1.Introdução à medidas de segurança física

A segurança física desempenha um papel fundamental na proteção dos ativos de TI de uma organização. Embora a segurança digital seja essencial, não devemos subestimar a importância de garantir a segurança física das instalações e equipamentos. Afinal, mesmo com as melhores medidas de segurança cibernética, uma vulnerabilidade física pode comprometer todo o sistema.

A principal razão pela qual a segurança física é tão importante é porque ela ajuda a prevenir o acesso não autorizado às instalações e aos equipamentos. Ela impede que pessoas não autorizadas tenham acesso aos recursos de TI, evitando roubos, vandalismo e outras atividades maliciosas. Além disso, a segurança física também ajuda a proteger contra ameaças internas, como funcionários descontentes ou ex-funcionários que possam tentar comprometer o ambiente de TI.

A segurança física também desempenha um papel crucial na garantia da confidencialidade, integridade e disponibilidade dos dados e sistemas de uma organização. Ela ajuda a prevenir o acesso não autorizado a informações confidenciais, como dados pessoais dos clientes ou informações estratégicas da empresa. Além disso, a segurança física ajuda a evitar a perda de dados devido a desastres naturais, falhas de energia ou outros eventos que possam impactar fisicamente os equipamentos de TI.

1.1 Controles de acesso físico

Os controles de acesso físico são os mecanismos e medidas implementados para regular e monitorar o acesso a áreas, instalações ou recursos físicos de uma organização. Eles são projetados para garantir que somente indivíduos autorizados possam entrar em espaços restritos, protegendo os ativos de TI, informações sensíveis e recursos críticos da organização contra acesso não autorizado, vandalismo, roubo ou outras atividades maliciosas.

Existem várias formas de controles de acesso físico, cada uma com suas características e níveis de segurança. Alguns dos principais controles de acesso físico incluem:

1.2 Fechaduras e chaves

As fechaduras e chaves são um dos métodos mais antigos e amplamente utilizados para controlar o acesso físico a áreas restritas. Esse sistema básico de controle de acesso envolve o uso de fechaduras físicas instaladas em portas, portões ou outras barreiras de acesso, juntamente com chaves correspondentes que são concedidas apenas a indivíduos autorizados.

As fechaduras podem variar em termos de complexidade e níveis de segurança. Existem diferentes tipos de fechaduras, como fechaduras de cilindro, fechaduras de alavanca, fechaduras eletrônicas, entre outras. Cada tipo de fechadura possui mecanismos internos específicos que determinam como ela pode ser trancada e destrancada.

As chaves são projetadas para corresponder ao mecanismo interno da fechadura e permitir o seu destravamento. Elas são geralmente feitas de metal e possuem um formato único que se encaixa perfeitamente na fechadura correspondente. As chaves são distribuídas apenas para pessoas autorizadas, que têm permissão de acesso à área protegida.

Uma das principais vantagens das fechaduras e chaves é a simplicidade de uso e a familiaridade geral. Elas são amplamente adotadas e facilmente compreendidas por usuários de todas as idades. Além disso, as fechaduras e chaves oferecem um certo nível de segurança física, especialmente se forem de alta qualidade e resistentes a técnicas de violação.

No entanto, é importante ter em mente que as fechaduras e chaves também têm suas limitações. Elas podem ser suscetíveis a técnicas de arrombamento, como picking (abertura da fechadura com ferramentas especiais) ou duplicação não autorizada de chaves. A próxima figura mostra um Kit de minhas ferramentas de abertura para travas fechaduras. Além disso, o gerenciamento e controle das chaves podem ser desafiadores em ambientes com muitos usuários e áreas de acesso restrito.

No Brasil, existem diversas marcas renomadas e amplamente reconhecidas no mercado de fechaduras e chaves. Alguns exemplos incluem: Papaiz, Yale, Haga e Pado.

1.3 Cartões de acesso

São dispositivos utilizados para controlar o acesso físico a áreas restritas de uma organização. Eles são projetados para conceder permissões de entrada a pessoas autorizadas e restringir o acesso a indivíduos não autorizados. Esses cartões geralmente são emitidos aos funcionários, contratados ou visitantes e são apresentados a leitores eletrônicos para permitir o acesso a portas, portões ou áreas específicas.

Os cartões de acesso contêm informações codificadas, como dados de identificação pessoal ou números de identificação exclusivos, que são lidos pelo leitor eletrônico. O leitor verifica a validade do cartão e, se as informações corresponderem às permissões de acesso atribuídas, ele desbloqueia a entrada para a pessoa.

Existem diferentes tipos de cartões de acesso, como cartões de proximidade, cartões inteligentes ou cartões de banda magnética. Cada tipo utiliza tecnologias específicas para armazenar e transmitir dados de identificação. Por exemplo, os cartões de proximidade contêm uma antena embutida que permite a comunicação sem fio com o leitor eletrônico quando estão próximos um do outro. Já os cartões inteligentes possuem um microchip que armazena informações criptografadas e podem executar funções avançadas, como autenticação de dois fatores.

Além disso, os cartões de acesso podem ser programados para fornecer diferentes níveis de permissões de acesso. Por exemplo, um cartão pode permitir acesso a uma área específica do prédio, enquanto outro cartão pode conceder acesso a todas as áreas.

Isso permite que a organização controle de maneira granular quem pode entrar em determinados locais e restringir o acesso não autorizado.

Existem várias marcas reconhecidas que fabricam cartões de acesso para controle de acesso físico: HID global, ASSA ABLOY e Zebra Technologies

1.4 Biometria

O controle de acesso por biometria é uma técnica que utiliza características físicas e comportamentais exclusivas de um indivíduo para autenticar sua identidade e permitir o acesso a determinadas áreas ou recursos.

Essa tecnologia se baseia no princípio de que cada pessoa possui características biométricas únicas, tornando-as altamente seguras para a identificação e verificação da identidade. Existem diversos fatores biométricos utilizados para o controle de acesso, sendo os principais:

- **Impressões digitais:** As impressões digitais são um dos fatores biométricos mais amplamente utilizados. Cada pessoa possui um padrão único de sulcos e cristas nas pontas dos dedos, e esses padrões são capturados e comparados com as informações previamente cadastradas para conceder ou negar o acesso.
- **Reconhecimento facial:** O reconhecimento facial envolve a análise e comparação das características do rosto de uma pessoa. Algoritmos avançados são utilizados para identificar pontos-chave do rosto, como distância entre os olhos, formato do nariz, contorno dos lábios, entre outros, para verificar a identidade do indivíduo.
- **Íris:** A análise da íris é outra forma de biometria utilizada para controle de acesso. Cada íris possui um padrão único de linhas, furinhos e pigmentação, e scanners especiais capturam esses detalhes para autenticar a identidade do usuário.
- **Reconhecimento de voz:** O reconhecimento de voz se baseia nas características vocais exclusivas de cada indivíduo, como tom, frequência e padrões de fala. Essas características são analisadas e comparadas com um modelo de voz previamente cadastrado para permitir o acesso.
- **Geometria da mão:** A geometria da mão envolve a captura e análise de características da mão, como o comprimento e a largura dos dedos, formato da palma e posição dos nós dos dedos. Essas informações são utilizadas para autenticar a identidade do usuário.

No processo de controle de acesso por biometria, os padrões biométricos de um indivíduo são capturados por um dispositivo de leitura especializado, como um leitor de impressão digital ou uma câmera para reconhecimento facial. Esses dados biométricos são então comparados com os dados armazenados previamente em um banco de dados seguro. Se houver uma correspondência suficiente entre os padrões biométricos capturados e os dados armazenados, o acesso é concedido.

A tecnologia de biometria é amplamente utilizada em diferentes setores, incluindo segurança física, aplicativos de controle de acesso a edifícios, dispositivos móveis, controle de fronteiras, sistemas de pagamento e muito mais. Além da alta segurança que oferece, a biometria também proporciona uma experiência de usuário conveniente, eliminando a necessidade de senhas ou cartões de identificação.

No entanto, apesar de sua eficácia, a implementação da biometria também apresenta desafios, como questões de privacidade e proteção de dados biométricos. É essencial que as organizações adotem medidas adequadas de segurança e conformidade para garantir o armazenamento seguro e o uso responsável dos dados biométricos dos indivíduos.

2.Sistemas de controle de acesso eletrônico

Os sistemas de controle de acesso eletrônico são soluções avançadas que integram diferentes tecnologias para controlar e monitorar o acesso físico a áreas restritas. Esses sistemas oferecem uma camada adicional de segurança e permitem um gerenciamento mais eficiente do acesso às instalações da organização.

Um sistema de controle de acesso eletrônico típico é composto por vários componentes, incluindo:

- **Leitores de cartões ou crachás:** São dispositivos eletrônicos que leem as informações contidas nos cartões de acesso ou crachás dos usuários. Esses leitores podem ser instalados em portas, catracas ou outros pontos de entrada.
- **Sistemas de identificação:** Os cartões de acesso podem conter informações únicas, como códigos de identificação ou chaves criptográficas, que são usados para autenticar a identidade do usuário.
- **Sensores de movimento:** São dispositivos que detectam a presença de uma pessoa na área de acesso. Eles podem acionar a abertura de uma porta ou alertar sobre atividades suspeitas.
- **Fechaduras eletrônicas:** São dispositivos controlados eletronicamente que permitem ou negam o acesso com base nas informações fornecidas pelo sistema de controle de acesso. Essas fechaduras podem ser acionadas remotamente ou por meio de autenticação do usuário.
- **Software de gerenciamento:** É uma interface de software que permite configurar e administrar o sistema de controle de acesso. Por meio do software, é possível criar perfis de usuários, definir horários de acesso, gerar relatórios de atividades e controlar as permissões de cada usuário.

No Brasil, existem várias marcas conhecidas de fechaduras eletrônicas que oferecem soluções de controle de acesso e segurança física. Algumas das principais marcas incluem: Intelbras, Samsung e Yale.

2.1 Barreiras físicas

As barreiras físicas têm a função de criar uma separação física clara entre espaços restritos e públicos, tornando mais difícil para pessoas não autorizadas entrar nas áreas protegidas. Elas atuam como uma linha de defesa inicial contra acesso não autorizado e ajudam a manter a integridade e a segurança das instalações.

As barreiras físicas podem ser usadas em diferentes tipos de ambientes e locais, desde edifícios comerciais e industriais até propriedades residenciais. Elas podem ser compostas por diferentes materiais, como metal, concreto, grades ou vidro resistente, dependendo do nível de segurança desejado e das necessidades específicas de cada local.

Existem diversos tipos de barreiras físicas que podem ser utilizadas como controles de acesso para restringir o fluxo de pessoas e veículos. Alguns dos principais tipos de barreiras físicas são:

- **Portões:** São estruturas que podem ser abertas e fechadas para controlar o acesso a uma área. Podem ser automáticos, acionados por controle remoto, ou manuais, necessitando de intervenção humana para abri-los.
- **Catracas:** São dispositivos rotativos que permitem o acesso de uma pessoa por vez. Geralmente são usados em ambientes com grande fluxo de pessoas, como estações de metrô, aeroportos e prédios comerciais.
- **Torniquetes:** São barreiras giratórias que permitem a passagem de uma pessoa por vez e impedem a entrada simultânea de mais de uma pessoa. São amplamente utilizados em locais que requerem alto nível de segurança, como instituições financeiras e instalações governamentais.
- **Grades:** São estruturas de metal que podem ser instaladas em portas, janelas e outras aberturas para impedir o acesso não autorizado. Podem ser fixas ou retráteis, permitindo o controle do acesso conforme necessário.
- **Barreiras retráteis:** São dispositivos que podem ser movidos para cima ou para baixo para bloquear ou liberar o acesso de veículos. São comumente usados em estacionamentos, garagens e entradas de condomínios.
- **Cancelas:** São estruturas móveis que se movem para abrir ou fechar o acesso de veículos. Podem ser controladas manualmente, por controle remoto ou por sistemas automatizados.
- **Cercas:** São estruturas de proteção feitas de materiais como metal, madeira ou arame. Podem ser instaladas ao redor de uma área para delimitar seu perímetro e dificultar o acesso não autorizado.

É importante ressaltar que o projeto e a implementação adequados das barreiras físicas devem levar em consideração a conveniência e o fluxo de pessoas autorizadas, de modo a evitar a obstrução ou dificuldade excessiva no acesso.

Também é fundamental realizar manutenções regulares nas barreiras físicas para garantir que estejam funcionando corretamente e cumprindo seu propósito de segurança.

2.2 Monitoramento e vigilância de instalações

O monitoramento e vigilância de instalações refere-se às práticas e tecnologias utilizadas para observar e supervisionar um local de forma contínua, a fim de garantir a segurança e detectar qualquer atividade suspeita ou intrusão.

É uma parte essencial da segurança física, permitindo que as organizações monitorem e protejam suas instalações contra possíveis ameaças. O monitoramento pode ser realizado por meio de diferentes métodos e tecnologias.

2.3 Circuito Fechado de Televisão (CFTV)

O CFTV é um sistema de monitoramento por câmeras que permite a captura, transmissão e gravação de imagens em um ambiente específico. O funcionamento básico do CFTV envolve os seguintes componentes:

- **Câmeras de vigilância:** São dispositivos responsáveis pela captura das imagens. Existem diferentes tipos de câmeras, como câmeras analógicas e câmeras IP (Internet Protocol). As câmeras podem ser fixas, com um ângulo de visão específico, ou móveis, com a capacidade de serem controladas remotamente para ajustar o foco e a direção da câmera.
- **Cabos e conexões:** As câmeras são conectadas a um sistema de cabeamento, que pode ser composto por cabos coaxiais, cabos de rede (para câmeras IP) ou cabos de fibra óptica. Esses cabos transportam o sinal de vídeo da câmera para outros componentes do sistema.
- **DVR (Digital Video Record):** São dispositivos de gravação que recebem e armazenam as imagens capturadas pelas câmeras. No caso do DVR, ele é utilizado em sistemas analógicos, enquanto o NVR é usado em sistemas IP. Esses dispositivos podem ter capacidade de armazenamento interno ou se conectar a unidades externas, como discos rígidos, para maior capacidade de gravação.
- **Monitoramento em tempo real:** O sinal de vídeo das câmeras é transmitido para um monitor, onde as imagens são exibidas em tempo real. Esse monitor pode ser local, permitindo que operadores visualizem as imagens em um centro de controle de segurança, ou remoto, possibilitando o monitoramento por meio de dispositivos conectados à rede, como computadores ou smartphones.
- **Gravação e reprodução:** O DVR ou NVR permite a gravação contínua ou agendada das imagens capturadas pelas câmeras. Essas gravações podem ser armazenadas por um período específico de tempo, de acordo com a capacidade de armazenamento disponível. Em caso de necessidade de análise ou investigação posterior, é possível reproduzir as gravações e revisar as imagens capturadas em momentos anteriores.
- **Gerenciamento e controle:** O sistema de CFTV pode incluir um software de gerenciamento que permite controlar e configurar as câmeras, ajustar suas funções, definir áreas de detecção de movimento, configurar alertas e acessar as gravações. Esse software também pode fornecer recursos avançados, como análise de vídeo, reconhecimento facial ou detecção de intrusão.

2.4 Sistemas de alarme

Os sistemas de alarme são projetados para detectar violações de segurança e alertar imediatamente os responsáveis pela segurança sobre a ocorrência de uma possível ameaça. Eles podem ser instalados em residências, empresas, instituições governamentais e outros locais que exigem proteção contra intrusões e atividades suspeitas.

Os sistemas de alarme geralmente consistem nos seguintes componentes:

- **Sensores:** Esses dispositivos são responsáveis por detectar atividades ou condições anormais. Existem diferentes tipos de sensores, como sensores de movimento, sensores de abertura de portas e janelas, sensores de quebra de vidro, sensores de fumaça, entre outros. Quando um sensor é ativado, ele envia um sinal para o sistema de alarme.
- **Painel de controle:** O painel de controle é o cérebro do sistema de alarme. Ele recebe os sinais dos sensores e processa as informações para determinar se uma violação de segurança ocorreu. O painel de controle também é responsável por acionar os alarmes sonoros e visuais, bem como enviar notificações para a central de monitoramento ou para os proprietários/responsáveis pelo local.
- **Alarmes sonoros e visuais:** Os alarmes sonoros emitem sons altos e audíveis para chamar a atenção e alertar as pessoas próximas sobre a violação de segurança. Os alarmes visuais, como luzes estroboscópicas, piscam ou emitem sinais visuais distintos para indicar a ocorrência de uma ameaça.
- **Comunicação:** Os sistemas de alarme podem estar conectados a uma central de monitoramento ou podem ser configurados para enviar notificações diretamente para os proprietários/responsáveis pelo local. A comunicação pode ser feita por meio de linhas telefônicas convencionais, redes celulares, internet ou conexões sem fio.

Quando ocorre uma violação de segurança, o sensor correspondente é ativado, enviando um sinal para o painel de controle. O painel de controle verifica o tipo de violação e ativa os alarmes sonoros e visuais, alertando as pessoas sobre a situação.

Ao mesmo tempo, a comunicação é estabelecida com a central de monitoramento ou com os responsáveis pelo local, para que medidas de resposta adequadas possam ser tomadas, como notificar as autoridades competentes ou despachar uma equipe de segurança para investigar a situação.

2.5 Patrulhas de segurança

A patrulha de segurança é um componente importante do monitoramento e da vigilância de instalações. Consiste em ter uma equipe de segurança dedicada a realizar rondas periódicas nas áreas protegidas, com o objetivo de garantir a segurança, detectar atividades suspeitas e responder a incidentes imediatamente.

O processo de patrulha pode variar dependendo das necessidades e características específicas de cada local, mas geralmente envolve as seguintes etapas:

- **Planejamento:** Antes de iniciar a patrulha, a equipe de segurança realiza um planejamento adequado. Isso pode incluir a definição de rotas de patrulha, horários de rondas, pontos de verificação críticos e instruções específicas para cada área.
- **Rondas regulares:** A equipe de segurança realiza rondas regulares de acordo com o cronograma estabelecido. Durante essas rondas, eles percorrem as áreas designadas, verificam a integridade das instalações, observam qualquer atividade suspeita e procuram por sinais de intrusão ou violações de segurança.
- **Verificação de pontos de verificação:** Durante as rondas, a equipe de segurança verifica pontos de verificação críticos, como portas, janelas, cercas e sistemas de alarme. Eles garantem que todas as entradas estejam seguras, que os dispositivos de segurança estejam funcionando corretamente e que não haja sinais de danos ou violações.
- **Resposta a incidentes:** Se durante uma ronda a equipe de segurança detectar uma atividade suspeita, violação de segurança ou incidente, eles devem responder de acordo com os procedimentos estabelecidos. Isso pode incluir a realização de abordagens e questionamentos, acionamento de alarmes, comunicação com a central de monitoramento, solicitação de apoio adicional ou notificação das autoridades competentes..
- **Registro de atividades:** Durante a patrulha, a equipe de segurança mantém registros detalhados de suas atividades, incluindo horários, locais visitados, observações relevantes e ações tomadas. Esses registros são importantes para acompanhamento, análise posterior e investigação de incidentes.

3.Clean desk

Refere-se à prática de manter a área de trabalho organizada e livre de documentos, informações ou dispositivos eletrônicos sensíveis quando não estão em uso. É uma medida preventiva para evitar o acesso não autorizado a informações confidenciais e minimizar os riscos de vazamento de dados.

Ao adotar o conceito de Clean Desk, os funcionários são instruídos a manter suas mesas limpas e livres de documentos sensíveis, como relatórios, senhas, anotações ou qualquer outra informação confidencial. Esses itens devem ser armazenados de forma segura em armários ou gavetas com chave quando não estiverem em uso.

Essa prática contribui para a segurança física, pois reduz as chances de informações confidenciais serem visualizadas ou roubadas por pessoas não autorizadas. Além disso, o Clean Desk também promove uma cultura de segurança nas organizações, reforçando a importância de proteger adequadamente os dados sensíveis.

É essencial que as empresas implementem políticas claras de Clean Desk, forneçam treinamento adequado aos funcionários e promovam a conscientização sobre a importância da segurança física no ambiente de trabalho. Dessa forma, é possível mitigar os riscos de acesso não autorizado às informações e manter a confidencialidade dos dados corporativos.