O P R O T O C O L O

PACOTE OPERACIONAL · CONCURSO PCPR 2026 · BANCA FGV

DOSSIÊ VERMELHO

01

TECNOLOGIA, SEGURANÇA CIBERNÉTICA E CRIMES DIGITAIS

1/6	25	57
MÓDULO NESTA AMOSTRA	QUESTÕES NA PROVA · COMPLETO	ITENS DO ANEXO I · COMPLETO

AMOSTRA GRATUITA
compartilhe à vontade · venda proibida

AGENTE DE POLÍCIA JUDICIÁRIA · PROVA 11/OUT/2026
AMOSTRA GRATUITA · MÓDULO 1 DE 6

MÓDULO 1

01 SEGURANÇA DA INFORMAÇÃO

Tec 1.4 — centro de gravidade previsto

POR QUE ISSO DERRUBA GENTE Todo mundo chega aqui achando que "sabe segurança da informação" porque usa antivírus em casa. Aí a FGV coloca cinco palavras parecidas na mesma questão — confidencialidade, integridade, autenticidade, autorização, rastreabilidade — e o candidato que estudou "por cima" marca o vizinho. É como confundir o conduzido com a testemunha no auto: os dois estão na delegacia, mas cada um tem um papel que não se troca. No corpus de 370 questões, este é o subtema líder da informática policial de 2025, e o distrator preferido da banca é sempre o conceito verdadeiro da porta ao lado (GD-01/GD-02). Quem discrimina o par, pontua; quem decorou definição solta, escorrega.

CONCEITO 1.1 os pilares e seus vizinhos

Os pilares da segurança da informação são os "princípios de plantão" do dado: cada um protege o dado contra UM tipo de ataque, e a banca vive perguntando qual pilar foi ferido em determinado cenário. Pense na delegacia: o inquérito trancado no armário do escrivão é confidencialidade (só quem pode, acessa); a certeza de que ninguém rasurou uma folha do inquérito é integridade; o sistema estar no ar quando o plantonista precisa lavrar o APF é disponibilidade. Se você consegue apontar QUAL pilar caiu em cada cena de delegacia, já resolve a maior parte das questões deste bloco.

Pilar	O que garante	Vizinho com que a banca troca
Confidencialidade	só quem pode, acessa	integridade (GD-01)
Integridade	o dado não foi alterado	disponibilidade
Disponibilidade	acessível quando necessário	confidencialidade
Autenticidade	quem diz ser, é	autorização
Rastreabilidade	dá para reconstruir quem fez o quê (logs/auditoria)	autenticidade
Irretratabilidade (não repúdio)	o autor não pode negar a autoria	autenticidade

Os 5 primeiros são a redação literal do edital (Tec 1.4) — decorar NESTA ordem de vocabulário.

Tríade de controle de acesso — a distinção que paga questão: - **Autenticação** = provar QUEM você é (senha, biometria, token) - **Autorização** = definir O QUE você pode fazer (perfis, permissões) - **Auditoria/logs** = registrar O QUE foi feito (rastreabilidade)

A tríade é a portaria da delegacia em três atos: o policial mostra a funcional na entrada (autenticação — quem é), o sistema define que ele consulta boletins mas não altera laudos (autorização — o que pode), e tudo que ele fez fica no livro de registro digital (auditoria — o que fez). A FGV adora dar um cenário com os três atos e pedir o nome de cada um — quem decora só a palavra, sem a pergunta que cada uma responde, permuta autenticação com autorização.

Fatores de autenticação: **conhecimento** (senha) · **posse** (token, celular) · **inerência** (biometria). MFA = 2+ fatores DIFERENTES (senha + PIN = 1 fator só, ambos conhecimento CASCA).

> **ERRO COMUM:** o candidato pensa que "duas senhas = dois fatores", mas MFA exige fatores de CATEGORIAS diferentes — senha + PIN continuam sendo um único fator (conhecimento).

EXEMPLO RESOLVIDO 1 — "A funcional e o perfil" (padrão caso-prático FGV)

Enunciado: O investigador Cardoso acessa o sistema da unidade com login, senha e leitura de digital; consegue consultar ocorrências, mas o sistema nega a edição de laudos; toda consulta fica registrada com data e matrícula. Os três mecanismos correspondem, respectivamente, a: *Como o instrutor raciocina:* pergunte a cada mecanismo QUAL pergunta ele responde. Login+senha+digital respondem "quem é você?" → autenticação (e note: senha = conhecimento, digital = inerência → isto é MFA). Negar edição responde "o que você pode?" → autorização. Registro com matrícula responde "o que foi feito?" → auditoria/rastreabilidade. *Por que cada distrator cai:* - "autorização / autenticação / auditoria" → swap GD-01 clássico: inverte as duas primeiras. - "autenticação / auditoria / autorização" → atribui à restrição de edição a função de registro. - "identificação / criptografia / backup" → vocabulário de outro bloco, fora da tríade.

CONCEITO 1.2

criptografia

> ◆ ZM **BASE EM 30 SEGUNDOS — chave criptográfica** *(já domina? pula.)* Chave é uma sequência de caracteres — uma senha matemática — usada por um algoritmo para transformar dado legível em ilegível (cifrar) e de volta (decifrar). Quanto maior e mais aleatória a chave, mais difícil quebrá-la por tentativa. É o segredo que só quem tem autorização conhece: a variável que faz a mesma fórmula produzir resultados diferentes para pessoas diferentes.

Criptografia é o lacre do envelope: transforma o conteúdo em algo ilegível para quem intercepta. A divisão que a banca cobra é UMA: quantas chaves o esquema usa. Na simétrica, remetente e destinatário compartilham a MESMA chave — rápida, mas alguém precisa entregar essa chave sem interceptação (o "problema da distribuição"). Na assimétrica, cada pessoa tem um PAR: a chave

pública (que qualquer um conhece, como o telefone do plantão) e a privada (que só o dono guarda, como a chave do armário de armas).

	Simétrica	Assimétrica
Chaves	**UMA** (compartilhada)	**PAR** (pública + privada)
Velocidade	rápida	lenta
Exemplo	AES	RSA
Problema	distribuir a chave	desempenho

As duas frases que resolvem 90% das questões: 1. Para **sigilo**: cifra-se com a chave **PÚBLICA do DESTINATÁRIO** (só a privada dele abre) — cobrado literal na PC-MG 2025 Q23 ✓ fonte. 2. Para **assinatura digital**: assina-se com a **PRIVADA do REMETENTE** (qualquer um verifica com a pública dele) → garante autenticidade + integridade + não repúdio, **não garante sigilo** CASCA.

> **ERRO COMUM:** o candidato pensa que assinatura digital "protege o conteúdo", mas ela só prova QUEM assinou e QUE nada mudou — o texto assinado continua legível para qualquer um; sigilo exige cifrar por cima.

Hash ≠ criptografia: função **unidirecional** (não se "descriptografa"), saída de tamanho fixo, qualquer alteração muda o resultado → uso: **integridade** (e cadeia de custódia digital, Módulo 3). Pense no hash como o lacre numerado do saco de evidências: ele não esconde o que está dentro — ele denuncia se alguém mexeu. Certificado digital = documento eletrônico que vincula chave pública a um titular, emitido por AC dentro da **ICP-Brasil** — é a "carteira funcional" da chave pública: alguém de confiança atesta que aquela chave pertence mesmo àquela pessoa.

> ◆ **SINAPSE → Dossiê Vermelho 03 (Ciências Forenses) · Módulo 3.2 (cadeia de custódia física, CPP 158-A a 158-F)** O hash que você acabou de ver aqui — o lacre numerado do saco de evidências digital — cumpre exatamente a mesma função que o lacre físico e o formulário de cadeia de custódia cumprem no Dossiê 03: provar que ninguém alterou o vestígio entre a coleta e a perícia. As DEZ etapas do art. 158-B (reconhecimento → isolamento → fixação → coleta → acondicionamento → transporte → recebimento → processamento → armazenamento → descarte) são as MESMAS para uma arma apreendida e para um HD apreendido — muda só o instrumento de garantia: lacre físico de um lado, hash do outro. Se a FGV cruzar os dois cenários, o critério de integridade é idêntico nos dois dossiês.

EXEMPLO RESOLVIDO 2 — "O ofício sigiloso" (derivado da PC-MG 2025 Q23 ✓ fonte)

Enunciado: A escrivã Helena precisa enviar ao delegado Souza, por canal inseguro, um relatório sigiloso, usando criptografia assimétrica. Para que somente Souza possa ler, Helena deve cifrar o relatório com: *Como o instrutor raciocina:* sigilo = só o destinatário abre. A única chave que SÓ Souza possui é a privada DELE — logo, cifra-se com o par correspondente que todos conhecem: a **pública de Souza**. Regra de bolso: sigilo olha para o destinatário; assinatura olha para o remetente. *Por que cada distrator cai:* - "chave privada de Helena" → isso é assinatura (autenticidade), não sigilo. - "chave pública de Helena" → cifraria para a própria Helena abrir; Souza não lê. - "chave privada de Souza" → Helena não tem acesso à privada de terceiro; inverteu o par. - "chave única compartilhada" → migrou para a simétrica; o enunciado fixou assimétrica.

CONCEITO 1.3 malware (a tabela dos pares gêmeos CASCA CB-16)

Malware é o gênero; as pragas da tabela são as espécies — e a questão FGV nunca pergunta "o que é malware", ela dá o comportamento e cobra a espécie exata. O truque de leitura: cada praga tem UMA assinatura discriminante (a coluna do meio). Vírus precisa de carona (hospedeiro + execução); worm anda sozinho pela rede; trojan entra pela porta da frente porque o usuário o convidou achando que era software legítimo — como o falso entregador que o próprio morador manda subir.

Praga	Assinatura discriminante	Não confundir com
Vírus	precisa de **hospedeiro** (infecta arquivo/programa) e de execução	worm
Worm	**autônomo** — propaga-se sozinho pela rede, sem hospedeiro	vírus (PC-MG Q21 ✓ fonte)
Trojan	**disfarce** — parece programa legítimo, o usuário instala	vírus/worm (não se autorreplica)
Ransomware	**cifra os dados** e exige resgate	—
Spyware / keylogger	espiona / registra teclas	trojan (pode vir dentro de um)
Rootkit	**esconde** a presença do invasor (apaga rastros, privilégio)	backdoor
Backdoor	porta de retorno para acesso futuro	rootkit
Bot/botnet	máquina zumbi controlada remotamente (dispara DDoS/spam)	worm

> **ERRO COMUM (CB-16):** o candidato pensa que "trojan se espalha como vírus", mas o trojan NÃO se autorreplica — ele depende de o usuário instalá-lo; autorreplicação é assinatura de vírus (com hospedeiro) e worm (sem).

Ataques sem código: engenharia social (explorar o humano) · **phishing** (isca genérica por e-mail/mensagem) · **spear phishing** (alvo específico, personalizado) · **smishing/vishing** (SMS/voz) · **pharming** (envenena o **DNS** — a vítima digita o endereço CERTO e cai no site falso CASCA par com phishing) · **DoS/DDoS** (derrubar disponibilidade; DDoS = distribuído, via botnet) · **força bruta** (tentativa exaustiva de senhas) · **MITM** (interceptação no meio do caminho).

A régua para separar a família phishing: quem errou primeiro? No phishing, a vítima CLICOU numa isca; no pharming, a vítima fez tudo certo — digitou o endereço correto — e a infraestrutura (DNS) a traiu. É a diferença entre a vítima que segue um mapa falso entregue pelo golpista (phishing) e a que segue o mapa oficial adulterado na parede (pharming).

> **ERRO COMUM (phishing×pharming, GD-01):** o candidato pensa "site falso = phishing", mas se o enunciado diz que a vítima digitou o endereço CORRETO e mesmo assim caiu na página falsa, é pharming — o veneno está no DNS, não na isca.

EXEMPLO RESOLVIDO 3 — "A praga sem hospedeiro" (derivado da PC-MG 2025 Q21 ✓fonte)

Enunciado: O setor de informática da delegacia detecta um programa malicioso que se propaga automaticamente pela rede interna, contaminando as máquinas do cartório sem se anexar a nenhum arquivo e sem qualquer ação dos usuários. Trata-se de: *Como o instrutor raciocina:* duas assinaturas no enunciado — "sem se anexar a arquivo" (elimina vírus) e "sem ação dos usuários" (elimina trojan, que depende de instalação voluntária). Propagação autônoma pela rede = **worm**, fechado. *Por que cada distrator cai:* - "vírus" → o gêmeo GD-01: vírus EXIGE hospedeiro e execução, ambos negados no enunciado. - "trojan" → exige o disfarce e o clique do usuário, expressamente ausentes. - "ransomware" → ninguém cifrou dados nem pediu resgate. - "spyware" → não há coleta oculta de informação descrita, só propagação.

CONCEITO 1.4 defesas

Defesas são os postos de controle da rede — e cada uma tem um verbo próprio, que é exatamente onde a banca troca. O firewall é a guarita na entrada: decide quem passa segundo regras. O IDS é a câmera de vigilância: VÊ e AVISA, mas não age. O IPS é o vigilante armado: vê E intervém. A VPN é a escolta cifrada: protege o trajeto do dado pela via pública, mas não torna o passageiro invisível.

- **Firewall**: filtra tráfego por regras. **Stateless** (analisa pacote a pacote, porta/IP) × **stateful** (acompanha o estado da conexão) — a FGV cobrou cenário de regras com portas na TRT-24 Q51 ✓fonte.

- **IDS** = **detecta** e alerta × **IPS** = detecta e **bloqueia** CASCA (GD-02 — um caractere de diferença).

> **ERRO COMUM (IDS×IPS):** o candidato pensa que "os dois protegem, tanto faz", mas a banca cobra o verbo: quem SÓ registra/alerta é o IDS; atribuir ao IPS a conduta passiva (ou vice-versa) é a casca da T24-II.

- **Antivírus** (assinaturas + heurística) · **proxy** (intermediário, filtro/cache) · **VPN** = túnel **cifrado** sobre rede pública — dá confidencialidade, não anonimato absoluto CASCA (GD-10: "garante anonimato total" = falso).

> **ERRO COMUM (VPN, GD-10):** o candidato pensa que VPN = navegação anônima, mas ela cifra o CANAL; o provedor da VPN e os serviços acessados ainda podem identificar o usuário — "anonimato total" é o advérbio absolutizador que derruba.

- **Backup**: **completo** × **incremental** (copia o alterado desde o ÚLTIMO backup de qualquer tipo — restauração mais lenta, cópia mais rápida) × **diferencial** (desde o último COMPLETO — cresce a cada dia) CASCA par clássico GD-01.

> **ERRO COMUM (incremental×diferencial):** o candidato pensa que os dois "copiam só o que mudou" e para de ler, mas a referência é diferente — incremental olha para o último backup DE QUALQUER TIPO; diferencial olha sempre para o último COMPLETO.

EXEMPLO RESOLVIDO 4 — "O sensor que só avisou"

Enunciado: Na rede da unidade, um equipamento identificou tráfego suspeito vindo de um IP externo, registrou o evento e emitiu alerta ao administrador, sem interromper a comunicação. Outro equipamento, diante do mesmo padrão, encerrou a conexão automaticamente. Os equipamentos são, respectivamente: *Como o instrutor raciocina:* sublinhe os verbos. "Registrou e alertou, sem interromper" = conduta passiva = **IDS**. "Encerrou automaticamente" = conduta ativa = **IPS**. A sigla acompanha o verbo: Detection × Prevention. *Por que cada distrator cai:* - "IPS e IDS" → o swap GD-02 puro, definições permutadas. - "firewall e proxy" → firewall filtra por REGRAS prévias, não por detecção de padrão suspeito; proxy é intermediário, não sensor. - "antivírus e VPN" → planos errados: um atua em arquivos, o outro é túnel cifrado.

APLICAÇÃO 1.5 (o verniz policial que a PC-MG 2025 confirmou)

Servidor da delegacia recebe e-mail "do banco" pedindo atualização de senha → phishing (se veio SMS: smishing; se a página falsa apareceu com o endereço correto digitado: pharming). Sistema da unidade fora do ar por sobrecarga de requisições → ataque à **disponibilidade** (DDoS). Planilha de inquérito alterada sem registro → quebra de **integridade** + falha de **rastreabilidade** (logs).

CASCAS 1.6 CASCAS DO MÓDULO

- **CB-16** (pares gêmeos) — **ERRO COMUM:** o candidato decora definições isoladas e não treina o CONTRASTE; a questão nunca traz uma praga só, traz o par, e a alternativa errada é a definição verdadeira do gêmeo.
- **GD-01** (swap simétrico: simétrica↔assimétrica, IDS↔IPS, incremental↔diferencial, phishing↔pharming) — **ERRO COMUM:** o candidato lê a alternativa, reconhece vocabulário correto e marca; o erro não está nas palavras, está em QUEM faz o quê.
- **GD-02** (sigla vizinha: WPA2/WPA3/WEP — Módulo 4) — **ERRO COMUM:** o candidato pensa que uma letra ou número a mais "é detalhe", mas a FGV monta a alternativa inteira sobre esse caractere.
- **GD-10** (absolutizador: "o antivírus impede QUALQUER infecção", "a VPN garante anonimato TOTAL" = falsos) — **ERRO COMUM:** o candidato aceita a frase porque a primeira metade é verdadeira; o "sempre/total/qualquer" no fim é o veneno.
- **GD-12** (atribuir ao hash função de cifra reversível) — **ERRO COMUM:** o candidato pensa que hash "criptografa e depois descriptografa", mas hash é via de mão única: serve para conferir integridade, nunca para recuperar o conteúdo.

▸ **PERGUNTE AO INSTRUTOR:** *"Numa questão que descreve login com senha e leitura de digital ao mesmo tempo, isso conta como MFA ou como um fator só?"* → https://oprotocolo.ia.br *"Qual a diferença prática entre cifrar com a chave pública do destinatário e assinar com a chave privada do remetente — e como não trocar as duas na hora da prova?"* → https://oprotocolo.ia.br

FICOU DÚVIDA NESTE MÓDULO?

Pergunte ao **VEKETOR**, o instrutor da Operação — ele explica no seu nível e cita a fonte de cada resposta.

→ oprotocolo.ia.br · diga: "módulo 1 do dossiê de Tecnologia"

ISTO FOI 1 MÓDULO DE 6

Você acabou de ler o Módulo 1 completo do Dossiê VERMELHO 01 — TECNOLOGIA, SEGURANÇA CIBERNÉTICA — E CRIMES DIGITAIS. O pacote operacional cobre os outros 5 módulos deste dossiê e mais 8 dossiês inteiros.

O QUE TEM NO PACOTE OPERACIONAL COMPLETO

- **9 dossiês** — cobertura completa dos blocos do edital, não só este
- **318+ páginas** densificadas — sem enchimento, cada seção resolve uma casca real da FGV
- Exemplos resolvidos no formato caso-prático FGV, com o raciocínio do instrutor e o porquê de cada distrator, do jeito que você acabou de ver neste módulo
- Instrutor IA — o **VEKETOR** — que responde dúvida dentro do próprio material, citando a fonte de cada resposta
- Curadoria calibrada sobre **370 questões FGV reais** — cascas e pares confundíveis mapeados, não achismo

PRÓXIMO PASSO

Esta amostra é só a ponta do pacote.

→ CONHECER O PACOTE · oprotocolo.ia.br/#pacote

→ TESTAR O INSTRUTOR · oprotocolo.ia.br