

ANALISTA DA CMB SEGURANÇA DA INFORMAÇÃO

LEIA ATENTAMENTE AS INSTRUÇÕES ABAIXO.

01 - Você recebeu do fiscal o seguinte material:

a) este caderno, com o enunciado das 30 (trinta) questões objetivas, sem repetição ou falha, com a seguinte distribuição:

Conhecimentos Básicos				Conhecimentos Específicos	
Língua Portuguesa II		Língua Inglesa II			
Questões	Pontuação	Questões	Pontuação	Questões	Pontuação
1 a 5	2 pontos cada	6 a 10	2 pontos cada	11 a 30	4 pontos cada
Total	10 pontos	Total	10 pontos	Total	80 pontos
Total: 100 pontos					

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

02 - Verifique se este material está em ordem e se o seu nome e número de inscrição conferem com os que aparecem no **CARTÃO-RESPOSTA**. Caso contrário, notifique o fato **IMEDIATAMENTE** ao fiscal.

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

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, a **caneta esferográfica transparente de tinta na cor preta**, de forma contínua e densa. A LEITORA ÓTICA é sensível a marcas escuras, portanto, preencha os campos de marcação completamente, sem deixar claros.

Exemplo: (A) ● (C) (D) (E)

05 - Tenha 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 em suas margens superior e/ou inferior - **BARRA DE RECONHECIMENTO PARA LEITURA ÓTICA**.

06 - 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. Você só deve assinalar **UMA RESPOSTA**: a marcação em mais de uma alternativa anula a questão, **MESMO QUE UMA DAS RESPOSTAS ESTEJA CORRETA**.

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

08 - **SERÁ ELIMINADO** do Processo Seletivo Público o candidato que:

a) se utilizar, durante a realização das provas, de máquinas e/ou relógios de calcular, bem como de rádios gravadores, *headphones*, telefones celulares ou fontes de consulta de qualquer espécie;

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

Obs. O candidato só poderá se ausentar do recinto das provas após **1 (uma) hora** contada a partir do efetivo início das mesmas. Por motivos de segurança, o candidato **NÃO PODERÁ LEVAR O CADERNO DE QUESTÕES**, a qualquer momento.

09 - Reserve 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**.

10 - Quando terminar, entregue ao fiscal o **CADERNO DE QUESTÕES**, o **CARTÃO-RESPOSTA** e **ASSINE** a **LISTA DE PRESENÇA**.

11 - **O TEMPO DISPONÍVEL PARA ESTAS PROVAS DE QUESTÕES OBJETIVAS É DE 4 (QUATRO)**, incluído o tempo para a marcação do seu **CARTÃO-RESPOSTA**.

12 - As questões e os gabaritos das Provas Objetivas serão divulgados no primeiro dia útil após a realização das mesmas, no endereço eletrônico da **FUNDAÇÃO CESGRANRIO** (<http://www.cesgranrio.org.br>).



LÍNGUA PORTUGUESA II

INCOERENTE, EU?

Uma reflexão sobre coerência e coesão textuais

Você já escreveu ou falou alguma coisa que foi considerada incoerente por outra pessoa? Não? Então, vamos reformular a pergunta: você já escreveu ou falou alguma coisa que foi entendida de maneira diferente da que você gostaria que entendessem?

E aí? Mudou de opinião?

Pois é, que atire o primeiro dicionário quem nunca foi interpretado de maneira diferente daquilo que quis veicular. Seja por causa da falta de informação ou do seu excesso; seja pelo fato de a mensagem não possuir elementos contextualizadores suficientes, como título, autoria, assinatura (no caso do escrito) ou gestos, olhares, entoação (no caso do falado); ou, ainda, seja porque o conhecimento do conteúdo veiculado não era partilhado suficientemente com o interlocutor (leitor ou ouvinte). Todas essas razões nos fazem pensar que, quando chamamos um texto de incoerente, estamos nos referindo à não ativação de elementos necessários para que tanto o falante/escritor como o ouvinte/leitor atribuam sentido. A escola nos ajudou a pensar assim?

Vários pedagogos e estudiosos da educação têm relatado que o ensino de Língua portuguesa, por muito tempo, se posicionou sobre o assunto de modo bastante negligente, não abordando os motivos empíricos que fazem com que os textos possam ser considerados incoerentes. Quem não se lembra de algum professor que tenha devolvido ao aluno seu texto escrito com uma cruz enorme em vermelho acompanhada da frase “Seu texto está incoerente”? Muitas vezes, nessas situações, o aluno recebe a correção, mas não chega a ele as orientações para entender o que pode melhorar no texto e o que faz dele incoerente. [...]

A coerência de um texto depende majoritariamente da troca de informações entre os interlocutores, muito mais do que a construção sintática que possui, assim como a atribuição de coerência está ligada diretamente aos nossos conhecimentos sobre o assunto. No entanto, o puro conhecimento sociocognitivo não é suficiente se não apreendemos os aspectos estritamente linguísticos. Caso o leitor não compreenda o código ali colocado, a coerência não se constituirá. Isso pode ocorrer quando há alguma expressão no texto de uma língua diferente daquela usada pelo leitor, como o latim (*ad hoc*), o francês (*déjà vu*), ou o inglês (*mainstream*). Ou, ainda, quando o registro é extremamente específico de uma área, como os famosos jargões técnicos: vocabulários jurídico, médico etc.

Além do conhecimento das palavras, a relação sintática também é de suma importância.

O estabelecimento da mútua compreensão sobre a sintaxe entre os interlocutores é chamado de coesão textual. Ela não só está comprometida com a estrutura do texto, isto é, a ligação entre os termos e as frases, como também com a semântica, ou seja, o sentido que advém dessa estrutura e que é atribuído pelos interlocutores.

MELO, Iran Ferreira de. Incoerente, eu? Uma reflexão sobre coerência e coesão textuais. **Revista Conhecimento Prático: Língua portuguesa**. São Paulo: Escala, n. 16, jan. 2009. p. 8-11. Adaptado.

1

De acordo com o texto, para que a coerência textual se estabeleça, é necessário, sobretudo, o(a)

- (A) conhecimento individual
- (B) diálogo entre os interlocutores
- (C) aspecto linguístico
- (D) fator intuitivo
- (E) construção sintática

2

No terceiro parágrafo do texto, por meio da metáfora “que atire o primeiro dicionário quem nunca foi interpretado de maneira diferente daquilo que quis veicular” (l. 7-9), o autor mostra que problemas relativos à coerência são comuns nas atividades comunicativas.

Para fundamentar sua tese, ele apresenta três razões, que são, respectivamente,

- (A) informações obscuras; excesso de elementos contextualizadores; conhecimento prévio
- (B) falta ou excesso de informações; desconhecimento da mensagem; conhecimento individual
- (C) quantidade desequilibrada de informações; falta de dados do contexto; conhecimento não compartilhado
- (D) não compartilhamento de informações; mensagem sem contexto; conhecimento excessivo
- (E) pouca clareza das informações; contexto esvaziado; conhecimentos desnecessários

3

Observa-se o uso adequado do acento grave no trecho “estamos nos referindo à não ativação de elementos” (l. 18-19).

Verifica-se um **DESRESPEITO** à norma-padrão quanto ao emprego desse acento em:

- (A) O professor se reportou àquele texto de Machado de Assis.
- (B) Sonhamos em viajar à terra de Gonçalves Dias.
- (C) Ele sempre fazia alusão à palavras de seu poeta favorito.
- (D) Os alunos compreenderam o poema à custa de muito empenho.
- (E) Prefiro as poesias de Drummond às de Olavo Bilac.



4

O elemento coesivo **Isso** (l. 44) tem como referente a ideia de que

- (A) a coerência independe da compreensão de certos aspectos linguísticos.
- (B) o conhecimento sobre o assunto é fundamental à construção da coerência.
- (C) o puro conhecimento sociocognitivo constitui os sentidos do texto.
- (D) os sentidos de um texto são construídos por um processo de troca.
- (E) os sentidos não se constroem caso não se compreenda o código linguístico.

5

No que se refere ao fenômeno da concordância nominal, no subtítulo do texto, o termo **textuais** também admite a forma singular.

O período em que, conforme a norma-padrão, o termo destacado pode assumir tanto a forma singular quanto a plural é:

- (A) **Bastantes** poemas foram lidos na aula.
- (B) Custam **caro** os jornais de domingo.
- (C) Vendem-se quadros e esculturas **usados**.
- (D) Compramos livro e jornal **velhos**.
- (E) Na estante, dicionário e livros **jogados**.

LÍNGUA INGLESA II

United States Mint Announces 2012 Presidential \$1 Coin Designs

WASHINGTON, January 5, 2012
(Press Release by the US Mint)

The United States Mint, created by Congress in 1792, is the Nation's unique manufacturer of dollars (bills and coins), so that the country can conduct its trade and commerce. In addition to producing currency, the United States Mint also produces uncirculated and commemorative coins; Congressional Gold Medals; and silver, gold and platinum coins.

Today the United States Mint announced the new designs that will appear on the Presidential \$1 Coins in 2012. Each coin has two sides: the heads and the tails. The obverse (heads sides) of the coins will bear portraits of former Presidents Chester Arthur, Grover Cleveland (first term), Benjamin Harrison and Grover Cleveland (second term).

Inscriptions on the obverse of each coin include the President's name, the years of his term in office, a number indicating the order in which he served, and the inscription *IN GOD WE TRUST*. The portraits of Chester Arthur and Grover Cleveland were designed and sculpted by United States Mint Sculptor-Engraver Don Everhart. The portrait of Benjamin Harrison was designed and sculpted by United States Mint Sculptor-Engraver Phebe Hemphill.

All coins in the Presidential \$1 Coin Program bear a common reverse (tails side) featuring the iconic Statue of Liberty, designed and sculpted by Everhart. Inscriptions on the reverse are \$1 and *UNITED STATES OF AMERICA*. The year of minting, or issuance, *E PLURIBUS UNUM* and the mint mark are incused on the edge of the coins.

The Presidential \$1 Coin Program is authorized by Public Law 109-145. Although production of circulating Presidential \$1 Coins will soon be suspended, collectible versions of the coin will continue to be available in select United States Mint offerings. For information on the availability and pricing of products featuring Presidential \$1 Coins, visit <http://www.usmint.gov/catalog> or call 1-800-USA-MINT (872-6468).

Available at: http://www.usmint.gov/pressroom/?action=press_release&id=1319. Retrieved on: Jan. 10, 2012. Adapted.

6

According to the text, the United States Mint is

- (A) an unofficial governmental organization.
- (B) an official governmental organization.
- (C) a private organization that establishes commerce and trade.
- (D) a governmental bank that operates for the Congress.
- (E) a department of the US Congress.



7

In the text, the word in parentheses that describes the idea expressed by the words in bold-face type is in:

- (A) “the Nation’s **unique** manufacturer” – line 2 (first)
- (B) “the country can conduct its **trade** and commerce.” – lines 3-4 (transportation)
- (C) “**In addition to** producing currency” – line 4 (Besides)
- (D) “producing **currency**, the United States Mint” – lines 4-5 (chain)
- (E) “commemorative **coins**; Congressional Gold Medals.” – line 6 (bills)

8

In 2012, the heads of the \$1 coins will carry illustrations of

- (A) former presidents’ portraits
- (B) former presidents standing up
- (C) a former president sitting down
- (D) the current president’s face
- (E) the current president standing up

9

According to the text, the obverse of each coin includes all the following pieces of information, **EXCEPT**

- (A) a former president’s portrait
- (B) a numeral with the president’s term order
- (C) an inscription
- (D) an engraving with Don Everhart’s face
- (E) the year the president served his term

10

An equivalent way of saying “The portrait of Benjamin Harrison was designed and sculpted by United States Mint Sculptor-Engraver Phebe Hemphill.” (lines 21-23) is in:

- (A) Benjamin Harrison designed and sculpted the portrait of Phebe Hemphill in the United States.
- (B) Authored by United States Mint Sculptor-Engraver Benjamin Harrison, the portrait of Phebe Hemphill was designed and sculpted.
- (C) Phebe Hemphill’s portrait of Benjamin Harrison was designed and sculpted by a United States Mint Sculptor-Engraver.
- (D) United States Mint Sculptor-Engraver Phebe Hemphill designed and sculpted the portrait of Benjamin Harrison.
- (E) United States Mint Sculptor-Engraver Phebe Hemphill had her portrait designed and sculpted by Benjamin Harrison.

CONHECIMENTOS ESPECÍFICOS

11

O processo de gerenciamento de risco se resume em identificar os riscos, avaliar a probabilidade dos riscos acontecerem e determinar os controles para

- (A) eliminar todos os riscos identificados e prover 100% de segurança.
- (B) eliminar alguns riscos identificados e prover entre 60% e 80% de segurança.
- (C) eliminar alguns riscos identificados e prover, no máximo, 50% de segurança.
- (D) reduzir os riscos identificados a um nível aceitável.
- (E) impedir todo e qualquer acesso ao ativo.

12

A atividade de segurança da informação visa a proteger os valiosos recursos de informação de uma empresa através da seleção e aplicação de salvaguardas apropriadas, ajudando a atingir o objetivo do negócio ou sua missão.

Nesse sentido, um programa de proteção da informação efetivo deve

- (A) ser restrito à área de tecnologia da informação (TI) da empresa.
- (B) ser restrito à área de protocolo de documentos da empresa.
- (C) englobar parte da área de TI e parte da área de protocolo de documentos da empresa.
- (D) englobar toda a área de TI e toda a área de protocolo de documentos da empresa.
- (E) ir além da área de TI e da área de protocolo de documentos da empresa.

13

Os worms (vermes) são códigos maliciosos que utilizam a rede como principal meio para replicação.

O tipo de worm que se mantém como uma cópia única de si mesmo em qualquer ponto no tempo enquanto se transfere para hosts vizinhos na rede é conhecido como

- (A) Downloader
- (B) Rabbit
- (C) Trojan Horse
- (D) Octopus
- (E) Logic bomb

14

Uma forma de monitorar os programas que são executados em uma estação de trabalho, com respeito à alocação não autorizada das portas de rede, é configurar adequadamente um guardião idealizado para essa tarefa conhecido como

- (A) antivírus
- (B) firewall pessoal
- (C) IDS de host
- (D) gerenciador de tarefas
- (E) escalonador de processos

**15**

O processo de autenticação de usuários é um método eficaz para proteger o acesso indevido de pessoas a computadores, sistemas operacionais, softwares, redes e ambientes físicos. Um sistema que utiliza um processo de forte autenticação deve verificar algo que o usuário sabe, algo que ele possui e algo que ele é.

Para acessar o sistema, nessa ordem de verificação, um usuário legítimo deve fornecer os seguintes itens pessoais:

- (A) senha pessoal, token com a chave pública e digital
- (B) senha pessoal, token com o certificado digital e digital
- (C) senha pessoal, token com a chave privada e digital
- (D) chave privada, token com a senha pessoal e certificado digital
- (E) chave pública, token com a senha pessoal e certificado digital

16

A técnica de defesa em profundidade é baseada em camadas de segurança. Um dos principais fatores dessa técnica é o perímetro de segurança que forma a borda fortificada de uma rede.

O componente do perímetro que utiliza métodos de detecção por anomalia e por assinatura para identificar tráfego malicioso na rede é o

- (A) IDS
- (B) Firewall com estado
- (C) Firewall sem estado
- (D) Firewall proxy
- (E) DMZ

17

A Autoridade Certificadora (AC) é a entidade da Infraestrutura de Chaves Públicas (ICP), que é responsável por emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular.

Esses certificados digitais são considerados à prova de falsificação, pois são

- (A) assinados digitalmente e unicamente pela AC
- (B) assinados digitalmente em conjunto pela AC e pelo titular
- (C) criptografados unicamente pela AC
- (D) criptografados em conjunto pela AC e pelo titular
- (E) criptografados e assinados digitalmente em conjunto pela AC e pelo titular

18

Um ataque é uma tentativa deliberada de burlar serviços de segurança para violar a política de segurança de um sistema.

Um tipo de ataque passivo é a

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

19

A transferência de informações através de redes públicas de comunicação de dados é uma atividade comum nas empresas. Para garantir segurança nessa atividade, pode-se fazer uso de VPN (Virtual Private Network).

O protocolo de VPN que usa o IKE (Internet Key Exchange), o ESP (Encapsulating Security Payload) e o AH (Authentication Header) é o

- (A) SSH
- (B) SSL
- (C) L2TP
- (D) PPTP
- (E) IPsec

20

O controle de acesso a redes de comunicação de dados é fundamental para a segurança da informação.

Para fazer o controle baseado em porta, o IEEE (Institute of Electrical and Electronics Engineers) desenvolveu o padrão 802.1x para prover o transporte de informações de

- (A) autenticação entre um Suplicante, conectado à porta de comunicação de um Servidor de Autenticação, e um Sistema Autenticador, possibilitando, assim, controlar o estado da porta de comunicação em função do resultado do processo de autenticação.
- (B) autenticação entre um Suplicante, conectado à porta de comunicação de um Sistema Autenticador, e um Servidor de Autenticação, possibilitando, assim, controlar o estado da porta de comunicação em função do resultado do processo de autenticação.
- (C) estado entre um Suplicante, conectado à porta de comunicação de um Servidor de Autenticação, e um Sistema Autenticador, possibilitando, assim, controlar a autenticação da porta de comunicação em função do resultado do processo de autenticação.
- (D) estado entre um Suplicante, conectado à porta de comunicação de um Sistema Autenticador, e um Servidor de Autenticação, possibilitando, assim, controlar a autenticação da porta de comunicação em função do resultado do processo de autenticação.
- (E) controle entre um Suplicante, conectado à porta de comunicação de um Servidor de Autenticação, e um Sistema Autenticador, possibilitando, assim, controlar o estado da porta de comunicação em função do resultado do processo de autenticação.

21

A forma de ataque na qual o atacante pode interceptar e modificar seletivamente dados comunicados para se passar por uma ou mais das entidades envolvidas em uma comunicação é conhecido como ataque do

- (A) Smurf
- (B) Fraggle
- (C) Teardrop
- (D) Man-in-the-Middle
- (E) Middleware

**22**

É muito mais fácil interromper a operação de uma rede ou sistema do que efetivamente ganhar acesso a eles. Por essa razão, as técnicas de ataque baseadas em negação de serviço (DoS – Denial of Service) são frequentemente utilizadas. Um atacante pode amplificar seu ataque DoS engajando múltiplos nós de rede para inundar a conexão de rede da vítima.

Esse ataque visa à(ao)

- (A) evasão de IDS
- (B) evasão de firewall
- (C) inanição de recursos
- (D) esgotamento de IP
- (E) consumo de largura de banda

23

Nas redes locais sem fio, a difusão do sinal no meio físico possibilita que qualquer indivíduo que possua um receptor de rádio intercepte comunicações nessas redes.

Para controlar o acesso e garantir o sigilo das informações nas redes Wi-Fi, vários esquemas de segurança foram criados, dentre os quais se incluem os seguintes:

- (A) WTC, WPA e WPA2
- (B) WTC, WSA e WPA2
- (C) WEP, WPA e WSA2
- (D) WEP, WPA e WPA2
- (E) WCP, WPA e WPA2

24

Na criptografia simétrica, um algoritmo utiliza uma chave para converter dados legíveis em dados sem sentido que permitem que um algoritmo (tipicamente o mesmo) utilize a mesma chave para recuperar os dados originais.

Por questão de segurança, quando é necessário reutilizar as chaves simétricas em diferentes operações, deve-se usar a cifração

- (A) de bloco
- (B) de fluxo
- (C) de enchimento
- (D) híbrida
- (E) invertida

25

O uso de criptografia simétrica no compartilhamento de informações secretas requer o compartilhamento de chave simétrica.

Uma forma segura para um emissor enviar uma chave simétrica por meios de comunicação inseguros para um receptor é criptografar essa chave com a chave

- (A) privada do emissor
- (B) privada do receptor
- (C) pública do emissor
- (D) pública do receptor
- (E) pública do emissor e a chave privada do receptor

26

A criptografia assimétrica pode ser utilizada para possibilitar a verificação da integridade e da autenticidade de uma mensagem.

Para isso, o emissor deve produzir a assinatura digital da mensagem, que é formada pela criptografia do(a)

- (A) código de hash da mensagem com a chave privada do emissor
- (B) código de hash da mensagem com a chave pública do emissor
- (C) código de hash da mensagem com a chave pública do receptor
- (D) chave pública do emissor com o código de hash da mensagem
- (E) chave privada do emissor com o código de hash da mensagem

27

O Hash Message Authentication Code (HMAC) pode ser utilizado para autenticar mensagens.

Esse esquema de autenticação combina o algoritmo de resumo de mensagem com a(o)

- (A) chave pública
- (B) chave privada
- (C) chave secreta
- (D) assinatura digital
- (E) certificado digital

28

Muitas funções críticas para o negócio de uma empresa são dependentes da disponibilidade dos ativos de informação. Diante da interrupção das operações normais de negócio, a equipe de segurança da informação da empresa deve executar um conjunto de atividades para manter ou recuperar as operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida.

De acordo com a ISO 27002, essas atividades devem fazer parte do

- (A) Guia de Atividades Emergenciais
- (B) Guia de Atividades para Recuperação
- (C) Plano de Continuidade do Negócio
- (D) Padrão de Restauração do Negócio
- (E) Padrão de Recuperação de Desastres

29

Para viabilizar uma comunicação segura no ambiente da Internet, vários protocolos de segurança podem ser adotados.

No caso do serviço Web, para garantir a segurança na comunicação, deve-se adotar o protocolo

- (A) HTML over SSL
- (B) HTML Secure
- (C) HTTP over SSL
- (D) HTTP Secure
- (E) XML Secure



30

O resumo de mensagem é produzido, de forma geral, por algoritmos que recebem qualquer comprimento de informação de entrada para produzir uma saída pseudoaleatória de largura fixa chamada digest.

Uma de suas principais propriedades, chamada efeito avalanche, visa a garantir que

- (A) pequenas variações na informação de entrada produzam digests iguais.
- (B) pequenas variações na informação de entrada produzam digests diferentes.
- (C) grandes variações na informação de entrada produzam digests iguais.
- (D) grandes variações na informação de entrada produzam digests mais seguros.
- (E) pequenas e grandes variações na informação de entrada produzam digests iguais.

RASCUNHO

RASCUNHO