

Segurança Física e Segurança Lógica

Como proteger equipamentos, ambientes, dados e sistemas contra ameaças

Unidade: Fundamentos de Segurança da Informação | Duração: 2 horas

Nome do aluno: _____

Turma: _____

Data: _____

1. Objetivos desta aula

Ao final desta apostila, você deverá ser capaz de:

- Definir o que é segurança da informação e explicar por que ela é dividida em segurança física e segurança lógica.
- Identificar os principais mecanismos de segurança física (controle de acesso, proteção ambiental e segurança patrimonial).
- Identificar os principais mecanismos de segurança lógica (senhas fortes/MFA, criptografia, firewall e antivírus).
- Classificar uma medida de segurança do dia a dia como física ou lógica e justificar essa classificação.

2. O que é segurança da informação?

Segurança da informação é o conjunto de práticas, tecnologias e regras que protegem os ativos de uma organização — equipamentos, prédios, dados, sistemas e pessoas — contra danos, roubos, vazamentos e invasões. Ela costuma ser dividida em duas frentes que se complementam: a segurança física e a segurança lógica.

Dica

Pense assim: a segurança física protege o "corpo" da infraestrutura de TI (o hardware, o prédio, os equipamentos). A segurança lógica protege a "informação" que circula dentro desse corpo (os dados, os sistemas, os softwares).

3. Segurança física

A segurança física protege o hardware, os prédios e os equipamentos contra danos ou roubos. Ela atua sobre o mundo real: quem pode entrar em um ambiente, o que pode acontecer com os equipamentos e como reagir a incidentes físicos (incêndio, alagamento, furto).

3.1 Controle de acesso

Mecanismos que restringem fisicamente quem pode entrar em um ambiente, como uma sala de servidores (data center) ou o prédio da empresa.

- Catracas: liberam a passagem apenas para pessoas autorizadas, geralmente após leitura de crachá ou biometria.
- Crachás: identificam o funcionário e podem ter níveis de permissão diferentes (ex.: um crachá comum não abre a sala de servidores).
- Portas com biometria: usam impressão digital, reconhecimento facial ou íris para liberar o acesso, evitando o uso de um crachá roubado ou emprestado.

3.2 Proteção ambiental

Mecanismos que protegem os equipamentos das condições do próprio ambiente onde estão instalados.

- Ar-condicionado: evita o superaquecimento de servidores e equipamentos, que pode causar falhas e desligamentos.
- Controle de umidade: umidade alta pode causar curto-circuito e corrosão; umidade baixa pode gerar eletricidade estática.
- Alarmes de incêndio: detectam fumaça ou calor precocemente, permitindo evacuação e acionamento de sistemas de combate a incêndio antes que o dano seja irreversível.

3.3 Segurança patrimonial

Mecanismos de vigilância e resposta contra roubo, invasão ou vandalismo do patrimônio físico.

- Câmeras de segurança (CFTV): monitoram e registram o que acontece em áreas críticas, servindo tanto para prevenção quanto para investigação de incidentes.
- Guardas: presença humana capaz de identificar e reagir a situações suspeitas em tempo real, algo que uma câmera sozinha não faz.

Exemplo resolvido

Uma escola instala uma sala de servidores com porta biométrica, ar-condicionado dedicado e uma câmera apontada para a porta. Se a energia do ar-condicionado falhar em um dia muito quente, os servidores podem superaquecer e desligar sozinhos — mesmo sem nenhuma invasão. Isso mostra que segurança física não é só "impedir entrada de pessoas": também é proteger o ambiente físico dos equipamentos.

4. Segurança lógica

A segurança lógica protege os dados digitais, os sistemas e os softwares por meio de códigos, senhas e restrições de rede. Ela atua sobre o mundo digital: quem pode acessar um sistema remotamente, como os dados são armazenados e transmitidos, e como impedir softwares maliciosos de agir.

4.1 Senhas fortes e múltiplos fatores de autenticação (MFA)

Uma senha forte combina letras maiúsculas e minúsculas, números e símbolos, evitando palavras óbvias ou dados pessoais (data de nascimento, nome do usuário).

O MFA (Multi-Factor Authentication) exige mais de uma prova de identidade para liberar o acesso — por exemplo, senha (o que você sabe) + código enviado ao celular (o que você tem) + biometria (o que você é). Mesmo que a senha seja descoberta, o invasor ainda precisa do segundo fator.

4.2 Criptografia

Criptografia é o embaralhamento de dados para torná-los ilegíveis a quem não tem a chave correta de decodificação. Um arquivo criptografado, mesmo que seja roubado, aparece como um conjunto de caracteres sem sentido para quem não possui a chave.

Dica

Criptografia não impede o roubo do dado — ela impede que o dado roubado seja útil para quem o roubou.

4.3 Firewall e antivírus

O firewall filtra o tráfego de rede, bloqueando conexões não autorizadas entre a rede interna e a internet, funcionando como um "porteiro" da rede. O antivírus identifica e bloqueia programas maliciosos (vírus, trojans, ransomware) que já tentaram entrar no computador ou sistema.

5. Física x Lógica: comparando as duas frentes

Critério	Segurança física	Segurança lógica
O que protege	Hardware, prédios, equipamentos	Dados, sistemas, softwares
Exemplo de ameaça	Roubo, incêndio, superaquecimento	Invasão de sistema, vazamento de dados, malware
Exemplos de mecanismo	Catraca, crachá, biometria, câmeras, guardas	Senha forte, MFA, criptografia, firewall, antivírus
Atua sobre	O mundo real / o ambiente	O mundo digital / a informação

As duas frentes trabalham juntas para garantir a proteção total: uma porta biométrica (física) de nada adianta se o sistema atrás dela usa senha "123456" e sem MFA (lógica) — e uma criptografia forte (lógica) de nada adianta se qualquer pessoa pode entrar na sala e levar o servidor embaixo do braço (física).

6. Exercícios de fixação

Responda no espaço abaixo de cada questão. O gabarito está na seção seguinte.

- 1)** Classifique cada medida abaixo como segurança física (F) ou segurança lógica (L), justificando em uma frase:
(a) instalação de alarme de incêndio na sala de servidores; (b) exigência de MFA para acessar o sistema

acadêmico da escola; (c) contratação de guardas para a portaria; (d) criptografia dos arquivos do backup na nuvem.

2) Explique, com suas palavras, por que um firewall bem configurado ainda não é suficiente para garantir a segurança total de uma escola, mesmo sem nenhum problema de segurança física.

3) Dê um exemplo (diferente dos citados na apostila) de uma medida de segurança física e uma de segurança lógica que poderiam ser aplicadas no laboratório de informática da sua escola.

Erros comuns

- Achar que segurança lógica "substitui" a física, ou vice-versa — na prática, uma falha em qualquer uma delas compromete a proteção total.
- Confundir criptografia com senha: a senha controla quem entra; a criptografia torna o dado ilegível mesmo para quem conseguiu roubá-lo.
- Achar que antivírus e firewall fazem a mesma coisa: o firewall filtra o tráfego de rede antes que ele chegue; o antivírus atua sobre arquivos e programas já presentes no sistema.

7. Desafio final

Uma empresa sofreu a invasão de sua rede interna durante a madrugada. Os invasores conseguiram acesso físico ao prédio (a porta dos fundos estava sem tranca) e, de dentro do prédio, conectaram um notebook diretamente à rede local, que não tinha firewall interno nem exigia autenticação adicional para acessar o servidor de arquivos.

Aponte pelo menos duas falhas de segurança física e duas falhas de segurança lógica nesse cenário, e proponha uma solução para cada uma.

8. Gabarito

Questão 1

(a) F — alarme de incêndio protege o ambiente físico dos equipamentos. (b) L — MFA é um mecanismo de autenticação para acesso digital. (c) F — guardas são um mecanismo de segurança patrimonial. (d) L — criptografia protege os dados em si, tornando-os ilegíveis.

Questão 2

Um firewall bem configurado protege o tráfego de rede, mas não impede que alguém entre fisicamente no prédio, roube um equipamento, conecte um dispositivo diretamente à rede interna (contornando o firewall de borda) ou copie dados de uma tela desbloqueada. Segurança total exige as duas frentes atuando juntas.

Questão 3

Respostas variam. Exemplos aceitáveis: física — trava eletrônica na porta do laboratório com registro de quem entrou; lógica — bloqueio automático de tela após poucos minutos de inatividade nos computadores do laboratório.

9. Resumo para estudar antes da prova

- Segurança física protege hardware, prédios e equipamentos; segurança lógica protege dados, sistemas e softwares.
- Segurança física: controle de acesso (catracas, crachás, biometria), proteção ambiental (ar-condicionado, umidade, alarme de incêndio) e segurança patrimonial (câmeras, guardas).
- Segurança lógica: senhas fortes e MFA, criptografia (embaralha dados para torná-los ilegíveis) e firewall/antivírus (bloqueiam invasões e programas maliciosos).
- As duas frentes são complementares: proteção total exige física E lógica trabalhando juntas, nunca uma no lugar da outra.