MATERIAL ESPECIAL

AULÃO DA MADRUGADA

12 ANOS

QUESTÕES DE INFORMÁTICA E TECNOLOGIA

C

ASSUNTOS TRABALHADOS

- CRIMINOLOGIA DIGITAL | PERFIL DO CRIMINOSO
- LGPD NA INVESTIGAÇÃO | CADEIA DE CUSTÓDIA
- INTELIGÊNCIA CIBERNÉTICA | LOGS E OSINT
- DEEP WEB | INDEXAÇÃO E ACESSO
- PHISHING E RANSOMWARE | BACKUP EM NUVEM
- AMBIENTES CRIMINÓGENOS | VITIMIZAÇÃO DIGITAL
- DNS, FIREWALL E VPN | RESPOSTA A INCIDENTES

AULA AO VIVO | ACESSE PELO QR CODE FINAL

PROFESSOR DEODATO NETO

Informática para concursos públicos | 16 de setembro de 2026

QUESTÃO 01 CRIMINOLOGIA DIGITAL E INVESTIGAÇÃO TECNOLÓGICA

1) Sobre criminologia digital e investigação tecnológica, no âmbito das ciências forenses, analise as afirmativas a seguir.

I. O perfil do criminoso cibernético não corresponde a um estereótipo único, podendo abranger desde indivíduos com elevado conhecimento técnico, capazes de explorar vulnerabilidades complexas, até agentes que se valem primordialmente de técnicas de engenharia social, com conhecimento técnico comparativamente limitado.

II. A deep web e a dark web são conceitos equivalentes, ambos definidos, em sua essência, pela finalidade ilícita do conteúdo neles hospedado, e não pela forma de indexação ou de acesso a esse conteúdo.

III. Redes sociais e outros ambientes digitais podem constituir, a depender do contexto, ambientes digitais criminógenos, potencialmente favoráveis à ocorrência de crimes e à vitimização digital de seus usuários, especialmente daqueles com menor letramento digital.

IV. Logs e metadados associados a um arquivo ou a uma comunicação eletrônica podem constituir evidências eletrônicas relevantes para a investigação tecnológica, desde que devidamente preservados, sendo seu rastreamento e sua análise tarefas típicas da inteligência cibernética voltada à investigação.

V. A técnica de OSINT (Open Source Intelligence), voltada à coleta de dados de fontes abertas, é incompatível com o uso investigativo por órgãos de segurança pública, por não gozar de reconhecimento técnico como método válido de inteligência cibernética.

(A) I, III, IV.

(B) I, II, V.

(C) II, III, IV.

(D) III, IV, V.

(E) II, IV, V.

QUESTÃO 02

PHISHING, RANSOMWARE E BACKUP EM NUVEM

2) Um servidor público recebeu, em seu e-mail corporativo, mensagem aparentemente enviada pelo setor de Tecnologia da Informação de seu órgão — que, dias antes, havia determinado a atualização obrigatória de todos os aplicativos institucionais, por conterem correção de vulnerabilidade recém-descoberta —, informando que sua senha expiraria em 24 horas e solicitando que ele clicasse em um link para "revalidar o acesso". O link direcionava a uma página com layout idêntico ao do sistema interno legítimo, na qual o servidor inseriu suas credenciais. Horas depois, arquivos do setor, armazenados em estação de trabalho com Windows 11, foram criptografados por um agente malicioso, que exigiu pagamento em criptomoeda para restabelecer o acesso. A recuperação dos arquivos mais recentes foi viabilizada, dias depois, graças a uma cópia de segurança mantida em serviço de armazenamento em nuvem, previamente configurado pela equipe de TI.

Os dois eventos maliciosos centrais descritos no cenário correspondem, respectivamente, a

(A) engenharia social e spyware.

(B) pharming e cavalo de troia (trojan).

(C) força bruta e worm.

(D) phishing e ransomware.

(E) spoofing e adware.

QUESTÃO 03

DNS, FIREWALL, VPN E RESPOSTA A INCIDENTES

3) Servidores de uma repartição pública passaram a apresentar lentidão incomum no acesso a sites externos. A equipe de TI constatou que as requisições de tradução de nomes de domínio para endereços IP estavam sendo redirecionadas para um servidor não autorizado, fazendo com que usuários, ao digitarem o endereço correto de um site institucional, fossem levados a uma página fraudulenta com aparência idêntica à original. Para conter o incidente, a equipe implementou regras específicas de bloqueio e liberação de tráfego na borda da rede e passou a exigir que o acesso remoto de servidores externos fosse feito por meio de um túnel criptografado estabelecido sobre a internet. Em razão de o incidente ter potencialmente exposto dados pessoais de cidadãos atendidos pelo órgão, foram também adotadas as medidas de resposta a incidente e de comunicação exigidas pela legislação de proteção de dados pessoais.

As duas medidas técnicas de contenção adotadas pela equipe de TI, na ordem em que foram descritas, correspondem, respectivamente, a

(A) firewall e VPN (rede privada virtual).

(B) proxy reverso e criptografia de disco.

(C) sistema de detecção de intrusão (IDS) e certificado digital.

(D) balanceador de carga e assinatura digital.

(E) antivírus corporativo e autenticação de dois fatores.

QUESTÃO 04

LGPD, OSINT E CADEIA DE CUSTÓDIA

4) No curso de operação policial para apuração de esquema de vazamento e comercialização de dados pessoais de milhares de cidadãos — identificado, em fase inicial, por meio de técnicas de inteligência cibernética e de fontes abertas (OSINT) que localizaram anúncios de venda dos dados em fórum hospedado em ambiente de acesso restrito da internet —, foram apreendidos servidores contendo as bases de dados negociadas. Após apreensão regularmente documentada e com preservação da cadeia de custódia, os peritos criminais realizaram a extração forense dos dados para fins de investigação e instrução processual, restringindo o acesso ao material exclusivamente à equipe técnica responsável pela perícia.

Considerando a LGPD (Lei nº 13.709/2018) e os princípios que regem o tratamento de dados pessoais no âmbito de investigações criminais, é correto afirmar que

(A) o tratamento dos dados pessoais extraídos pelos peritos criminais está totalmente fora do alcance da LGPD, por se tratar de lei voltada, em sua concepção, a relações de consumo e a tratamentos realizados por pessoas jurídicas de direito privado, não havendo, na lei, qualquer previsão aplicável a atividades de persecução penal conduzidas por entes públicos.

(B) o tratamento de dados pessoais para fins de investigação e repressão de infrações penais, realizado por pessoa jurídica de direito público, submete-se a regime próprio, devendo a autoridade competente observar, enquanto não sobrevier diploma específico, os princípios gerais de proteção de dados, tais como finalidade, necessidade e segurança, restringindo o acesso ao estritamente necessário à investigação.

(C) por se tratar de dados obtidos originalmente de bancos de dados públicos, os dados pessoais em questão perdem, a partir de sua apreensão, a natureza de dados pessoais para fins de qualquer proteção legal, tornando-se informação de domínio público sem restrição de uso.

(D) a restrição de acesso ao material exclusivamente à equipe técnica de perícia é medida sem relevância jurídica, podendo os dados pessoais apreendidos no curso de investigação criminal ser livremente compartilhados entre todos os órgãos públicos envolvidos, direta ou indiretamente, na apuração.

(E) a LGPD exige, em qualquer hipótese, o consentimento prévio dos titulares dos dados pessoais como condição indispensável para que peritos criminais possam realizar a extração forense de bases de dados apreendidas no curso de investigação criminal.

QUESTÃO 05

DEEP WEB: INDEXAÇÃO E ACESSO

5) Sobre a deep web, analise as afirmativas a seguir.

I. A deep web compreende todo o conteúdo da internet não indexado pelos mecanismos de busca convencionais, categoria que abrange, predominantemente, conteúdo lícito, como bancos de dados acadêmicos, sistemas internos de organizações e caixas de correio eletrônico.

II. O acesso a conteúdos hospedados na deep web pressupõe, em todos os casos, a utilização de navegadores ou de softwares específicos de anonimização, não sendo possível o acesso a esse tipo de conteúdo por meio de um navegador convencional.

III. Um extrato bancário disponibilizado a um correntista mediante autenticação em um sistema de internet banking é exemplo de conteúdo tipicamente classificado como pertencente à deep web, por não ser indexado nem acessível a mecanismos de busca convencionais.

IV. A extensão da deep web, em termos de volume de dados, é, segundo estimativas amplamente aceitas na literatura especializada, significativamente inferior à da chamada surface web (internet indexada e de acesso público), invertendo-se essa proporção apenas no caso específico da dark web.

V. A existência da deep web decorre, em essência, de uma característica técnica de indexação, a ausência de rastreamento do conteúdo por robôs de busca (crawlers), e não necessariamente da natureza lícita ou ilícita do conteúdo nela hospedado.

(A) I, III, V.

(B) I, II, IV.

(C) II, III, V.

(D) III, IV, V.

(E) I, II, III.

AULÃO DA MADRUGADA 12 ANOS

A AULA É AO VIVO.
A APROVAÇÃO É O FOCO.

AULA AO VIVO | ENTRE PELO QR CODE

ESTUDE COM O PROFESSOR DEODATO NETO

16 de setembro de 2026

Questões estratégicas, explicação direta e foco na sua aprovação

TRANSFORMANDO SONHOS EM APROVAÇÕES

INSTAGRAM

@profdeodatoneto

WHATSAPP

67 99217-6565

SITE

Acesse o portal

AULA AO VIVO

Acesse a aula ao vivo

APONTE A CÂMERA E ENTRE NA AULA.

Professor Deodato Neto | Informática para concursos públicos