ser inseridos. Isso depende do tipo de sala. O método mais comum utilizado é a detecção passiva por infravermelho. O movimento aparente é detectado

quando uma fonte de infravermelho com uma temperatura tal como um humano, passa em frente de uma fonte de infravermelho que possui outra temperatura, tal como uma parede. Claro que se acontecer um disparo de alarme, é necessário uma resposta imediata.

Salas separadas podem ser usadas para armazenar materiais sensíveis. Estes podem ser informações, mas também remédios ou itens explosivos. Essas salas requerem medidas adicionais para garantir a sua segurança. O acesso a salas especiais deve ser monitorado, preferencialmente incluindo tais salas como parte do sistema geral de controle de acesso às instalações. Mídias como fitas de backup não devem ser armazenadas em salas de rede. É melhor armazená-las em outro lugar, de forma que as fitas não sejam avariadas no caso de um desastre na sala de servidores. Não há nada pior do que descobrir que, após um incêndio, nenhuma informação pode ser recuperada porque as fitas de backup também foram destruídas.

Há uma série de outras salas importantes e requisitos relacionados:

- Depósito de materiais sensíveis
- Salas de servidores
- Resfriamento
- Energia de emergência
- Umidade
- Incêndio

Um armário é a forma mais simples de armazenar coisas. Deve ser possível trancar o armário, e a chave não deve ser mantida próxima. Entretanto, um armário não é particularmente resistente ao fogo e pode ser arrombado de forma relativamente fácil. Um armário resistente ao fogo protege o conteúdo contra incêndio. Esses armários estão disponíveis em diversas classes, que indicam o grau ao qual são resistentes ao fogo. Armários resistentes ao fogo não são cofres, mas também podem ter propriedades anti arrombamento. Eles são um bom meio para armazenar, por exemplo, fitas de backup, documentos em papel e dinheiro.

Note que as fitas de backup de um sistema não devem ser armazenadas nas mesmas instalações que o sistema de informação. Se as instalações forem completamente destruídas, é vital que as fitas ainda estejam intactas.

As salas de servidores e salas de rede merecem uma menção à parte, já que devem ser abordadas separadamente quando consideram a segurança física. As salas de servidores e salas de rede contêm equipamentos sensíveis que são vulneráveis à umidade e ao calor, e produzem seu próprio aquecimento. Além disso, um sistema de informação pode parar de funcionar devido a uma falha de energia.

Uma das maiores ameaças a uma sala de servidores é o fogo. Além dos requisitos arquitetônicos, as salas de servidores e de rede também possuem requisitos especiais de controle de acesso.

Toda sala dedicada a equipamentos deve ser controlada e monitorada. Essas salas não devem conter nenhuma umidade. Por essa razão, o ar nessas salas é desumidificador. Devem também garantir que nenhum cano de água e equipamento de aquecimento central tenha sido instalado nessas salas. No começo, os computadores centrais eram refrigerados a água, e embora até hoje ainda seja possível refrigerar equipamentos com água, essas soluções devem ser inspecionadas com muito cuidado.

Os sistemas de resfriamento necessitam de manutenção regular e geralmente usam água desmineralizada, da qual um suprimento reserva, suficiente para reabastecer o sistema, deve sempre ser mantido no local.

Proteção contra incêndios é uma área especial dentro da segurança física. Existem requisitos obrigatórios de proteção contra incêndios que devem ser cumpridos. O fogo é uma ameaça que sempre pode ocorrer. Por conseguinte, a todo momento devem ser tomadas medidas de proteção. Incêndios podem começar de várias maneiras, tais como curtos-circuitos, aquecedores defeituosos, ação humana, equipamentos defeituosos e entre outros.

Incêndios requerem os seguintes componentes:

- Material inflamável
- Oxigênio
- Temperatura de ignição

Um fogo pode ser combatido usando um agente extintor, cujo propósito é quebrar esse triângulo do fogo eliminando o acesso do fogo ao oxigênio ou ao combustível. Algumas salas são mantidas a um nível de oxigênio extremamente baixo como forma de proteção contra incêndio. Essas áreas devem ser claramente marcadas e, antes de dar acesso a tais salas, devem ser dadas instruções claras de como trabalhar nelas, juntamente com explicações de quais são os perigos quando se trabalha em condições de oxigênio extremamente baixas.

O fogo pode ter uma variedade de efeitos nocivos. O mais óbvio é o dano direto causado pela queima do material, mas mesmo o material não exposto diretamente às chamas pode ser danificado. Em particular, o equipamento eletrônico é muito sensível às pequenas partículas presentes na fumaça, as quais podem levar a curtos-circuitos ou falhas de componentes. Mesmo quando os danos devidos ao fogo, calor ou fumaça são muito limitados, por terem sido detectados numa fase muito inicial, danos podem resultar do material utilizado para apagar o incêndio.

Uma forma de prevenir um incêndio é limitar o fumo a áreas onde não há materiais inflamáveis. Adicionalmente, limitar materiais inflamáveis a uma quantidade mínima é uma forma muito boa de reduzir o risco de incêndio.

Para sinalizar a presença de incêndio, alarmes de fumaça são geralmente usados e normalmente conectados a um sistema separado. É muito importante que os alarmes de fumaça sejam regularmente verificados. As organizações devem conduzir regularmente exercícios de incêndio e evacuação, de forma que todos estejam familiarizados com o som do alarme e com os procedimentos de evacuação.

Agentes extintores de incêndio são destinados a combater um ou mais dos três componentes do fogo e, ao fazê-lo, apagar o fogo. Existem diferentes tipos de incêndio e, portanto, também diferentes métodos de acabar com esses incêndios.

Os vários agentes extintores de incêndio incluem:

- Gases inertes, tais como dióxido de carbono e argônio
- Inergen e Argonite: são conhecidos como sistemas de inundação
- Espuma, à base de água, não é adequada para eletricidade
- Pó, adequado para eletricidade, mas danifica metal
- Água, não é adequada para eletricidade
- Areia, adequada para óleo

2.2 Utilidades de apoio

Equipamentos utilizam energia. Em uma sala de servidores, é recomendável usar várias fontes de energia independentes. Diversas outras medidas são usadas além dessa: baterias ou uma fonte ininterrupta de alimentação (UPS) que, além de ajustar as flutuações da fonte de alimentação, filtra a energia e absorve quaisquer picos. Tipicamente, baterias duram desde questão de minutos até algumas poucas horas. Por isso, é aconselhável ter também um gerador de emergência para fornecer energia durante qualquer interrupção que seja maior do que a duração da bateria. O gerador deve ser testado regularmente e deve estar abastecido com combustível por um período de tempo suficientemente longo. Baterias também precisam ser substituídas a cada quatro anos aproximadamente. Falhas de energia são um problema não só para computadores, mas também para empresas fabris.

Em salas de servidores, o ar tem que ser resfriado e o calor produzido pelos equipamentos deve ser transportado para fora. O ar também é desumidificado e filtrado. O que muitas vezes acontece é que equipamentos extras são colocados na sala sem o ajuste da sua capacidade de refrigeração.

2.3 Segurança do cabeamento

Os cabos devem ser colocados de tal forma que não possa ocorrer interferência entre cabos distintos. Interferência é quando cabos de rede captam ruído e sinal eletromagnético de outros cabos que correm paralelos a eles. Esses efeitos muitas vezes não são visíveis ou audíveis. Dutos de cabo também devem ser protegidos. Salas de servidores geralmente usam fontes de alimentação separadas. Não é incomum para um servidor ter duas fontes de alimentação, cada uma ligada ao seu próprio grupo de energia.

2.4 Manutenção de equipamentos

A fim de evitar qualquer avaria desnecessária ao equipamento, sua manutenção e seu manuseio só devem ser realizados por pessoal autorizado, que tenha tido treinamento suficiente, que saiba quais são as diretrizes dos fabricantes e que entenda como executar essas diretrizes. O pessoal autorizado também deve ser informado de quaisquer requisitos decorrentes de políticas de seguro. Para isso, uma pessoa responsável deve analisar quais políticas de seguro são aplicáveis e quais são requisitos específicos. Uma parte da manutenção é inspecionar e testar o equipamento antes de introduzi-lo no ambiente operacional. A principal razão para isso é evitar interrupções desnecessárias ao introduzir equipamentos defeituosos que poderiam ter sido detectados através da realização de testes. Um plano de teste deve ser estabelecido e avaliado para ativos importantes.

2.5 Remoção de ativos

Deve estar claro para os funcionários de uma organização como eles devem lidar com meios de armazenamento. Medidas específicas podem ser aplicadas a certos equipamentos. Considere, por exemplo, a exclusão de informações confidenciais em meios de armazenamentos quando uma pessoa deixa a organização. Meios de armazenamento incluem mais do que apenas as formas óbvias, tais como pen drives e discos rígidos. Documentos podem ser armazenados temporariamente em impressoras e podem ser parcialmente recuperados. É possível também armazenar uma grande quantidade de informações em equipamentos móveis. É importante que, se um funcionário deixar a empresa, ele devolva todos os seus equipamentos, e as informações contidas neles sejam excluídas. Também deve haver procedimentos claros para quando tais equipamentos forem perdidos ou roubados.

2.6 Segurança de equipamentos e ativos fora das instalações

Ativos importantes de segurança são:

- Não deixe equipamento ou mídia abandonada
- As orientações do fabricante do equipamento quanto ao manuseio de mídias e equipamentos devem ser seguidas
- Mantenha um registro de quem tem qual equipamento/ativo

- Devem ser estabelecidos controles e orientações adicionais sobre a forma de lidar com equipamentos e ativos, dependendo da localização, e com dados onde estiverem sendo transportados.

2.7 Alienação segura ou reutilização do equipamento

Notificações de segurança importantes visam verificar se alguma informação confidencial ou software licenciado foi deixado na mídia antes de descartá-la. As medidas de segurança devem incluir a destruição de dispositivos de armazenamento de dados, a criptografia de dispositivos de armazenamento de dados ou a exclusão de dados armazenados em dispositivos, caso estes não sejam mais relevantes.

2.8 Equipamentos não acompanhados

Impeça que pessoas não autorizadas acessem serviços/ativos das seguintes formas:

- Encerrando sessões ativas quando concluídas
- Fazendo log-off de aplicativos ou serviços de rede quando eles não forem mais necessários
- Bloqueando a tela/acesso por meio de um mecanismo seguro, como um protetor de tela protegido por senha