UNIVERSIDADE FEDERAL DO PIAUÍ - UFPI
CURSO: BACHARELADO EM SISTEMAS DE INFORMAÇÃO
DISCIPLINA: PROGRAMAÇÃO PARA WEB II
PROFESSOR (A): JÚLIO VÍTOR MONTEIRO
ALUNO: LUÍS EDUARDO SILVA BRITO
C.H.: 60 h CRÉDITOS: 2.2.0 PERÍODO: 2024.1

1. Qual é a definição de criptografia e sua importância na segurança da informação?
A) Técnica de esconder informações de quem não tem acesso físico ao sistema.
B) Método de proteger informações convertendo dados em um formato ilegível para quem não tem a chave secreta.
C) Processo de compilar informações para análise posterior.
D) Técnica de dividir informações em partes para segurança adicional.

2. Qual das alternativas abaixo representa a principal diferença entre criptografia simétrica e assimétrica?
A) Simétrica usa duas chaves diferentes, enquanto assimétrica usa apenas uma.
B) Simétrica usa uma chave para cifrar e decifrar, enquanto assimétrica usa um par de chaves.
C) Assimétrica é mais rápida e eficiente que a simétrica.
D) Simétrica é usada apenas para comunicações seguras pela internet.

3. Quais são os principais algoritmos utilizados em criptografia simétrica?
A) RSA e ECC.
B) DES e AES.
C) SSL e TLS.
D) SHA e MD5.

4. O que é uma assinatura digital?
A) Método de compactar informações para armazenamento eficiente.
B) Técnica de verificar a autenticidade do remetente e a integridade da mensagem.
C) Processo de dividir informações em pequenos blocos.
D) Técnica de criptografar mensagens para que apenas o destinatário possa ler.

5. Como um certificado digital é utilizado para autenticação em websites?
A) Ele criptografa todos os dados no website.
B) Ele assina digitalmente os dados do usuário.
C) Ele valida a identidade do website e estabelece um canal seguro (SSL/TLS).
D) Ele verifica a senha do usuário em cada login.

6. O que é uma Infraestrutura de Chave Pública (PKI)?
A) Sistema para emissão e gerenciamento de certificados digitais usando criptografia de chave pública.
B) Rede de servidores que compartilham chaves simétricas.
C) Método de armazenar chaves privadas em dispositivos seguros.

D) Processo de distribuir chaves públicas entre usuários.

7. Quais são os componentes principais de uma política de controle de acesso?
A) Políticas de controle, procedimentos de controle, e exemplos práticos.
B) Políticas de uso aceitável, segurança física, e criptografia.
C) Controle de acesso baseado em funções, gestão de senhas, e auditoria.
D) Autenticação, autorização, e auditoria.

8. Quais são os principais métodos de autenticação mencionados na gestão de acesso do usuário?
A) Senhas, tokens, biometria.
B) Cartões magnéticos, chaves físicas, e-mails.
C) Códigos de barras, números de série, respostas secretas.
D) Assinatura digital, criptografia, firewalls.

9. O que é segurança operacional?
A) Medidas para proteger apenas os dados digitais.
B) Controles implementados para proteger ativos físicos e de informação.
C) Uso de senhas fortes e autenticação multifatorial.
D) Implementação de políticas de uso aceitável.

10. Por que a segurança das comunicações é importante?
A) Para garantir que todos os dados sejam armazenados em um único local.
B) Para proteger dados em trânsito contra interceptação e manipulação.
C) Para garantir que todos os usuários tenham acesso a todas as informações.
D) Para facilitar a transferência de dados entre sistemas diferentes.

11. Qual é a importância da segurança física na proteção de ativos?
A) Garantir que apenas dados digitais sejam protegidos.
B) Proteger ativos físicos contra danos, roubo ou acesso não autorizado.
C) Implementar políticas de segurança cibernética.
D) Manter um inventário atualizado de todos os ativos digitais.

12. O que é um plano de contingência organizacional?
A) Conjunto de regras para o uso de senhas.
B) Conjunto estruturado de procedimentos e recursos preparados para responder a incidentes ou crises.
C) Lista de contatos de emergência para a organização.
D) Documento que descreve a política de segurança de uma empresa.

13. Explique como a ISO 27001 e a ISO 27002 se complementam na gestão de segurança da informação.
R= **A ISO 27001 é o que deve ser feito para proteger as informações, basicamente é o que você precisa ter em lugar, por exemplo os requisitos e estrutura do sistema de gestão. Enquanto que a ISO 27002 é como você pode implementar essas ideias na prática, por exemplo as boas práticas.**

14. Descreva um cenário em que um plano de contingência organizacional seria ativado e as etapas envolvidas na resposta ao incidente.

R= **Se uma determinada empresa sofrer um ataque de ransomware, as estampas que devem ser seguidas na resolução do incidente são: *Detecção e Notificação*: um determinado funcionário percebe que os arquivos estão bloqueados e recebe uma mensagem de resgate. Imediatamente ele deve notificar o departamento de TI. *Avaliação do Incidente*: A equipe de TI analisa e identifica quais arquivos foram danificados. *Isolamento e Contenção*: Desconectam os sistemas que foram infectados. *Recuperação*: Após remover o ransomware, é feita a restauração dos arquivos a partir de backups. *Comunicação*: Às partes interessadas são informadas dos acontecimentos.**

***Revisão*: Analisa o incidente e melhora as práticas de segurança.**

15. Explique o processo de auditoria de segurança segundo as normas ISO 27001 e ISO 27002, detalhando as etapas de planejamento, execução e relatório.

R= **O processo de auditoria de segurança segundo as normas ISO 27001 e ISO 27002 envolve três etapas principais: planejamento, execução e relatório. No planejamento, define-se o escopo, seleciona-se a equipe de auditoria, desenvolve-se um plano detalhado e revisa-se a documentação existente. Na execução, realiza-se uma reunião de abertura, coleta-se evidências através de entrevistas, observações e testes, avaliam-se os controles de segurança e identificam-se não conformidades. Por fim, na etapa de relatório, analisam-se as evidências coletadas, elabora-se um relatório detalhado dos achados da auditoria, realiza-se uma reunião de encerramento para discutir os resultados e recomendações, e monitora-se a implementação das ações corretivas para garantir a conformidade contínua. Esse processo assegura que a empresa esteja protegida contra ameaças e cumpra os padrões de segurança da informação.**