Pergunta 1:

Num sistema hospitalar que armazena dados clínicos dos pacientes, a tríade Confidencialidade (Confidentiality), Integridade (Integrity) e Disponibilidade (Availability), ou seja, CIA é fundamental para garantir a proteção da informação e a continuidade dos serviços médicos.

A Confidencialidade assegura que apenas os profissionais autorizados (médicos, enfermeiros ou administradores do sistema) têm acesso aos dados clínicos. Em ambiente hospitalar isto é critico, pois a divulgação indevida de diagnósticos, alergias ou históricos médicos pode violar a privacidade do paciente e a legislação de proteção de dados. Um exemplo de incidente seria um colaborador sem permissões aceder a registos médicos de familiares ou de figuras publicas.

A Integridade garante que a informação armazenada não é alterada indevidamente, seja por erro humano, falha técnica ou ataque malicioso. Num hospital, uma alteração incorreta na medicação ou no grupo sanguíneo de um paciente pode ter consequências graves para a sua saúde. Um cenário realista seria um erro de sistema ou malware modificar dosagens de medicamentos, levando a decisões clínicas erradas.

A Disponibilidade assegura que os sistemas e dados estão acessíveis quando necessários. Em contexto hospitalar, esta dimensão é critica porque atrasos no acesso a exames, prescrições ou históricos clínicos podem comprometer tratamentos urgentes. Um exemplo seria um ataque DoS ou ransomware que bloqueie o sistema informático, impedindo médicos de consultar informações vitais durante uma emergência.

Assim, no contexto hospitalar, a tríade CIA não é apenas um conceito teórico, mas um requisito fundamental e essencial para proteger vidas, garantir a qualidade do serviço e cumprir obrigações legais e éticas.

Pergunta 2:

Num sistema universitário que armazena dados pessoais, académicos e financeiros sensíveis, a utilização de Criptografia Simétrica revela-se frequentemente mais apropriada para a proteção de dados em repouso e grandes volumes de informação, devido à sua elevada eficiência computacional e rapidez de execução. Algoritmos como AES (Advanced Encryption Standard) permitem criar bases de dados inteiras, backups e ficheiros de forma continua sem impacto significativo no desempenho do sistema, o que é crucial em ambientes com milhares de acessos concorrentes.

A principal vantagem da criptografia simétrica reside na sua performance e baixo custo de processamento, tornando-a ideal para proteção de dados armazenados e comunicações internas. Contudo a sua desvantagem critica é a gestão e distribuição segura da chave secreta, pois a exposição dessa chave compromete toda a informação cifrada. Por outro lado a Criptografia Assimétrica baseia-se num par de chaves pública/privada, oferecendo maior

robustez na autenticação e troca segura de informação entre entidades que não partilham segredos prévios. No entanto, apresenta maior sobrecarga computacional, sendo menos eficiente para cifrar grandes volumes de dados de forma contínua.

Assim, uma solução mais equilibrada consiste numa abordagem Híbrida, amplamente utilizada em protocolos TLS/HTTPS, onde a criptografia assimétrica é utilizada inicialmente para estabelecer um canal seguro e trocar uma chave simétrica, passando posteriormente a criptografia simétrica a proteger o fluxo de dados efetivo. Esta estratégia combina confidencialidade forte, eficiência operacional e melhor gestão de chaves, reduzindo o risco de exposição e garantindo escalabilidade e desempenho adequado em sistemas académicos de grandes dimensões.

Pergunta 3:

Num cenário de trabalho híbrido com BYOD, a implementação de MFA deve ser feita de forma estruturada e integrada com o sistema de identidade da organização (por exemplo, Active Directory/SSO). O primeiro passo consiste em tornar o MFA obrigatório para todos os acessos remotos e aplicações criticas, especialmente VPN, email corporativo e sistemas internos. Em seguida, define-se uma política de autenticação baseada em risco, onde os acessos fora da rede interna ou de dispositivos desconhecidos exigem sempre múltiplos fatores.

Os fatores a utilizar devem combinar categorias distintas:

- Algo que o utilizador sabe - palavra passe forte com políticas de complexidade e rotação;
- Algo que o utilizador possui - aplicação autenticadora (TOTP) ou chave física (FIDO2);
- Algo que o utilizador é - biometria local no dispositivo, quando disponível;

A escolha de aplicações autenticadoras é geralmente preferível ao SMS, pois reduz riscos de SIM swapping. As chaves físicas oferecem elevada segurança para contas administrativas. A biometria aumenta a usabilidade sem expor dados sensíveis, pois a verificação ocorre localmente no dispositivo.

A implementação deve ainda incluir um registo inicial seguro dos dispositivos, mecanismos de recuperação de conta controlados e limitação de tentativas falhadas. Em ambiente BYOD é aconselhável complementar com verificação de conformidade do dispositivo (antivírus ativo, sistema atualizado) antes de permitir os acessos.

Os principais desafios incluem resistência dos utilizadores, custos de licenciamento, suporte técnico adicional e risco de perda do dispositivo de autenticação. Existe também o risco de dispositivos pessoais comprometidos, pelo que o MFA de integrar-se numa estratégia de defesa em profundidade e não atuar isoladamente.

Desta forma, a implementação de MFA aumenta significativamente a confidencialidade e integridade dos acessos remotos, equilibrando segurança e usabilidade num modelo híbrido.

Pergunta 4:

Numa empresa de comércio eletrónico sujeita a ataques externos, a utilização de sistemas de deteção de intrusões permite identificar comportamentos suspeitos e responder atempadamente a incidentes de segurança. Existem duas abordagens principais, NIDS (Network-based Intrusion Detection System) e HIDS (Host-based Intrusion Detection System).

O NIDS é colocado na rede, normalmente junto ao firewall ou em pontos de agregação de tráfego, e monitoriza pacotes que circulam entre a Internet e os servidores. A sua principal vantagem é a capacidade de detetar ataques distribuídos, scans de portas, tentativas de DoS ou padrões de exploração antes de atingirem diretamente os sistemas. Permite ainda proteger vários equipamentos com um único sensor. Contudo, apresenta desvantagens como dificuldade em analisar tráfego cifrado (HTTPS) e menor visibilidade sobre o que ocorre dentro de cada servidor.

O HIDS, por sua vez, é instalado diretamente nos servidores ou endpoints e monitoriza ficheiros, processos, logs e integridade do sistema. A sua vantagem é a elevada precisão na deteção de alterações locais, malware ou escaladas de privilégios, mesmo quando o tráfego esta cifrado. A desvantagem é o maior consumo de recursos e a necessidade de gestão individual por máquina.

Uma estratégia eficaz consiste em combinar ambos. O NIDS seria implementado na fronteira da rede e na DMZ para identificar tráfego malicioso externo e padrões de ataque em larga escala. Em paralelo, o HIDS seria instalado nos servidores críticos (web, base de dados, pagamentos) para detetar alterações internas e comportamentos anómalos ao nível do sistema operativo. Ambos devem enviar eventos para um sistema central de logs/SIEM, permitindo a correlação de alertas e resposta mais rápida.

Desta forma obtém-se cobertura de rede e de host simultaneamente, reforçando a defesa em profundidade e aumentando a probabilidade de deteção precoce de intrusões.

Pergunta 5:

Numa empresa de média dimensão, a implementação de firewalls deve seguir uma lógica de segmentação de rede e defesa em profundidade, colocando diferentes firewalls em pontos estratégicos da topologia.

Na ligação à Internet deve existir um firewall do tipo stateful inspection, responsável por todo o tráfego de entrada e saída. Aqui apenas seriam abertas portas estritamente necessárias, como HTTPS (443) para serviços web públicos e VPN para acesso remoto autenticado. A política base deve ser deny all by default, permitindo apenas exceções definidas.

Entre o firewall perimetral e a rede interna deve ser criada um DMZ, onde ficam alojados os servidores web e de email. Entre a DMZ e a LAN interna deve existir um segundo firewall, também stateful, mas com regras ainda mais restritivas. Por exemplo, permitir apenas que o

servidor web comunique com a base de dados interna numa porta especifica e IP autorizado, impedindo qualquer outro tráfego direto para a rede de colaboradores.

Para proteção adicional dos serviços web externos, pode ser implementado um Application Gateway/Web Application Firewall (WAF), capaz de analisar o conteúdo HTTP/HTTPS e bloquear ataques com SQL Injection ou XSS. Nos computadores internos recomenda-se ainda firewalls locais de endpoint, reforçando a proteção contra ameaças internas.

Exemplos de regras concretas:

- Bloquear portas inseguras como Telnet (23) e FTP não cifrado;
- Permitir apenas HTTPS (443) para acesso externo;
- Permitir VPN autenticada para colaboradores remotos;
- Ativar logs e alertas de tentativas de intrusão;
- Limitar tráfego entre DMZ e LAN apenas a serviços necessários;

Desta forma, a organização protege simultaneamente os serviços externos e a rede interna, reduzindo a superfície de ataque garantindo confidencialidade, integridade e disponibilidade mesmo que uma camada de defesa seja ultrapassada.

Pergunta 6.a:

Um firewall é uma ferramenta de controlo de tráfego de redes, mas não consegue resolver todos os vetores de ataque porque muitos deles não passam pelo perímetro tradicional ou exploram fatores humanos e internos.

1. Ameaças Internas - Um colaborador mal intencionado ou um utilizador que cometa erros pode aceder a dados sensíveis ou instalar software indevido estando já dentro da rede autorizada. O firewall não consegue impedir este tipo de ação porque o tráfego é considerado legitimo e interno. Assim, mesmo com regras de filtragem corretas, o firewall não deteta abuso de privilégios, cópia indevida de ficheiros ou exfiltração de dados feita por um utilizador autenticado.
2. Dispositivos portáteis infetados (BYOD/USB) - Um portátil ou pen USB infetados podem introduzir malware diretamente na rede interna quando se ligam ao WI-Fi ou a uma porta física. Neste caso o ataque não atravessa o firewall perimetral, entrando por dentro. O firewall não consegue verificar o estado de segurança do dispositivo nem impedir infeções locais que depois se propagam lateralmente.

Desta forma, embora o firewall seja essencial para o controlo de acessos externos, estes vetores demonstram que ele não é suficiente isoladamente, sendo necessário complementar com antivírus/EDR, controlo de acessos, NAC, políticas de privilégios e formação de utilizadores dentro de uma estratégia de defesa em profundidade.

Pergunta 6.b:

Para mitigar de forma credível estes riscos em conjunto com firewalls, é necessário aplicar controlos técnicos e de gestão adicionais, integrando uma estratégia de defesa em profundidade.

No caso das ameaças internas, devem ser implementados controlos de acesso baseados em privilégios mínimos (RBAC), registo e monitorização de atividades (logs/SIEM) e separação de funções administrativas. Estes mecanismos permitem identificar abusos de privilégios e rastrear ações suspeitas que o firewall, por si só, não consegue detetar. A nível de gestão, políticas claras de segurança e formação de utilizadores reduzem o risco de erro humano e engenharia social.

Relativamente aos dispositivos portáteis infetados, é importante aplicar NAC (Network Acess Control) para verificara o estado de segurança do equipamento antes de permitir ligação, bem como soluções de antivírus/EDR atualizadas e bloqueio de dispositivos USB não autorizados. A segmentação de rede e VLANs também limitam a propagação lateral de malware caso um equipamento seja comprometido.

Desta forma, os firewall continuam a proteger o perímetro, mas estes controlos complementares asseguram a proteção interna, deteção precoce de ameaças e redução do impacto de infeções ou comportamentos maliciosos.