5

PETROBRAS TRANSPORTE S.A.
TRANSPETRO

Processo Seletivo Público - Edital Nº 02 - TRANSPETRO/ PSP/TERRA/NÍVEL SUPERIOR - 2023.2, de 29 de setembro de 2023.

# ANÁLISE DE SISTEMAS - SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

## LEIA ATENTAMENTE AS INSTRUÇÕES ABAIXO.

**01 -** O candidato recebeu do fiscal o seguinte material:

**a)** este **CADERNO DE QUESTÕES**, com o enunciado das 70 (setenta) questões objetivas, sem repetição ou falha, com a seguinte distribuição:

| Conhecimentos Básicos | | | | Conhecimentos Específicos | |
|---|---|---|---|---|---|
| Língua Portuguesa | | Língua Inglesa | | | |
| Questões | Pontuação | Questões | Pontuação | Questões | Pontuação |
| 1 a 10 | 1,0 cada | 11 a 20 | 1,0 cada | 21 a 70 | 1,0 cada |
| Total: 20,0 pontos | | | | Total: 50,0 pontos | |
| Total: 70,0 pontos | | | | | |

**b) CARTÃO-RESPOSTA** destinado às respostas das questões objetivas formuladas nas provas.

**02 -** O candidato deve verificar se este material está em ordem e se o seu nome e número de inscrição conferem com os que aparecem no **CARTÃO-RESPOSTA**. Caso não esteja nessas condições, o fato deve ser **IMEDIATAMENTE** notificado ao fiscal.

**03 -** Após a conferência, o candidato deverá assinar, no espaço próprio do **CARTÃO-RESPOSTA**, com **caneta esferográfica de tinta preta, fabricada em material transparente**.

**04 -** No **CARTÃO-RESPOSTA**, a marcação das letras correspondentes às respostas certas deve ser feita cobrindo a letra e preenchendo todo o espaço compreendido pelos círculos, com **caneta esferográfica de tinta preta, fabricada em material transparente**, de forma contínua e densa. A leitura ótica do **CARTÃO-RESPOSTA** é sensível a marcas escuras; portanto, os campos de marcação devem ser preenchidos completamente, sem deixar claros.

Exemplo: Ⓐ ● Ⓒ Ⓓ Ⓔ

**05 -** O candidato deve ter muito cuidado com o **CARTÃO-RESPOSTA**, para não o **DOBRAR, AMASSAR ou MANCHAR**. O **CARTÃO-RESPOSTA SOMENTE** poderá ser substituído se, no ato da entrega ao candidato, já estiver danificado.

**06 -** Imediatamente após a autorização para o início das provas, o candidato deve conferir se este **CADERNO DE QUESTÕES** está em ordem e com todas as páginas. Caso não esteja nessas condições, o fato deve ser **IMEDIATAMENTE** notificado ao fiscal.

**07 -** As questões objetivas são identificadas pelo número que se situa acima de seu enunciado.

**08 -** Para cada uma das questões objetivas, são apresentadas 5 alternativas classificadas com as letras (A), (B), (C), (D) e (E); só uma responde adequadamente ao quesito proposto. O candidato só deve assinalar **UMA RESPOSTA**: a marcação em mais de uma alternativa anula a questão, **MESMO QUE UMA DAS RESPOSTAS ESTEJA CORRETA**.

**09 - SERÁ ELIMINADO** deste Processo Seletivo Público o candidato que:

**a)** for surpreendido, durante as provas, em qualquer tipo de comunicação com outro candidato;

**b)** portar ou usar, durante a realização das provas, aparelhos sonoros, fonográficos, de comunicação ou de registro, eletrônicos ou não, tais como agendas, relógios de qualquer natureza, *notebook*, transmissor de dados e mensagens, máquina fotográfica, telefones celulares, *pagers*, microcomputadores portáteis e/ou similares;

**c)** se ausentar da sala em que se realizam as provas levando consigo o **CADERNO DE QUESTÕES** e/ou o **CARTÃO-RESPOSTA**;

**d)** se recusar a entregar o **CADERNO DE QUESTÕES** e/ou o **CARTÃO-RESPOSTA**, quando terminar o tempo estabelecido;

**e)** não assinar a **LISTA DE PRESENÇA** e/ou o **CARTÃO-RESPOSTA.**

**Obs.** O candidato só poderá ausentar-se do recinto das provas após **2 (duas) horas** contadas a partir do efetivo início das mesmas. Por motivos de segurança, o candidato **NÃO PODERÁ LEVAR O CADERNO DE QUESTÕES**, a qualquer momento.

**10 -** O candidato deve reservar os 30 (trinta) minutos finais para marcar seu **CARTÃO-RESPOSTA**. Os rascunhos e as marcações assinaladas no **CADERNO DE QUESTÕES NÃO SERÃO LEVADOS EM CONTA**.

**11 -** O candidato deve, ao terminar as provas, entregar ao fiscal o **CADERNO DE QUESTÕES** e o **CARTÃO-RESPOSTA** e **ASSINAR A LISTA DE PRESENÇA.**

**12 - O TEMPO DISPONÍVEL PARA ESTAS PROVAS DE QUESTÕES OBJETIVAS É DE 4 (QUATRO) HORAS E 30 (TRINTA) MINUTOS,** já incluído o tempo para marcação do seu **CARTÃO-RESPOSTA**, findo o qual o candidato deverá, obrigatoriamente, entregar o **CARTÃO-RESPOSTA** e o **CADERNO DE QUESTÕES**.

**13 -** As questões e os gabaritos das Provas Objetivas serão divulgados a partir do primeiro dia útil após sua realização, na página da **FUNDAÇÃO CESGRANRIO (www.cesgranrio.org.br)**.

## CONHECIMENTOS BÁSICOS

## LÍNGUA PORTUGUESA

### À moda brasileira

1 Estou me vendo debaixo de uma árvore, lendo a pequena história da literatura brasileira.

2 Olavo Bilac! – eu disse em voz alta e de repente parei quase num susto depois que li os primeiros versos do soneto à língua portuguesa: Última flor do Lácio, inculta e bela / És, a um tempo, esplendor e sepultura.

3 Fiquei pensando, mas o poeta disse sepultura?! O tal de Lácio eu não sabia onde ficava, mas de sepultura eu entendia bem, disso eu entendia, repensei baixando o olhar para a terra. Se escrevia (e já escrevia) pequenos contos nessa língua, quer dizer que era a sepultura que esperava por esses meus escritos?

4 Fui falar com meu pai. Comecei por aquelas minhas sondagens antes de chegar até onde queria, os tais rodeios que ele ia ouvindo com paciência enquanto enrolava o cigarro de palha, fumava nessa época esses cigarros. Comecei por perguntar se minha mãe e ele não tinham viajado para o exterior.

5 Meu pai fixou em mim o olhar verde. Viagens, só pelo Brasil, meus avós é que tinham feito aquelas longas viagens de navio, Portugal, França, Itália... Não esquecer que a minha avó, Pedrina Perucchi, era italiana, ele acrescentou. Mas por que essa curiosidade?

6 Sentei-me ao lado dele, respirei fundo e comecei a gaguejar, é que seria tão bom se ambos tivessem nascido lá longe e assim eu estaria hoje escrevendo em italiano, italiano! – fiquei repetindo e abri o livro que trazia na mão: Olha aí, pai, o poeta escreveu com todas as letras, nossa língua é sepultura mesmo, tudo o que a gente fizer vai para debaixo da terra, desaparece!

7 Calmamente ele pousou o cigarro no cinzeiro ao lado. Pegou os óculos. O soneto é muito bonito, disse me encarando com severidade. Feio é isso, filha, isso de querer renegar a própria língua. Se você chegar a escrever bem, não precisa ser em italiano ou espanhol ou alemão, você ficará na nossa língua mesmo, está me compreendendo? E as traduções? Renegar a língua é renegar o país, guarde isso nessa cabecinha. E depois (ele voltou a abrir o livro), olha que beleza o que o poeta escreveu em seguida, Amo-te assim, desconhecida e obscura, veja que confissão de amor ele fez à nossa língua! Tem mais, ele precisava da rima para sepultura e calhou tão bem essa obscura, entendeu agora? – acrescentou e levantou-se. Deu alguns passos e ficou olhando a borboleta que entrou na varanda: Já fez a sua lição de casa?

8 Fechei o livro e recuei. Sempre que meu pai queria mudar de assunto ele mudava de lugar: saía da poltrona e ia para a cadeira de vime. Saía da cadeira de vime e ia para a rede ou simplesmente começava a andar. Era o sinal, Não quero falar nisso, chega. Então a gente falava noutra coisa ou ficava quieta.

9 Tantos anos depois, quando me avisaram lá do pequeno hotel em Jacareí que ele tinha morrido, fiquei pensando nisso, ah! se quando a morte entrou, se nesse instante ele tivesse mudado de lugar. Mudar depressa de lugar e de assunto. Depressa, pai, saia da cama e fique na cadeira ou vá pra rua e feche a porta!

TELLES, Lygia Fagundes. **Durante aquele estranho chá**: perdidos e achados. Rio de Janeiro: Rocco, 2002, p.109-111. Fragmento adaptado.

**1**

O fragmento de abertura da crônica “Estou me vendo debaixo de uma árvore, lendo a pequena história da literatura brasileira.” (parágrafo 1) faz referência a uma

(A) previsão
(B) fantasia
(C) esperança
(D) expectativa
(E) reminiscência

**2**

No texto, as palavras que marcam o sentimento de insegurança vivenciado pela narradora ao conversar com seu pai são:

(A) confissão (parágrafo 7) e andar (parágrafo 8)
(B) rodeios (parágrafo 4) e gaguejar (parágrafo 6)
(C) cabecinha (parágrafo 7) e mudar (parágrafo 8)
(D) sepultura (parágrafo 3) e renegar (parágrafo 7)
(E) severidade (parágrafo 7) e esquecer (parágrafo 5)

**3**

De acordo com o texto, na opinião do pai, a filha deveria

(A) aprender a língua da avó.
(B) valorizar a língua materna.
(C) escrever em idiomas diversos.
(D) ler outros poemas de Olavo Bilac.
(E) estudar história da literatura brasileira.

**4**

Ao ler os versos de Olavo Bilac, o “quase” susto da narradora, mencionado no parágrafo 2, foi motivado pela

(A) possibilidade de seus escritos não serem conhecidos.
(B) falta de conhecimento sobre a localização do Lácio.
(C) necessidade de aprender uma língua diferente.
(D) surpresa com a postura pessimista do poeta.
(E) abordagem da temática da morte.

**5**
O emprego do acento grave em “soneto à língua portuguesa” (parágrafo 2) explica-se a partir do entendimento de que Olavo Bilac escreveu um soneto

(A) em língua portuguesa
(B) com a língua portuguesa
(C) para a língua portuguesa
(D) sobre a língua portuguesa
(E) por causa da língua portuguesa

**6**
A palavra **que** funciona como um mecanismo de coesão textual, retomando um antecedente, em:

(A) “parei quase num susto depois **que** li os primeiros versos”. (parágrafo 2)
(B) “Não esquecer **que** a minha avó, Pedrina Perucchi, era italiana”. (parágrafo 5)
(C) “ficou olhando a borboleta **que** entrou na varanda” (parágrafo 7)
(D) “Sempre **que** meu pai queria mudar de assunto ele mudava de lugar”. (parágrafo 8)
(E) “quando me avisaram lá do pequeno hotel em Jacareí **que** ele tinha morrido”. (parágrafo 9)

**7**
A frase em que as vírgulas estão empregadas com a mesma função que em “Não esquecer que a minha avó, Pedrina Perucchi, era italiana” (parágrafo 5) é:

(A) Mude de lugar, meu pai, porque a morte vai chegar.
(B) A filha, preocupada e triste, questionava a própria língua materna.
(C) A língua portuguesa, embora inculta, constrói belos textos literários.
(D) Os poemas, textos de uma beleza sem igual, encantam seus leitores.
(E) Colocou os óculos e, caminhando pela sala, revelou a beleza do poema.

**8**
Considerando-se a correlação adequada entre tempos e modos verbais, a alternativa que, respeitando a norma-padrão, completa o período iniciado pelo trecho “A autora também teria sido lida se...” é

(A) escrever seus contos em outra língua.
(B) escrevera seus contos em outra língua.
(C) tiver escrito seus contos em outra língua.
(D) teria escrito seus contos em outra língua.
(E) tivesse escrito seus contos em outra língua.

RASCUNHO

**9**
No parágrafo 6, “nossa língua é sepultura mesmo, **tudo o que a gente fizer vai para debaixo da terra, desaparece!**”, o segmento em destaque pode articular-se com o segmento anterior, sem alteração do sentido original, empregando-se o conector

(A) quando
(B) portanto
(C) enquanto
(D) embora
(E) ou

**10**
Em “O soneto é muito bonito, disse me encarando com **severidade**” (parágrafo 7), a palavra que pode substituir **severidade**, sem alteração no sentido da frase, é

(A) firmeza
(B) rispidez
(C) discrição
(D) desgosto
(E) incompreensão

RASCUNHO

Continua

## LÍNGUA INGLESA

### How space technology is bringing green wins for transport

1 Space technology is developing fast, and, with every advance, it is becoming more accessible to industry. Today, satellite communications (satcoms) and space-based data are underpinning new ways of operating that boost both sustainability and profitability. Some projects are still in the planning stages, offering great promise for the future. However, others are already delivering practical results.

2 The benefits of space technology broadly fall into two categories: connectivity that can reach into situations where terrestrial technologies struggle to deliver and the deep, unique insights delivered by Earth Observation (EO) data. Both depend on access to satellite networks, particularly medium earth orbit (MEO) and low earth orbit (LEO) satellites that offer low-latency connectivity and frequently updated data. Right now, the satellite supplier market is booming, driving down the cost of access to satellites. Suppliers are increasingly tailoring their services to emerging customer needs and the potential applications are incredible – as a look at the transportation sector shows.

3 Satellite technology is a critical part of revolutionizing connectivity on trains. The Satellites for Digitalization of Railways (SODOR) project will provide low latency, highly reliable connectivity that, combined with monitoring sensors, will mean near real-time data guides operational decisions. This insight will help trains run more efficiently with fewer delays for passengers. Launching this year, SODOR will help operators reduce emissions by using the network more efficiently, allowing preventative maintenance and extending the lifetime of some existing trains. It will also make rail travel more attractive and help shift more passengers from road to rail (that typically emits even less $CO_2$ per passenger than electric cars do).

4 Satellite data and communications will also play a fundamental role in shaping a sustainable future for road vehicles. Right now, the transport sector contributes around 14% of the UK's greenhouse gas emissions, of which 91% is from road vehicles – and this needs to change.

5 A future where Electric Vehicles (EV) dominate will need a smart infrastructure to monitor and control the electricity network, managing highly variable supply and demand, as well as a large network of EV charging points. EO data will be critical in future forecasting models for wind and solar production, to help manage a consistent flow of green energy.

6 Satellite communications will also be pivotal. As more wind and solar installations join the electricity network – often in remote locations – satcoms will step in to deliver highly reliable connectivity where 4G struggles to reach. It will underpin a growing network of EV charging points, connecting each point to the internet for operational management purposes, for billing and access app functionality and for the users' comfort, they may access the system wherever they are.

7 Satellite technology will increasingly be a part of the vehicles themselves, particularly when automated driving becomes more mainstream. It will be essential for every vehicle to have continuous connectivity to support real-time software patches, map updates and inter-vehicle communications. Already, satellites provide regular software updates to vehicles and enhanced safety through an in-car emergency call service.

8 At our company, we have been deeply embedded in the space engineering for more than 40 years – and we continue to be involved with the state-of-the-art technologies and use cases. We have a strong track record of translating these advances into practical benefits for our customers that make sense on both a business and a sustainability level.

Available at: https://www.cgi.com/uk/en-gb/blog/space/how-space-technology-is-bringing-green-wins-to-transport. Retrieved on April 25, 2023. Adapted.

**11**

The main idea of the text is to

(A) disapprove space technology.
(B) relate space technology to diseases.
(C) figure out the costs of space technology.
(D) list potential dangers of space technology.
(E) describe space technology improvements.

**12**

In the fragment in the first paragraph of the text "**However**, others are already delivering practical results", the word **However** can be associated with the idea of

(A) time
(B) condition
(C) emphasis
(D) opposition
(E) accumulation

**13**

From the fragment in the second paragraph of the text "connectivity that can reach into situations where terrestrial technologies struggle to deliver", it can be concluded that terrestrial technologies can present data problems related to their

(A) price
(B) safety
(C) choice
(D) marketing
(E) transmission

**14**
From the fragment in the second paragraph of the text "Right now, the satellite supplier market is booming, driving down the cost of access to satellites", one can infer that the more access to the satellite supplier market is feasible,

(A) the lower its price will be.
(B) the higher its price will be.
(C) the better its quality will be.
(D) the poorer its quality will be.
(E) the more reliable its quality will be.

**15**
The fragment in the third paragraph of the text "The Satellites for Digitalization of Railways (SODOR) project will provide low latency" means that

(A) low volume of data will be conveyed within hours.
(B) low volume of data will be interrupted for a few minutes.
(C) low volume of data will be communicated within minutes.
(D) high volume of data will be transmitted with minimal delay.
(E) high volume of data will be transferred after a few minutes.

**16**
In the fragment in the fourth paragraph of the text "a sustainable future for road vehicles. Right now, the transport sector contributes around 14% of the UK's greenhouse gas emissions, of **which** 91% is from road vehicles", the word **which** refers to

(A) road vehicles
(B) transport sector
(C) United Kingdom
(D) sustainable future
(E) greenhouse gas emissions

**17**
From the fifth paragraph of the text, one can infer that models for wind and solar production can provide sources of

(A) unreliable power
(B) intermittent energy
(C) constant power flow
(D) scarce energy sources
(E) dangerous power sources

**18**
In the fragment in the sixth paragraph of the text "Satellite communications will also be **pivotal**", the word **pivotal** can be replaced, with no change in meaning, by

(A) tricky
(B) erratic
(C) essential
(D) haphazard
(E) problematic

**19**
From the seventh paragraph of the text, one can infer that automated driving will have the benefits of

(A) human drivers
(B) space technology
(C) terrestrial connectivity
(D) traffic controlled by people
(E) 20$^{th}$ century designed cars

**20**
In the eighth paragraph of the text, the author states that, for the last 40 years, the company where he works has been

(A) embedded in antipollution laws.
(B) dedicated to space travel medicine.
(C) involved with cutting-edge space industry.
(D) concerned with the Earth's polar ice caps.
(E) engaged in antinuclear weapon campaigns.

RASCUNHO

Continua

## CONHECIMENTOS ESPECÍFICOS

**21**

Para proteger as transações eletrônicas contra fraudes, é importante implantar serviços de segurança da informação adequados. É possível, por exemplo, haver proteção contra um tipo de fraude que consiste na negação falsa de envolvimento em uma associação, mais especificamente, uma associação de comunicação que transfere dados.

O serviço de segurança que assegura a proteção contra esse tipo de fraude é a

(A) integridade
(B) confidencialidade
(C) disponibilidade
(D) irretroatividade
(E) irretratabilidade

**22**

O Advanced Encryption Standard (AES) é uma cifra de bloco para aplicações comerciais. Sua especificação define três alternativas para o tamanho de chave: 128, 192 ou 256 bits.

Por outro lado, o AES limita o tamanho do bloco a quantos bits?

(A) 128
(B) 192
(C) 256
(D) 512
(E) 1024

**23**

Diversos conceitos da teoria dos números são essenciais para o projeto de algoritmos de chave pública.

Um exemplo de algoritmo de chave pública que, para sua segurança, depende da dificuldade de se calcular logaritmos discretos é o

(A) Diffie-Hellman
(B) RSA
(C) DES
(D) AES
(E) RC4

**24**

Uma certa infraestrutura de chaves públicas (ICP) define a utilização de uma hierarquia de autoridades certificadoras. Nessa hierarquia, a autoridade certificadora raiz ($AC_{raiz}$) emite apenas o certificado digital da autoridade certificadora do segundo nível da hierarquia ($AC_{n2}$). Por sua vez, a $AC_{n2}$ pode emitir certificado digital para um usuário ($Cert_{usuário}$) dessa ICP.

Para a $AC_{n2}$ assegurar a integridade e a autenticidade do $Cert_{usuário}$ , esse certificado digital deve conter **APENAS** a(s) assinatura(s) digital(is) da(o)

(A) $AC_{raiz}$
(B) $AC_{n2}$
(C) $AC_{raiz}$ e do usuário titular do $Cert_{usuário}$
(D) $AC_{n2}$ e do usuário titular do $Cert_{usuário}$
(E) usuário titular do $Cert_{usuário}$

**25**

O esquema desenvolvido por Rivest, Shamir e Adleman utiliza uma expressão com exponenciais para garantir o sigilo de dados. Considerando-se esse esquema, suponha que os primos *p* e *q* foram escolhidos e que *n* é igual ao produto de *p* * *q*. Sabe-se que a chave pública consiste no par [*e*,*n*], a chave privada consiste no par [*d*,*n*] e o texto cifrado (C) foi gerado a partir da chave pública.

Nesse contexto, o cálculo do texto plano (M) a partir do texto cifrado (C) será

(A) $M = C^p \bmod n$
(B) $M = C^q \bmod n$
(C) $M = C^d \bmod n$
(D) $M = C^n \bmod d$
(E) $M = C^e \bmod d$

**26**

Os algoritmos de resumo de mensagem e de hash são amplamente aplicados na proteção de dados. Esses algoritmos produzem códigos de verificação para os dados com tamanhos variados, tipicamente representados em hexadecimal.

É um exemplo de código produzido pelo algoritmo SHA256 o seguinte código de verificação:

(A) 06afa6c8b54d3cc80d269379d8b6a078
(B) 4d750439e3f39848345c6ef74ef3d719e34e7111
(C) db662d3a62b9d35365d14000c48d087aaee9c904dc18614961a7f02f
(D) ebdf496f67651cddf6aaa1f0b130f1b99ce9e2e93dc2503d926edcff15aee668
(E) 2410b19a07684bf1a6e79a6d2f8bc72b50a992f3992cb2e972c9fc72b472be0fb2174b1bcccde2c318b2a6aa356ada75

**27**
A comunicação segura é essencial para assegurar a proteção dos dados em trânsito nas redes de dados. Nesse contexto, o principal objetivo do Transport Layer Security (TLS) é fornecer um canal seguro entre duas partes que se comunicam.

No TLS, o servidor

(A) é opcionalmente autenticado e o cliente é sempre autenticado.
(B) é sempre autenticado e o cliente nunca é autenticado.
(C) é sempre autenticado e o cliente é sempre autenticado.
(D) é sempre autenticado e o cliente é opcionalmente autenticado.
(E) nunca é autenticado e o cliente é sempre autenticado.

**28**
Para aplicar uma cifra de bloco em diferentes situações, o National Institute of Standards and Technology (NIST) define alguns modos de operações usados para aprimorar o efeito do algoritmo criptográfico ou para adaptar o algoritmo para uma aplicação em particular. Em um desses modos de operação, a primeira entrada do algoritmo criptográfico é o resultado do XOR entre os primeiros 64 bits de texto claro e um vetor de inicialização (IV), e as demais entradas do algoritmo criptográfico são o resultado do XOR entre os próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado.

Esse modo de operação é o

(A) EBC
(B) CBC
(C) CFB
(D) CTR
(E) OFB

**29**
No padrão do Transport Layer Security (TLS), quando um cliente se conecta pela primeira vez a um servidor, o envio da mensagem ClientHello é obrigatório como primeira mensagem TLS. Considere que o servidor ao qual o cliente se conectou é capaz de negociar um conjunto aceitável de parâmetros de handshake com base no conteúdo da mensagem ClientHello.

Nesse caso, o servidor irá responder com a seguinte mensagem:

(A) ServerParamsAccepted
(B) ServerAcknowledge
(C) ServerParamsOk
(D) ServerResponse
(E) ServerHello

RASCUNHO

**30**
No IP Security (IPsec), o cabeçalho de autenticação, Authentication Header (AH), oferece suporte para integridade de dados e para autenticação dos pacotes de IP. O valor de verificação de integridade, Integrity Check Value (ICV), pode ser calculado com um algoritmo de HMAC, mas deverá caber no campo reservado para os dados de autenticação.

Por essa razão, se usarmos o algoritmo HMAC-SHA1, o valor do HMAC deverá ser truncado em quantos bits?

(A) 32
(B) 64
(C) 96
(D) 128
(E) 160

**31**
Um administrador de rede observou uma situação atípica em várias estações da rede local. Nessas estações, o endereço IP do roteador padrão da rede local encontra-se associado, de forma dinâmica, ao endereço físico da interface de rede (MAC Address) de uma estação de trabalho presente na rede local e que está operando como man-in-the-middle. Ele concluiu que a rede estava sendo atacada e que a associação maliciosa descrita estava sendo realizada.

Nesse caso, a técnica de ataque utilizada foi a de

(A) phishing
(B) cryptojacking
(C) eavesdropping
(D) session hijacking
(E) ARP spoofing

**32**
Os registros do Common Weakness Enumeration (CWE) estão se tornando uma base de conhecimento valiosa sobre exposição a vulnerabilidades. Dentre os 25 pontos fracos de softwares, que são considerados os mais perigosos na listagem de 2023, consta a neutralização inadequada de entrada durante a geração de páginas da Web, que pode ser dividida em três principais tipos.

O tipo de neutralização inadequada na qual o cliente realiza a injeção de XSS na página é o

(A) DOM-Based XSS
(B) Reflected XSS
(C) Stored XSS
(D) CRLF Injection
(E) LDAP Injection

Continua

**33**
Assegurar a disponibilidade dos sistemas diante de um ataque de Denial of Service (DoS) é uma tarefa bastante complicada, devido à grande sobrecarga exercida por esse tipo de ataque sobre os sistemas.

Dentre os ataques de DoS, o que causa o consumo excessivo da largura de banda é o

(A) spoofing
(B) snooping
(C) sniffing
(D) flooding
(E) exploiting

**34**
Uma política de segurança de redes efetiva requer o controle de acesso a redes de dados da organização. O padrão do IEEE 802.1X permite fazer esse controle utilizando uma infraestrutura formada pelo suplicante, pelo autenticador e pelo servidor de autenticação. Considere que o suplicante não está devidamente autenticado, e, por isso, o sistema de comunicação está operando de forma limitada, restringindo o uso da rede de comunicação de dados.

Nessa situação, para se comunicar com o autenticador e proceder com o processo de autenticação, o suplicante utilizará o protocolo

(A) DHCP
(B) EAP
(C) SMB
(D) HTTP
(E) HTTPS

**35**
A técnica de escuta (wire tapping) é amplamente utilizada para atacar as redes de comunicação de dados, sendo a escuta passiva uma técnica comum em ataques passivos.

Um exemplo de ataque passivo é a(o)

(A) análise de tráfego
(B) modificação de mensagem
(C) negação de serviço
(D) repetição
(E) disfarce

**36**
Para a realização de um ataque bem direcionado a um alvo, é importante que se colha grande quantidade de informações, e essa etapa de preparação do ataque é conhecida como footprinting. Combinando ferramentas e técnicas, um atacante pode facilmente obter informações públicas sobre os blocos de rede de um domínio e sobre o endereço de contato dos responsáveis por ele.

Uma ferramenta utilizada para essa finalidade é a

(A) ping
(B) nmap
(C) whois
(D) telnet
(E) traceroute

**37**
As organizações estão cada vez mais conscientes sobre os riscos do uso de uma autenticação de usuários com base em um único fator, como, por exemplo, uma senha. Tipicamente, usuários escolhem péssimas senhas para facilitar a sua lembrança no futuro. Comumente, são utilizadas palavras de dicionários combinadas com números ou símbolos, o que facilita os ataques on-line de força bruta. Os hackers utilizam amplamente uma ferramenta que estabelece a comunicação com um serviço de rede e testa a autenticação de usuários usando listas de nomes de login e senhas em busca de uma combinação válida no sistema alvo.

A ferramenta descrita é a

(A) crunch
(B) cewl
(C) samdump2
(D) hydra
(E) bkhive

**38**
Os usuários de um sistema estão sujeitos a ataques de engenharia social. Um vetor comum nesses ataques é o e-mail, usado para atrair alvos a visitarem sites maliciosos ou a fazerem o download de anexos maliciosos, entre outras atividades maliciosas. Um meio de realizar esse tipo de ataque é utilizando uma ferramenta de código aberto, concebida para ajudar na realização dos ataques de engenharia social, permitindo fazer um ataque de spear-phishing.

A ferramenta descrita é o

(A) msfvenom
(B) setoolkit
(C) iptables
(D) burp
(E) ettercap

**39**
Enquanto alguns ataques de Denial of Service (DoS) focam o consumo da largura de banda, outros focam a inanição de recursos. Em um desses ataques de inanição de recursos, o atacante comanda os seus bots para que abram conexões TCP com o servidor alvo e dividam solicitações GET ou POST do protocolo HTTP em vários pacotes ou sessões. Para ser mantida a conexão aberta com o servidor, cabeçalhos HTTP são enviados em cada solicitação, antes que a conexão TCP atinja o tempo limite.

Esse ataque de DoS geralmente é realizado de forma distribuída, sendo conhecido como

(A) smurf
(B) mirai
(C) slowloris
(D) brobot
(E) PoD

**40**
Os códigos maliciosos são construídos para atender a ataques com diferentes finalidades. Muitas vezes, o objetivo do ataque é furtar os dados sensíveis do usuário a partir do monitoramento dos dados fornecidos para uma aplicação, tais como o nome do login e a senha pessoal.

Um código malicioso que tem essa característica é o

(A) trojan
(B) worm
(C) backdoor
(D) keylogger
(E) ransomware

**41**
A varredura de portas é o processo de enviar mensagens para as portas de comunicação dos serviços de rede para identificar quais estão ativos. Há um método de varredura furtiva de porta TCP que usa um zumbi para determinar os serviços ativos no computador alvo, sem deixar rastros, pois o alvo conhecerá apenas o endereço IP desse zumbi.

Esse método é conhecido como TCP

(A) SYN scan
(B) ACK scan
(C) NULL scan
(D) FIN scan
(E) IDLE scan

**42**
A MITRE ATT&CK® tornou-se uma referência global sobre as táticas e técnicas adversárias.

Dentre as técnicas listadas para a tática de persistência, estão as três a seguir:

(A) manipulação de conta, extensões do navegador e implantação de imagem interna
(B) manipulação de conta, extensões do navegador e autenticação forçada
(C) manipulação de conta, interceptação de autenticação multifator e autenticação forçada
(D) extensões do navegador, interceptação de autenticação multifator e autenticação forçada
(E) implantação de imagem interna, interceptação de autenticação multifator e autenticação forçada

**43**
O Internet Protocol Security (IPsec) é um conjunto de protocolos que fornece segurança às comunicações da internet na camada IP.

O protocolo de negociação e de gerenciamento de chaves mais comumente usado para fornecer material de chaves negociado e atualizado dinamicamente para IPsec é o

(A) PPTP
(B) L2TP
(C) IKE
(D) ESP
(E) AH

**44**
No OWASP Top 10, relatório regularmente publicado pela Open Web Application Security Project (OWASP), descrevem-se os riscos de segurança mais críticos encontrados em aplicações web em um certo período de análise. Considere o ambiente de uma aplicação web no qual o servidor da aplicação é fornecido com os sistemas de amostra não removidos do servidor de produção, e os aplicativos de amostra têm falhas de segurança conhecidas, usadas pelos invasores para comprometer o servidor.

Esse cenário evidencia um risco de segurança classificado no OWASP Top 10 2021, na seguinte categoria:

(A) falhas criptográficas
(B) design inseguro
(C) componentes vulneráveis e desatualizados
(D) configuração incorreta de segurança
(E) falhas de registro e monitoramento de segurança

**45**
Um atacante quer atuar como man-in-the-middle (MITM) em uma rede local. Para conseguir executar esse ataque, esse atacante deseja fazer com que o tráfego destinado à rede externa seja enviado para a sua estação de controle. Considere que, na situação apresentada, o switch de acesso não faz nenhum tipo de monitoramento de tráfego de rede nem fornece isolamento entre as estações de trabalho presentes nessa rede local.

Nesse caso, o atacante pode usar a técnica de

(A) Rogue ICMP
(B) Rogue DHCP
(C) Rogue SNMP
(D) SNMP Spoofing
(E) HTTP Spoofing

**46**
Os ataques cibernéticos realizados contra as redes de comunicação de dados exigem uma defesa em profundidade, que é um esquema de proteção no qual se utilizam camadas de segurança compostas por componentes de segurança independentes. Considere que uma rede, na qual é utilizada a defesa em profundidade, está diante de um ataque de inundação no nível de transporte.

Nesse caso, o componente capaz de detectar o ataque e de alertar o centro de monitoramento é o

(A) firewall com estado
(B) firewall sem estado
(C) firewall proxy
(D) gateway VPN
(E) sistema de detecção de intrusão

Continua

**47**

Os ataques cibernéticos empregam várias táticas que consistem em etapas e em ações individuais para atingir um propósito específico. Uma dessas táticas utiliza técnicas para evitar a detecção do ataque durante todo o seu comprometimento, tais como desinstalar/desativar software de segurança ou ofuscar/criptografar dados e scripts.

De acordo com a MITRE ATT&CK®, a tática descrita é a de

(A) reconhecimento
(B) escalação de privilégio
(C) evasão de defesa
(D) acesso inicial
(E) descoberta

**48**

Os usuários tipicamente digitam o endereço do site desejado sem prefixar as URLs com http:// ou https://. Nesses casos, os navegadores tipicamente irão adotar o prefixo http:// e estabelecer uma comunicação insegura com os servidores web. Essa situação é uma oportunidade para o Man-In-The-Middle (MITM) monitorar a comunicação entre o navegador e o servidor web, mesmo que o servidor esteja configurado para redirecionar o navegador a mudar para uma comunicação segura com HTTPS.

Quando o servidor web obriga uma conexão com HTTPS, o MITM pode executar o ataque de SSL Stripping, no qual ele intercepta as requisições em HTTP do navegador e

(A) redireciona o navegador web para um site falsificado do servidor web, usando HTTP, e monitora a comunicação HTTP do início ao fim.
(B) redireciona o navegador web para um site falsificado do servidor web, usando HTTPS, e monitora a comunicação HTTPS do início ao fim.
(C) redireciona o navegador web para o servidor web verdadeiro, usando HTTPS, e monitora a comunicação HTTPS do início ao fim.
(D) força a comunicação HTTP com o servidor web verdadeiro, e a resposta do servidor web, em HTTP, será, então, monitorada e entregue ao navegador web.
(E) faz a comunicação HTTPS com o servidor web verdadeiro, e a resposta do servidor web, em HTTPS, será, então, convertida pelo MITM para HTTP e entregue ao navegador web.

RASCUNHO

**49**

Um ataque é um ato intencional executado por um agente malicioso para evadir os serviços de segurança de um sistema. Esse agente malicioso pode comandar um terceiro agente na execução do ataque às vítimas, e o fluxo de dados malicioso será direcionado às vítimas por esse terceiro agente.

Nesse caso, o método de execução do ataque é classificado como

(A) direto
(B) indireto
(C) off-line
(D) reverso
(E) truncado

**50**

Um atacante ordenou aos seus bots a continuamente estabelecerem inúmeras conexões TCP diretamente com um servidor web alvo, usando um endereço de origem falsificado e inexistente. Todas as solicitações realizadas pelos bots foram recebidas e respondidas por esse servidor alvo durante algum tempo e, agora, não há mais recursos no servidor para responder a novas solicitações de conexão.

Esse servidor alvo está diante de um ataque de TCP

(A) SYN Flood
(B) SYN/ACK Flood
(C) FIND Drain
(D) SEND Drain
(E) REVC Drain

**51**

As organizações estabelecem e implementam um Sistema de Gestão de Segurança da Informação (SGSI) com base em suas necessidades e em seus objetivos, em seus requisitos de segurança, em seus processos organizacionais, em seu tamanho e em sua estrutura.

A NBR ISO 27001:2013 define vários itens que fazem parte da avaliação de desempenho do SGSI, dentre os quais

(A) a auditoria interna
(B) a avaliação de riscos de segurança da informação
(C) as ações para contemplar riscos e oportunidades
(D) o planejamento operacional e o controle
(E) o tratamento de riscos de segurança da informação

**52**

Como parte do gerenciamento de usuários, na NBR ISO 27002:2013, é recomendado o estabelecimento de controles para assegurar acesso de usuário autorizado e para prevenir acesso não autorizado a sistemas e serviços.

Dentre esses controles, está o gerenciamento de

(A) mudança e capacidade
(B) direitos de acesso privilegiado
(C) cópias de segurança das informações
(D) mudanças em pacotes de software
(E) mudanças para serviços com fornecedores

**53**
Na NBR ISO 27002:2013, são listados controles e objetivos de controles que devem ser aplicados de forma alinhada com o tratamento de riscos de segurança da informação. Um desses controles visa assegurar que a segurança da informação está implementada e é operada de acordo com as políticas e com os procedimentos da organização.

O objetivo descrito é o do controle de

(A) análise crítica da segurança da informação
(B) gerenciamento da segurança em redes
(C) gestão de incidentes de segurança da informação e melhorias
(D) segurança da informação na cadeia de suprimento
(E) segurança em processos de desenvolvimento e de suporte

**54**
Na NBR ISO 27005:2019, é estabelecido que a análise de riscos pode ser empreendida com diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização. Há uma metodologia de análise de riscos que utiliza uma escala com atributos que descrevem a magnitude das consequências potenciais (por exemplo, pequena, média e grande) e a probabilidade de essas consequências ocorrerem (por exemplo, alta, média e baixa).

Essa metodologia de análise de riscos é classificada como

(A) combinada
(B) geométrica
(C) ponderada
(D) qualitativa
(E) quantitativa

**55**
A Resolução nº 740/2020, da Anatel, aprovou o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, que tem por objetivo estabelecer condutas e procedimentos para a promoção da segurança nas redes e nos serviços de telecomunicações. Nessa resolução, é apresentada a seguinte definição:

> espaço virtual composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantem a interconexão de dispositivos de TIC e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente.

Na resolução citada, essa é a definição de espaço

(A) inter-rede
(B) intrarrede
(C) extrarrede
(D) cibernético
(E) metaverso

**56**
Na NBR ISO 27002:2013, é recomendada a aplicação de controles para lidar com os recursos humanos que, em geral, são o elo mais fraco da segurança da informação.

Com relação à segurança em recursos humanos, essa norma estabelece controles para serem aplicados

(A) antes da contratação, apenas
(B) durante a contratação, apenas
(C) no encerramento e na mudança da contratação, apenas
(D) durante a contratação e no encerramento e na mudança da contratação, apenas
(E) antes da contratação, durante a contratação e no encerramento e na mudança da contratação

**57**
Na NBR ISO 29100:2020, é fornecida uma estrutura de alto nível para a proteção de dados pessoais no contexto dos sistemas de tecnologia da informação e de comunicações (TIC). Para assegurar a privacidade de dados pessoais, há um processo pelo qual esses dados são irreversivelmente alterados, de forma que um titular de dados pessoais não mais possa ser identificado, direta ou indiretamente, seja por um controlador de dados pessoais ou em colaboração com qualquer outra parte.

Esse processo é definido nessa norma como

(A) cifração
(B) deformação
(C) deterioração
(D) higienização
(E) anonimização

**58**
Na NBR ISO 29134:2020, é recomendada a elaboração de um instrumento para avaliar os potenciais impactos de um processo, de um sistema de informação, de um programa, de um módulo de software, de um dispositivo ou de outra iniciativa que trate dados pessoais na privacidade. Além disso, é recomendada, também, a consulta às partes interessadas, para tomar ações necessárias para tratar os riscos à privacidade. A partir desse instrumento, é possível elaborar um relatório incluindo uma documentação sobre medidas tomadas para o tratamento de riscos.

De acordo com essa norma, esse relatório é o de

(A) DP
(B) PIA
(C) P&D
(D) R&D
(E) SGSI

Continua

**59**

Na NBR ISO 29100:2020, são adotados princípios de privacidade derivados de princípios existentes, desenvolvidos por vários países e organizações internacionais. Dentre esses princípios, há um que implica conceber e implementar procedimentos de tratamento de dados e sistemas de tecnologia da informação e de comunicações (TIC) de forma a assegurar a adoção de um princípio de necessidade de conhecer (need to know).

Esse princípio de privacidade é o de

(A) limitação de coleta
(B) precisão e qualidade
(C) minimização de dados
(D) especificação e legitimidade de objetivo
(E) consentimento e escolha

**60**

O Secure Socket Layer Version 3 (SSLv3) já foi amplamente utilizado como protocolo de comunicação segura, principalmente para assegurar a proteção das comunicações entre clientes e servidores Web. Esse protocolo, disponível em várias bibliotecas criptográficas mais antigas, obteve um registro no Common Vulnerabilities and Exposures (CVE) por causa de uma vulnerabilidade na sua criptografia CBC, na qual o preenchimento de cifra de bloco não é determinístico e não é coberto pelo Message Authentication Code (MAC). Essa vulnerabilidade facilita que invasores intermediários obtenham dados supostamente protegidos por meio de um ataque padding-oracle.

O ataque padding-oracle também é conhecido como

(A) Logjam
(B) Heartbleed
(C) FMS
(D) POODLE
(E) FREAK

**61**

A segurança dos sistemas de controle e automação industrial vem ganhando a atenção da indústria, e várias iniciativas de padronização de um modelo de segurança foram propostas. O NIST SP 800-82 mais recente descreve o processo de aplicação do NIST Risk Management Framework (RMF) para sistemas de Operational Technology (OT). Em uma das etapas desse processo de aplicação, determinam-se os potenciais impactos adversos da perda de confidencialidade, de integridade e de disponibilidade das informações e do sistema.

Essa etapa é a de

(A) avaliar
(B) autorizar
(C) selecionar
(D) categorizar
(E) implementar

**62**

Um processo de autenticação simples é aquele que usa uma senha como informação necessária para verificar uma identidade reivindicada por um usuário do sistema de informação. Para aumentar a segurança do processo de autenticação, o sistema pode exigir a verificação de algo que o usuário possui, como, por exemplo, um certificado digital. Nesse processo de verificação, o usuário envia seu certificado digital para o sistema que, por sua vez, deve verificar se o certificado está válido, ou seja, se está íntegro, se é autêntico, se está no prazo de validade e se não está revogado.

Considerando-se que está tudo em ordem com o certificado digital enviado pelo usuário, o sistema deve verificar se o usuário tem a posse da

(A) chave pública, que é par da chave privada que consta do certificado digital.
(B) chave privada, que é par da chave pública que consta do certificado digital.
(C) assinatura digital, gerada pela chave pública que consta do certificado digital.
(D) assinatura digital, gerada pela chave privada que consta do certificado digital.
(E) assinatura digital, gerada pela chave pública fornecida pelo sistema de informação.

**63**

O padrão IEEE 802.1X possibilita a troca de informação entre o autenticador, que fornece o acesso à rede de dados, e o servidor de autenticação, que valida a credencial de acesso de um suplicante.

Um protocolo amplamente utilizado para troca de informação entre o autenticador e o servidor de autenticação é o

(A) RADIUS
(B) HTTPS
(C) WEP
(D) WPA
(E) SSH

**64**

No sistema de arquivos EXT3 do sistema operacional Linux, é possível fazer o controle de acesso aos arquivos e às pastas. Considere que um administrador deseja ajustar as permissões do arquivo teste.txt do seguinte modo: permitir apenas o acesso de leitura e de escrita para o dono do arquivo; permitir apenas o acesso de leitura para o grupo do arquivo; negar o acesso de leitura, escrita e execução para os demais usuários do sistema.

O comando que deve ser executado para realizar essa tarefa é o

(A) chown 640 teste.txt
(B) chown 610 teste.txt
(C) chmod 640 teste.txt
(D) chmod 610 teste.txt
(E) chmod 410 teste.txt

**65**
Sistemas computacionais estão sujeitos a falhas que provocam a sua indisponibilidade. Sistemas tolerantes a falhas adotam técnicas de redundância capazes de minimizar os efeitos colaterais de diferentes tipos de adversidades. Quando se deseja aumentar a disponibilidade do sistema de armazenamento, é comum que se adote a redundância com o uso de cálculo de paridade ou de espelhamento.

Um padrão de armazenamento de dados que adota a redundância com o uso de espelhamento é o RAID

(A) 0
(B) 4
(C) 5
(D) 6
(E) 10

**66**
Os arquivos armazenados no sistema de arquivos EXT3 do sistema operacional Linux podem ter vários atributos diferentes. Dentre eles, estão os atributos de identificação do usuário (UID) dono do arquivo, os de identificação do grupo (GID) ao qual o arquivo pertence e os de permissões de acesso de leitura, de escrita e de execução. Tais atributos possibilitam que o sistema determine o que cada um dos usuários pode fazer com o arquivo. Esses atributos ficam armazenados em uma estrutura de dados associada ao arquivo.

Essa estrutura de dados é o

(A) folder
(B) i-node
(C) attrblock
(D) MFT
(E) FAT

**67**
As pragas maliciosas (malwares) sempre foram ameaças à segurança dos computadores, mas os sistemas de controle e automação industrial passaram também a ser vítimas dos ataques cibernéticos. Dentre essas ameaças, está um worm de computador que foi projetado especificamente para atacar o sistema operacional SCADA, desenvolvido pela Siemens. Esse worm foi supostamente usado para controlar as centrífugas de enriquecimento de urânio iranianas. De acordo com a Cybersecurity & Infrastructure Security Agency (CISA), os métodos conhecidos de propagação desse worm incluíam dispositivos USB infectados, compartilhamentos de rede, arquivos do projeto STEP 7, arquivos de banco de dados WinCC e uma vulnerabilidade do spooler de impressão do sistema operacional Microsoft Windows.

O worm descrito é o

(A) meltdown
(B) spectre
(C) stuxnet
(D) defray
(E) petya

**68**
Quando os usuários viajam, os dados confidenciais da sua organização os acompanham e, por essa razão, devem ser protegidos contra acessos não autorizados. O BitLocker, do sistema operacional Windows, é um recurso projetado para tornar a unidade de disco criptografada irrecuperável, caso não se faça a autenticação necessária. Considere que o administrador do sistema deseja consultar o método de criptografia utilizado em uma unidade de disco criptografada.

Para tal consulta, esse administrador usará o comando

(A) bcdedit /bitlocker
(B) bcdedit /status /bitlocker
(C) manage-bde -status
(D) manage-bitlck -status
(E) manage-bitlck /status

**69**
O Windows Firewall é um firewall do sistema operacional Microsoft Windows e foi desenvolvido para proteger o dispositivo. Essa proteção é baseada em regras de controle de acesso que filtram o tráfego de rede destinado ao dispositivo ou oriundo do dispositivo. Considere que um administrador usará o Powershell para visualizar as informações da profile Public do Windows Firewall, tais como o nome do arquivo de registro e o tamanho máximo desse arquivo.

Para tal fim, esse administrador deve usar o seguinte comando:

(A) Get-NetFirewallProfile -Name Public
(B) Get-NetFirewallProfile -Name Public -LogInfo
(C) Get-NetFirewallProfile -Name Public -LogConfig
(D) Get-NetFirewallLog -Name Public -LogInfo
(E) Get-NetFirewallLog -Name Public -LogConfig

**70**
As ameaças aos sistemas de controle e automação industrial provocaram várias iniciativas de padronização de processos mais seguros para a implantação de infraestruturas de Operational Technology (OT). Um dos documentos publicados pelo International Electrotechnical Commission (IEC) tem uma parte que especifica requisitos de processo para o desenvolvimento seguro de produtos e define um ciclo de vida de desenvolvimento seguro (SDL) com a finalidade de desenvolver e manter produtos seguros.

Este documento é o IEC

(A) 27001
(B) 27002
(C) 27005
(D) 60488
(E) 62443