11 - FSA - 2025 - FSA-SP - Analista de Suporte I:
O que é um ataque de phishing?

(A) Uma tentativa de sobrecarregar um servidor com tráfego
(B) Uma técnica para interceptar comunicações de rede
(X) Uma tentativa de enganar usuários para revelar informações sensíveis
(D) Um método para quebrar senhas por força bruta

12 - EDUCA - 2025 - Prefeitura de Santa Cecília - PB - Assistente Administrativo:
A Segurança da Informação é um conjunto de práticas, políticas e ferramentas que visam proteger dados e sistemas contra acessos não autorizados, perdas, alterações ou danos.
Sobre os principais tipos de ameaças digitais, assinale CORRETAMENTE:

(A) Um worm é um programa malicioso que precisa se anexar a um arquivo legítimo para se propagar e infectar sistemas.
(B) Trojans são vírus que se replicam automaticamente através de redes, sem necessidade de intervenção do usuário.
(X) Ransomware é um tipo de malware que criptografa arquivos e exige pagamento de resgate para liberar o acesso aos dados.
(D) Alguns keyloggers e adwares são classificados como softwares de segurança pela indústria antivírus, pois monitoram atividades e registram dados com a finalidade de aumentar a proteção do usuário.

13 - Instituto Access - 2025 - UFAC - Técnico em Laboratório - Área: Anatomia Animal:
Durante uma campanha de phishing, vários usuários clicaram em links de e-mails falsos e acabaram baixando arquivos maliciosos.
Após a execução, o sistema foi bloqueado e uma mensagem exigia pagamento em criptomoedas para liberar o acesso aos arquivos. É correto afirmar que esse tipo de ameaça é classificado como:

(A) Ransomware.
(B) Rootkit.
(C) Vírus stealth.
(D) Adware.
(E) Botnet.

14 - UNIFAL-MG - 2025 - UNIFAL-MG - Administrador:
Durante o expediente, profissionais de diversas áreas utilizam computadores conectados à internet, o que os expõe a diferentes tipos de ameaças virtuais.
Conhecer as características dessas ameaças é essencial para garantir a segurança da informação no ambiente de trabalho.
Em relação a tipos de vírus, ameaças virtuais e soluções de segurança, é adequado afirmar que:

(A) Spam é um antivírus gratuito usado em webmails.
(B) Spyware é um tipo de firewall usado para proteger o computador.
(C) Ransomware é um recurso de segurança do navegador Google Chrome.
(X) Worms são programas que se autorreplicam e se espalham sem ação do usuário.

15 - Instituto Consulplan - 2025 - CISBAF - RJ - Técnico Administrativo:
Considere que certo servidor abriu um link suspeito de determinado e-mail e foi redirecionado para uma página que solicitava dados bancários.
Esse tipo de golpe na internet é conhecido como:

(A) Vírus.
(X) Phishing.
(C) Ransomware.
(D) Cavalo de Troia.

16 - FGV - 2025 - TCE-PE - Analista de Controle Externo - Tecnologia da Informação:
Para proteger dados sensíveis contra acessos não autorizados utilizam-se mecanismos de autenticação, criptografia e certificação digital, entre outras técnicas.
Com relação à segurança da informação, analise as afirmativas a seguir.
I. A autenticação multifator eleva a segurança de sistemas ao exigir a combinação de dois ou mais fatores de autenticação distintos, como algo que o usuário sabe, algo que possui e algo que é.
II. Na criptografia simétrica, cada parte da comunicação usa um par de chaves diferentes - uma pública e uma privada - para criptografar e descriptografar mensagens.
III. A certificação digital utiliza uma estrutura chamada Infraestrutura de Chaves Públicas (PKI) e serve para associar uma identidade a uma chave pública, por meio de uma Autoridade Certificadora (CA).

Está correto o que se afirma em:

(A) I e II, apenas.
(X) I e III, apenas.
(C) II e III, apenas.
(D) II, apenas.
(E) I, II e III.

17 - IF-MG - 2025 - IF-MG - Assistente de Aluno:
Qual das alternativas apresenta um exemplo válido de autenticação de dois fatores (2FA), ou seja, o uso de dois métodos distintos para confirmar a identidade do usuário?

(A) Uso exclusivo de senha e login para acessar um sistema.
(X) Login com usuário e senha, seguido por um código enviado por SMS.

(C) Acesso ao computador somente com reconhecimento facial.
(D) Login com um token físico, sem necessidade de senha.
(E) Acesso ao celular por Biometria.

18 - FURB - 2025 - Prefeitura de Florianópolis - SC - Auditor Fiscal de Tributos Municipais - Tecnologia da Informação - 2º Dia:
No protocolo OAuth 2.0, qual é o ator responsável por verificar a identidade do usuário final e obter seu consentimento antes de emitir um código de autorização?

(A) Servidor de Recurso (Resource Server).
(B) Usuário Final (Resource Owner).
(C) Cliente (Client Application).
(D) Servidor de Metadados (Metadata Server).
(X) Servidor de Autorização (Authorization Server).

19 - FCC - 2025 - TRF - 4ª REGIÃO - Técnico Judiciário - Área Apoio Especializado - Especialidade: Desenvolvimento de Sistema da Informação:
O Art. 11 da Portaria CNJ nº 253/2020 estabelece que o acesso aos microsserviços deverá ser protegido com mecanismos de autenticação e autorização:

(X) baseados em OAuth2 a ser provido pelo serviço de Single SignOn da PDPJ-Br.
(B) por meio de autenticação de usuário já cadastrado no sistema de processo eletrônico específico do tribunal em que o processo tramita.
(C) e utilizar exclusivamente navegadores de internet homologados pelo Conselho Nacional de Justiça (CNJ).
(D) baseados em SSL a serem providos pelo serviço de suporte operacional da PDPJ-Br.
(E) mediante concórdia com os termos de uso da plataforma no primeiro acesso.

20 - FGV - 2025 - TCE-PE - Auditor de Controle Externo – Tecnologia da Informação:
Considerando a norma ISO/IEC 27002:2022, os atributos dos domínios de segurança do controle “Inventário de informações e outros ativos associados” são:

(A) defesa, apenas.
(B) proteção, apenas.
(C) resiliência e defesa, apenas.
(X) governança, ecossistema e proteção, apenas.
(E) confidencialidade, integridade e disponibilidade, apenas.