AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Tecnologista
Classe Pleno I
Padrão I
Código 15

Provas objetivas e discursiva

Aplicação: 19/9/2004

CESPE
UNIVERSIDADE DE BRASÍLIA
Criando Oportunidades para Realizar Sonhos

LEIA COM ATENÇÃO AS INSTRUÇÕES ABAIXO.

1 Ao receber este caderno, confira se ele contém **cento e vinte** itens, correspondentes às provas objetivas, corretamente ordenados de **1** a **120**, e a prova discursiva, acompanhada de uma página para rascunho.

2 A página para rascunho é de uso opcional; não contará, portanto, para efeito de avaliação.

3 Caso o caderno esteja incompleto ou tenha qualquer defeito, solicite ao fiscal de sala mais próximo que tome as providências cabíveis.

4 Nos itens das provas objetivas, recomenda-se não marcar ao acaso: a cada item cuja resposta divirja do gabarito oficial definitivo, além de não marcar ponto, o candidato recebe pontuação negativa, conforme consta em edital.

5 Não utilize nenhum material de consulta que não seja fornecido pelo CESPE.

6 Não serão distribuídas folhas suplementares para rascunho nem para texto definitivo.

7 Durante as provas, não se comunique com outros candidatos nem se levante sem autorização do chefe de sala.

8 A duração das provas é de **quatro horas e trinta minutos**, já incluído o tempo destinado à identificação — que será feita no decorrer das provas —, ao preenchimento da folha de respostas e à transcrição do texto definitivo para a folha de texto definitivo.

9 Na prova discursiva, não será avaliado texto escrito a lápis, em local indevido ou que tenha identificação fora do local apropriado.

10 Ao terminar as provas, chame o fiscal de sala mais próximo, devolva-lhe as suas folhas de respostas e de texto definitivo e deixe o local de provas.

11 A desobediência a qualquer uma das determinações constantes no presente caderno, na folha de rascunho, na folha de respostas ou na folha de texto definitivo poderá implicar a anulação das suas provas.

AGENDA

I **20/9/2004**, a partir das 10 h (horário de Brasília) – Gabaritos oficiais preliminares (provas objetivas): Internet — www.cespe.unb.br.

II **21** e **22/9/2004**, das 9 às 16 h (horário local) – Recursos (provas objetivas): exclusivamente nos locais que serão informados na divulgação dos referidos gabaritos.

III **13/10/2004** – Resultado final das provas objetivas e resultado provisório da prova discursiva: Diário Oficial da União e Internet — www.cespe.unb.br.

IV **14** e **15/10/2004** – Recursos (prova discursiva): em locais e horários que serão informados na divulgação do resultado provisório.

V **29/10/2004** – Resultado final da prova discursiva e convocação para a entrega da documentação da avaliação de títulos: locais mencionados no item III.

OBSERVAÇÕES

- Não serão objeto de conhecimento recursos em desacordo com o item 11 do Edital n.º 1/2004 – ABIN, de 19/7/2004.
- Informações adicionais: telefone 0(XX)61 448 0100 e Internet: www.cespe.unb.br.
-

• De acordo com o comando a que cada um dos itens de **1** a **120** se refira, marque, na **folha de respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a folha de rascunho e, posteriormente, a **folha de respostas**, que é o único documento válido para a correção das suas provas.

• Nos itens que avaliam **Conhecimentos de Informática**, a menos que seja explicitamente informado o contrário, considere que todos os programas mencionados estão em configuração-padrão, em português, que o *mouse* está configurado para pessoas destras e que expressões como clicar, clique simples e clique duplo referem-se a cliques com o botão esquerdo do *mouse*. Considere também que não há restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios e equipamentos mencionados.

CONHECIMENTOS BÁSICOS

A criação do Sistema Brasileiro de Inteligência (SISBIN) e a consolidação da Agência Brasileira de Inteligência (ABIN) permitem ao Estado brasileiro institucionalizar a atividade de Inteligência, mediante uma ação coordenadora do fluxo de informações necessárias às decisões de governo, no que diz respeito ao aproveitamento de oportunidades, aos antagonismos e às ameaças, reais ou potenciais, relativos aos mais altos interesses da sociedade e do país. Todo o trabalho de reformulação da atividade vem sendo balizado, também, por enfoques doutrinários condizentes com o processo atual de globalização, em que as barreiras fronteiriças são fluidas, sugerindo cautelas para garantir a preservação dos interesses da sociedade e do Estado brasileiros, de forma a salvaguardar a soberania, a integridade e a harmonia social do país.

Internet: <http://www.abin.gov.br/abin/historico.jsp> (com adaptações).

Considerando o texto acima, julgue os itens subseqüentes.

1 Como o sujeito do primeiro período sintático é formado por duas nominalizações articuladas entre si pelo sentido — "criação" (ℓ.1) e "consolidação" (ℓ.2) —, estaria também gramaticalmente correta a concordância com o verbo **permitir** (ℓ.3) no singular — **permite**.

2 O primeiro período sintático permaneceria gramaticalmente correto e as informações originais estariam preservadas com a substituição da palavra "mediante" (ℓ.4) por qualquer uma das seguintes expressões: por meio de, por intermédio de, com, desencadeando, realizando, desenvolvendo, empreendendo, executando.

3 Em "às ameaças" (ℓ.8), o sinal indicativo de crase justifica-se pela regência da palavra "antagonismos" (ℓ.7).

4 As vírgulas que isolam a expressão "reais ou potenciais" (ℓ.8) são obrigatórias, uma vez que se trata de um aposto explicativo.

5 Depreende-se dos sentidos do texto que, imediatamente após a palavra "atividade" (ℓ.10), há elipse do qualificativo da ação, que seria adequadamente explicitado por meio da inserção da palavra **diplomática**.

6 O emprego da estrutura "vem sendo balizado" (ℓ.10), em que não há agente explícito, constitui um recurso de impessoalização do texto adequado à redação de documentos e correspondências oficiais.

7 Na palavra "fluidas" (ℓ.13), dispensa-se o acento gráfico porque se trata de particípio passado flexionado do verbo **fluir** e a pronúncia da primeira sílaba considera "ui" um hiato.

O Ministério da Defesa vai receber R$ 1 bilhão de aumento no orçamento de 2005 para investir prioritariamente no programa de blindagem da Amazônia e no reequipamento geral. As Forças Armadas do Brasil estão intensificando a proteção do território e do espaço aéreo do Norte, Nordeste e Oeste por meio da instalação de novas bases, transferência para a região de tropas do Sul-Sudeste e expansão da flotilha fluvial da Marinha.

O contingente atual, de 27 mil homens, chegará a 30 mil militares entre 2005 e 2006. As dotações de investimentos na área militar devem superar os R$ 7,3 bilhões no próximo ano. O dinheiro será destinado a atender às necessidades do programa de segurança da Amazônia e para dar início ao processo de reequipamento das forças. A estimativa é de que até 2010 sejam aplicados de US$ 7,2 bilhões a US$ 10,2 bilhões na área de defesa.

Em 2005, uma brigada completa, atualmente instalada em Niterói — com aproximadamente 4 mil soldados —, será deslocada para a linha de divisa com a Colômbia.

Roberto Godoy. **Forças armadas terão mais R$ 1 bi para reequipamento**. *In*: **O Estado de S. Paulo**, 8/8/2004, p. A12 (com adaptações).

Com referência ao texto acima e considerando os diversos aspectos do tema por ele abordado, julgue os itens seguintes.

8 Embora partilhada com um número reduzido de países, a fronteira amazônica é considerada estratégica, porque corresponde à área de maior intercâmbio comercial do Brasil com seus vizinhos da América do Sul.

9 A palavra "blindagem" (ℓ.3) está sendo utilizada em seu sentido denotativo ou literal, uma vez que o período está tratando de equipamentos de segurança.

10 A decisão de promover uma espécie de "blindagem da Amazônia" (ℓ.3) decorre da constatação de que a região é suscetível a graves problemas, a exemplo da ação de guerrilheiros e de narcotraficantes.

11 Pelos sentidos do texto, infere-se que, na expressão "flotilha fluvial" (ℓ.7), o termo sublinhado indica a idéia de esquadra constituída de embarcações com características idênticas ou semelhantes: grande porte, elevado nível tecnológico e finalidade bélica.

12 Para a segurança nacional, a relevância estratégica de um sistema integrado de vigilância cobrindo a Amazônia, como é o caso do SIVAM, justifica a forma pela qual se deu sua licitação, restrita a empresas nacionais e sem suscitar controvérsias no âmbito do governo federal.

13 A rigor, a ênfase dada pelo texto ao montante de recursos com o qual se pretende dotar o Ministério da Defesa não se justifica. Afinal, nos últimos anos, o orçamento da União não tem sido modesto quanto a investimentos, especialmente em relação às Forças Armadas.

14 As regras gramaticais permitem que os travessões que isolam a expressão "com aproximadamente 4 mil soldados" (ℓ.17) sejam substituídos tanto por vírgulas como por parênteses, sem prejuízo para a sintaxe e a correção do período.

15 A substituição de "será deslocada" (ℓ.17-18) por **deslocar-se-á** mantém a correção gramatical do período.

Segurança do medo

A síndrome de Nova Iorque, 11 de setembro, projetou-se sobre Atenas, agosto, sexta-feira, 13, data da abertura dos 28.º Jogos Olímpicos. De tal forma que os gastos de 1,2 bilhão de euros (cerca de R$ 4,8 bilhões) são a maior quantia já investida em segurança na história da competição. O dinheiro foi aplicado em um poderoso esquema para evitar ataques terroristas, como ocorreu nos Jogos de Munique, em 1972, quando palestinos da organização Setembro Negro invadiram a Vila Olímpica e mataram dois atletas israelenses. Do esquema grego, montado em colaboração com sete países — Estados Unidos da América (EUA), Austrália, Alemanha, Inglaterra, Israel, Espanha e Canadá —, faz parte o sistema de navegação por satélite da Agência Espacial Européia. Da terra, ar e água, 70 mil policiais, bombeiros, guarda costeira e mergulhadores da Marinha vão zelar pela segurança. Até a Organização do Tratado do Atlântico Norte (OTAN) emprestará sua experiência militar no combate ao terrorismo.

Correio Braziliense, 7/8/2004, "Guia das Olimpíadas", p. 3 (com adaptações).

A respeito do texto acima e considerando as informações e os múltiplos aspectos do tema que ele focaliza, julgue os itens que se seguem.

16 A edição de 2004 das Olimpíadas, sediadas na Grécia, berço desses jogos, reafirma uma tendência consolidada nas últimas décadas do século XX, qual seja, a crescente interseção entre competições desportivas e interesses econômico-financeiros, realidade também visível nos diversos setores da cultura, como os da música popular e do cinema.

17 A "síndrome de Nova Iorque" (ℓ.1) remete à inusitada ação de 11 de setembro de 2001, quando terroristas árabes destruíram as torres do World Trade Center e parte das instalações do Pentágono, espalhando o pânico entre os norte-americanos e desvelando a vulnerabilidade do mais poderoso país do planeta.

18 Do ponto de vista gramatical, para o trecho "A síndrome (...) 28.º Jogos Olímpicos" (ℓ.1-3), estaria igualmente correta a seguinte reescritura: A síndrome do ocorrido em 11 de setembro em Nova Iorque projetou-se sobre a sexta-feira, 13 de agosto, data da abertura, em Atenas, dos 28.º Jogos Olímpicos.

19 A partir de suas bases situadas no Iraque e do comando remoto de Saddam Hussein, a organização terrorista Al Qaeda assumiu a responsabilidade pelos atentados contra os EUA, o que foi determinante para a decisão de George W. Bush de invadir aquele país.

20 No trecho "cerca de R$ 4,8 bilhões" (ℓ.4), mantém-se a correção gramatical ao se substituir o termo sublinhado por qualquer uma das seguintes expressões: aproximadamente, por volta de, em torno de, acerca de.

21 A inserção de **o que** imediatamente antes de "ocorreu" (ℓ.7) prejudicaria a sintaxe do período e modificaria o sentido da informação original.

22 Para os especialistas, a inexistência na estrutura da administração federal brasileira de um ministério específico para tratar do desporto, tanto o de rendimento quanto o educacional, ajuda a explicar os relativamente modestos resultados obtidos pelo país nos Jogos Olímpicos de Atenas.

23 A presença da preposição em "Do esquema grego" (ℓ.10) é uma exigência sintática justificada pela regência da palavra "sistema" (ℓ.13).

24 O fato de nenhum integrante da União Européia ter colaborado com o país anfitrião das Olimpíadas de 2004 na organização do poderoso e dispendioso esquema de segurança para a competição pode ser interpretado como mais uma expressão de atrito entre o gigantesco bloco europeu e os norte-americanos.

25 A substituição do trecho "Da terra, ar e água" (ℓ.14) por **Da terra, do ar e da água** representaria uma transgressão ao estilo próprio do texto informativo, pois trata-se de um recurso de subjetividade próprio dos textos literários.

26 Citada no texto, a OTAN é uma organização militar criada no ambiente de confronto típico da Guerra Fria. Ainda que não mais existam a União das Repúblicas Socialistas Soviéticas e o cenário de rivalidade entre capitalismo e socialismo, a OTAN permanece de pé, tendo ampliado o número de países que a integram.

O Mercado Comum do Sul (MERCOSUL) ganha uma sede oficial para funcionamento do Tribunal Permanente de Revisão do bloco, que vai funcionar como última instância no julgamento das pendências comerciais entre os países-membros. Melhorar o mecanismo de solução de controvérsias é um dos requisitos para o fortalecimento do MERCOSUL, vide as últimas divergências entre Brasil e Argentina. As decisões do tribunal terão força de lei. Sua sede será Assunção, no Paraguai.

Até agora, quando os países-membros divergiam sobre assuntos comerciais, era acionado o Tribunal Arbitral. Quem estivesse insatisfeito com o resultado do julgamento, no entanto, tinha de apelar a outras instâncias internacionais, como a Organização Mundial do Comércio (OMC).

Gisele Teixeira. **MERCOSUL ganha tribunal permanente**. *In*: **Jornal do Brasil**, ago./2004 (com adaptações).

A propósito do texto acima e considerando a abrangência do tema nele tratado, julgue os itens que se seguem.

27 A existência do MERCOSUL insere-se no quadro mais geral da economia contemporânea, que, crescentemente globalizada e com notável grau de competição entre empresas e países, estimula a formação de blocos econômicos como forma de melhor inserção de seus participantes nesse mercado mundial.

28 A expressão "bloco" (ℓ.3) retoma, sem necessidade de repetição da mesma palavra, a idéia de "MERCOSUL" (ℓ.1).

29 O ponto de partida para a constituição do MERCOSUL foi a aproximação entre Brasil e Argentina, ainda nos anos 80 do século passado. O passo seguinte foi a incorporação do Paraguai e do Uruguai a esse esforço de integração, sendo esses os quatro países integrantes do bloco.

30 Infere-se das informações do texto que um dos pontos frágeis do funcionamento do MERCOSUL está no mecanismo de solução de controvérsias entre os países que o compõem.

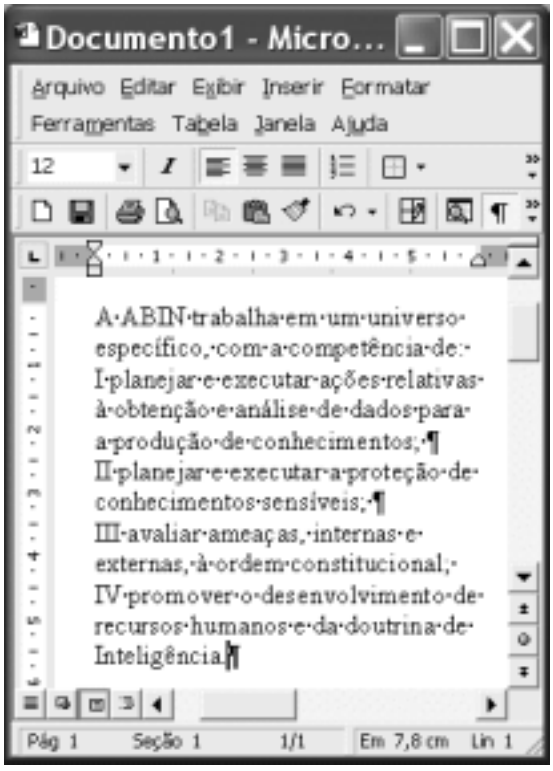
31 Mantém-se a obediência à norma culta escrita ao se substituir a palavra "vide" (ℓ.7) por **haja visto**, uma vez que as relações sintáticas permanecem sem alteração.

32 Ao mencionar as "últimas divergências entre Brasil e Argentina", o texto se reporta à decisão do país platino de impor obstáculos à importação de eletrodomésticos brasileiros, como ocorreu com as geladeiras.

33 Ao escolherem Assunção para sede do Tribunal Permanente de Revisão, é provável que os países integrantes do MERCOSUL tenham considerado o grande potencial paraguaio na produção de manufaturados e sua reconhecida vocação para a formação de juristas.

34 Com a criação do tribunal a que o texto se refere, o MERCOSUL iguala-se à União Européia quanto ao número, à diversidade e à abrangência de instituições criadas para dar suporte ao processo integracionista.

35 Pelo emprego do subjuntivo em "estivesse" (ℓ.12), estaria de acordo com a norma culta escrita a substituição de "tinha de apelar" (ℓ.13) por **teria de apelar**.



A figura acima ilustra uma janela do Word 2000 que contém parte de um texto extraído e adaptado do sítio http://www.abin.gov.br. Considerando essa figura, julgue os itens subseqüentes, acerca do Word 2000.

36 Considere o seguinte procedimento: clicar imediatamente antes de "I planejar"; teclar Enter; clicar imediatamente antes de "IV promover"; teclar Enter; selecionar o trecho iniciado em "I planejar" e terminado em "Inteligência"; clicar . Após esse procedimento, a numeração em algarismos romanos será removida do texto mostrado.

37 Sabendo que o ponto de inserção se encontra posicionado no final do texto mostrado, considere as seguintes ações, executadas com o *mouse*: posicionar o ponteiro no ponto de inserção; pressionar e manter pressionado o botão esquerdo; arrastar o cursor até imediatamente antes de "IV promover"; liberar o referido botão. Após essas ações, o trecho "IV promover (...) Inteligência." será selecionado e o botão ficará ativo, mudando para a forma .

38 Considere o seguinte procedimento: clicar sobre o segundo parágrafo mostrado do documento; clicar . Após esse procedimento, o referido parágrafo terá o estilo de fonte alterado para itálico e os botões de alinhamento de parágrafo ficarão na forma .

39 No *menu* Ferramentas, encontra-se uma opção que permite proteger o documento em edição de tal forma que ele não possa ser impresso em papel por meio de impressora nem copiado, em parte ou totalmente, para a área de transferência do Windows.

40 Considere que o botão seja clicado. Após essa ação, um novo documento, em branco, será aberto. Caso, a seguir, se clique o *menu* Janela, será disponibilizada uma lista que contém o nome de pelo menos dois arquivos abertos na atual sessão de uso do Word. Nessa lista, é possível alternar entre esses arquivos para ativar o que se deseja editar.

Um usuário do Internet Explorer 6 (IE6), a partir de um computador PC e em uma sessão de uso desse aplicativo, acessou a janela Opções da Internet ilustrada na figura acima. Com relação às funcionalidades do IE6 acessíveis por meio dessa janela, julgue os itens de **41** a **44**, considerando que o computador do usuário pertence a uma *intranet* e tendo por referência as informações apresentadas na janela ilustrada.

41 Ao se clicar o botão [Sites...], será obtida uma lista contendo o endereço eletrônico de todas as máquinas pertencentes à *intranet* a que o computador pertence. A partir dessa lista e dos recursos disponibilizados após se clicar o referido botão, o usuário poderá configurar o IE6 de forma a impedir que informações sejam trocadas entre o seu computador e outras máquinas pertencentes à *intranet*. O usuário poderá, dessa forma, descartar automaticamente mensagens de *e-mail* enviadas por usuários a partir de computadores da *intranet*, impedir o acesso a arquivos que estejam armazenados em seu computador a outros usuários e impedir o *download* de componentes de páginas *web* que estejam armazenadas em computadores da *intranet*.

42 Ao se clicar o botão [Nível personalizado...], o usuário poderá definir um nível de segurança desejado, para a zona identificada por 
Intranet local, diferente do estabelecido como padrão pelo IE6. A qualquer momento, o usuário poderá retornar ao nível pré-definido pelo IE6 para essa zona ao clicar o botão [Nível padrão], caso este botão esteja ativado.

43 Por meio da guia [Privacidade], o usuário poderá utilizar recursos do IE6 que mascaram o número IP do seu computador, evitando que este seja identificado na Internet por outros usuários. Esse recurso aumenta a privacidade na Internet e, conseqüentemente, diminui a possibilidade de invasão por parte de *hackers*. Para que esse recurso possa funcionar corretamente, é necessário que o computador tenha instalado *software* de filtragem de *spam*.

44 Por meio de funcionalidades acessíveis a partir da guia [Geral], o usuário poderá eliminar *cookies* que porventura estejam armazenados em seu computador, na pasta Internet Temporary Files.

Pedro é o administrador da LAN (*local area network*) implantada na gerência de informações de seu órgão. Essa rede é composta de diversos servidores que utilizam os sistemas operacionais Linux e Windows 2000, sob os quais encontram-se os computadores dos funcionários dessa gerência e outros componentes da rede. O controle e a identificação de intrusão na rede que administra é preocupação constante para Pedro, que, para minimizar as possibilidades de ataques, já providenciou a implantação de um sistema fundamentado em *firewalls* e em roteadores devidamente configurados, de forma a definir o perímetro de sua rede.

Em face da situação hipotética apresentada acima, considerando que os componentes do sistema de segurança descrito operem em condições típicas, julgue o item abaixo.

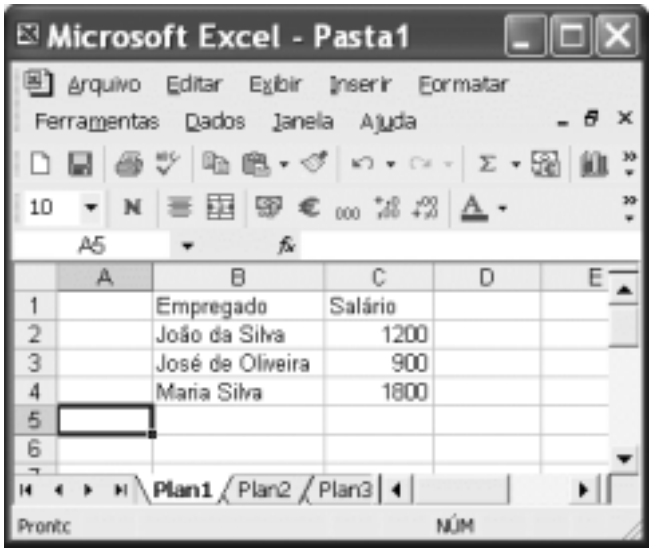
45 A LAN administrada por Pedro está protegida com relação à intrusão por parte de *hackers*, principalmente se a intrusão, para que possa ocorrer, necessitar, em uma etapa prévia, da instalação de informação não-autorizada em algum servidor da rede. Essa proteção deve-se à capacidade de um *firewall* de identificar o conteúdo dos dados que por ele são filtrados e, a partir de uma biblioteca de assinaturas de ataques, de determinar se uma informação é proveniente de uma tentativa de ataque.

Considere que o Windows XP esteja sendo executado em determinado computador. Ao se clicar o botão Iniciar desse *software*, será exibido um *menu* com uma lista de opções. Com relação a esse *menu* e às opções por ele disponibilizadas, julgue os itens seguintes.

46 Ao se clicar a opção Pesquisar, será exibida uma janela com funcionalidades que permitem a localização de um arquivo com determinado nome.

47 Ao se clicar a opção Meus documentos, será exibida uma lista contendo os nomes dos últimos arquivos abertos no Windows XP, desde que esses arquivos estejam armazenados no computador, independentemente do local.

48 Ao se clicar a opção Minhas músicas, será aberto o Windows Media Player, que permitirá executar músicas armazenadas no disco rígido do computador.



A figura acima mostra uma janela do Excel 2002, com uma planilha em processo de edição, contendo uma lista com os salários de três empregados de uma empresa. Com base nessa figura e nos recursos do Excel 2002, julgue os itens a seguir.

49 Para se calcular a soma dos salários dos três empregados da empresa e pôr o resultado na célula C5, é suficiente realizar a seguinte seqüência de ações com o *mouse*: posicionar o ponteiro no centro da célula C2; pressionar e manter pressionado o botão esquerdo; posicionar o ponteiro sobre o centro da célula C4; liberar o botão esquerdo; clicar Σ.

50 Caso se clique o cabeçalho da linha 1 — 1 — e, em seguida, o botão **N**, será aplicado negrito aos conteúdos das células B1 e C1.

CONHECIMENTOS ESPECÍFICOS

As técnicas criptográficas oferecem importantes ferramentas para obtenção de proteção contra diversas ameaças em um ambiente de segurança de sistemas de informações. No referente a sistemas criptográficos, julgue os itens a seguir.

51 Os denominados sistemas simétricos são mais adequados para processamento *online* ou de grandes quantidades de dados, enquanto os sistemas assimétricos são mais adequados em protocolos usados no estabelecimento seguro de chaves em sistemas simétricos.

52 Funções de *hashing* são elementos importantes em diversas aplicações criptográficas. Em particular, funções de *hashing* são utilizadas em procedimentos de geração de assinaturas digitais para impedir que um oponente possa tomar conhecimento do documento assinado, já que essas funções devem ter a propriedade de serem não-inversíveis.

53 Um único sistema criptográfico, denominado sistema de chave única, é considerado matematicamente inquebrável. Esse sistema tem o inconveniente de ter de dispor de uma chave secreta distinta, imprevisível e de, pelo menos, mesmo tamanho que a mensagem, para cada mensagem a ser cifrada. Todos os demais sistemas são, em princípio, quebráveis.

54 O sistema Kerberos, um sistema de autenticação e distribuição de chaves simétricas em ambiente de rede, é embasado no compartilhamento de uma chave secreta distinta entre um servidor Kerberos e cada usuário. Nesse sistema, o conhecimento da chave secreta é equivalente a uma prova de identidade.

55 A cifração baseada em identidade (CBI) ou IBE (*identity based encryption*) é uma técnica moderna de gerar um par de chaves — públicas ou privadas — a partir de uma cadeia qualquer de caracteres. Por outro lado, a criptografia de chaves públicas tradicional baseia-se em chaves formadas por cadeias binárias difíceis de serem memorizadas por um usuário humano. Dessa forma, a CBI facilita o uso de chaves públicas, permitindo que se envie uma mensagem cifrada para um usuário antes mesmo deste ter seu par de chaves.

56 Diversos modos de operação são definidos para cifradores de bloco. Entre eles, tem-se destacado ultimamente o modo contador, que permite implementações de alta velocidade por meio de paralelização e(ou) pré-processamento, mas que apresenta a desvantagem de ser menos seguro em relação a outros modos, pois o conhecimento do valor inicial do contador simplifica a determinação da chave utilizada.

57 O protocolo conhecido como DH (*key exchange protocol*) utiliza o algoritmo DH (Diffie-Hellman) para o estabelecimento de uma chave secreta entre dois usuários. A segurança desse sistema é fundamentada na intratabilidade do problema de computar um logaritmo discreto. Sua vantagem em relação ao esquema RSA para troca de chaves (RSA *key exchange*) é que o DH não está sujeito ao tipo de ataque conhecido como homem-no-meio (*man-in-the-midle*).

58 Protocolos de conhecimento-zero (*zero-knowledge protocols*) são protocolos criptográficos em que uma parte pode provar a uma segunda parte que detém o conhecimento de um determinado segredo, sem revelar o segredo.

Com relação aos diversos aspectos de segurança de um sistema de informações, julgue os itens de **59** a **68**.

59 Quanto mais facilmente se detectarem ações não-autorizadas, melhor será a segurança em um sistema. Dessa forma, é preferível concentrar a maioria dos serviços em um servidor central único, de modo a ter-se apenas um ponto de controle para monitorar.

60 Um dos problemas em segurança de sistemas é que os sistemas operacionais e outros *softwares* vêm configurados de fábrica para serem amigáveis a um usuário leigo, ou seja, sem conhecimento especializado na área. As boas práticas de segurança requerem que essas configurações sejam totalmente revistas e adequadas à condição de utilização do equipamento de instalação.

61 Segurança requer mecanismos de controle de acesso aos recursos de qualquer sistema. A vantagem do uso de controles de acesso discricionários é que estes são transparentes para o usuário.

62 Confidencialidade é a garantia dada a um objeto de um sistema de apenas poder ser dado a conhecer a uma entidade autorizada. A confidencialidade assegura automaticamente a integridade do objeto.

63 O protocolo IPSec acrescenta mecanismos de segurança ao protocolo de rede IP, permitindo a configuração de VPNs (*virtual private networks*). Por meio do uso de recursos do IPSec, é possível estabelecer controle de acesso, proteção contra análise de tráfego e proteção criptográfica aos dados que estão sendo transmitidos.

64 O primeiro passo para a obtenção de um sistema adequadamente seguro é estabelecer uma política de segurança. Essa é a razão pela qual os especialistas consideram que é melhor ter-se uma política de segurança simples e bem difundida na organização a não ter nenhuma.

65 Uma ameaça é uma violação potencial da segurança. Ameaças acidentais, por causas fortuitas como incêndio, terremoto, falhas de *hardware* etc., podem afetar somente a integridade dos objetos protegidos, sendo, portanto, menos críticas que ameaças intencionais.

66 Um mecanismo de senhas (*passwords*) é uma das barreiras mais simples e largamente utilizada para se evitar acessos não autorizados a um sistema. Nos mecanismos de autenticação por senhas, normalmente é armazenado um *hashing* das senhas, para evitar que elas possam ser obtidas simplesmente pela leitura do arquivo de senhas, e ainda é acrescentado um parâmetro modificador variável, denominado *salt*, que individualiza o *hashing* das senhas, mesmo para senhas idênticas. Esse procedimento de acrescentar o *salt* é essencial, por impedir os denominados ataques de dicionário ao arquivo de senhas.

67 O termo DMZ (*demilitarized zone*) é normalmente empregado para designar uma pequena rede, geralmente contendo um servidor *web*, situada entre a rede interna da organização e a rede pública. O tráfego para essa zona é controlado por meio de *firewalls* de forma a permitir que qualquer usuário externo tenha acesso à DMZ (serviço *web*), mas não à rede interna, e que usuários internos possam ter acesso à Internet.

68 Em segurança de sistemas computacionais, engenharia social é um termo usado para descrever um tipo de intrusão não-técnica, que se baseia fortemente na interação humana, geralmente envolvendo alguma forma de persuadir pessoas a quebrar procedimentos normais de segurança ou revelar segredos, sem que elas tenham consciência disso.

Um protocolo pode ser definido como um conjunto especial de regras utilizadas por duas partes para levarem a bom termo uma comunicação entre si. Existem protocolos definidos para diversos níveis de uma comunicação. Quanto a protocolos e sistemas de comunicação, julgue os itens que se seguem.

69 Com a arquitetura TCP/IP utilizada na Internet, tem-se o serviço de nome de domínio, que associa o endereço IP de um equipamento a um nome simbólico, mais ameno aos usuários. Uma vantagem da utilização do nome de domínio é que pode-se conhecer a localização geográfica (país) do equipamento antecipadamente por meio da terminação do nome. Como exemplo hipotético, um equipamento identificado por www.naoexisto.com.br está no Brasil, enquanto ftp.mycompany.co.uk está no Reino Unido (United Kingdom).

70 Transmissão em banda base é a técnica de transmissão de sinais que ocupa toda a banda disponível em um dado meio físico. Por esse motivo, as redes locais de computadores geralmente utilizam a técnica de banda larga, em que vários canais limitados em banda podem ser utilizados para finalidades diferentes.

71 Em uma rede TCP/IP, um datagrama somente pode ser entregue por um equipamento a outro situado na mesma rede física. Isso ocorre em função de um equipamento apenas responder ao protocolo ARP quando estiver dentro do domínio de *broadcasting* do outro.

72 O protocolo CSMA/CD de acesso ao meio exige que a duração de um quadro seja pelo menos igual ao dobro do tempo de propagação do sinal no meio para que seja possível a deteção de colisões.

73 Nas redes ATM (*asynchronous transfer mode*), a unidade de transmissão no meio físico são pacotes de tamanho fixo de 53 *bytes*, denominados células, o que, aliado a velocidades de transmissão de dados usualmente na faixa de 155 Mbps a 2,4 Gbps, permite a implementação de *switches* muito rápidos. Dessa forma, células que carregam informações de vídeo e voz podem ser facilmente multiplexadas no fluxo de dados com freqüência suficiente para a transmissão em tempo real.

74 Uma aplicação de transferência de arquivos em rede, tal como FTP, requer a utilização de um protocolo de transporte sem perdas, como o TCP, sendo, porém, bastante tolerante a retardos. Por sua vez, uma aplicação de tempo real, tipo multimídia, é pouco tolerante a retardos, mas é tolerante a perdas, o que permite o uso do protocolo de transporte UDP.

Um sistema operacional é o programa que, após ser inicializado em um computador, gerencia todos os outros programas e recursos disponíveis. Eles determinam, efetivamente, a maioria das características perceptíveis por um usuário da máquina. Com relação a sistemas operacionais, julgue os itens a seguir.

75 Todo sistema operacional, como qualquer *software*, está sujeito a falhas de projeto e de construção. A grande vantagem de sistemas abertos é permitir a auditagem de seu código, possibilitando, assim, que a comunidade de usuários possa, de forma relativamente simples, identificar eventuais falhas e criar correções.

76 Uma facilidade normalmente encontrada nos sistemas operacionais do tipo Unix é que estes dispõem de mais de um *shell*. Assim, o usuário pode escolher o *shell* conforme as suas preferências.

77 Para aplicações de tempo real, deve ser dada preferência a sistemas operacionais multitarefa do tipo não-preemptivo.

78 Sistemas operacionais de rede são aqueles utilizados em servidores de rede, os quais permitem que toda uma rede possa ser gerenciada a partir de um ponto central, incluindo autenticação de usuários e configuração de estações de trabalho.

79 O mecanismo básico para proteção de objetos em um sistema operacional é o mecanismo de separação, em que objetos relativos a um usuário são mantidos separados de outros usuários. A técnica de separação física é a mais simples e, por isso, a mais comumente empregada em sistemas operacionais de uso geral.

80 A popularidade do sistema operacional MS Windows decorre do fato de ele ter uma interface amigável com o usuário, não requerendo deste conhecimento especializado acerca de sistemas. Essa popularidade torna o MS Windows bastante vulnerável, pois seus usuários, em geral, desconhecem os mecanismos e configurações de segurança para proteger o sistema de ataques, principalmente um usuário doméstico com conexão à Internet.

Cabeamento estruturado é um padrão de cabeamento para uso integrado em comunicações de voz, dados e imagem, de forma a atender aos mais variados leiautes de uma rede corporativa, por um longo período de tempo, sem exigir modificações físicas da infra-estrutura. Segundo os padrões correntes de cabeamento estruturado, julgue os itens de **81** a **87**.

81 Para se interligar uma estação de trabalho a um roteador, a norma EIA/TIA 568 estabelece que se utilize a conexão padrão 568-A em uma das terminações do cabo e a 568-B na outra. Para a conexão de qualquer um desses equipamentos a um *hub* ou *switch*, pode-se utilizar um cabo com as duas terminações do mesmo padrão, 568-A ou 568-B.

82 Designa-se por cabeamento vertical e cabeamento horizontal o conjunto de cabos permanentes usados para a distribuição vertical e horizontal de uma rede em um prédio.

83 No ambiente de uma rede com cabeamento estruturado, um armário de telecomunicações é o local onde se guardam os equipamentos-reserva de comunicação, indispensáveis para a garantia da continuidade de serviços.

84 O acessório de infra-estrutura para cabeamento estruturado denominado *patch panel* permite a seleção das conexões cruzadas, estabelecendo a que canais de comunicação cada ponto terminal estará conectado.

85 Em um ambiente de cabeamento estruturado, a denominada área de trabalho é uma área reservada dentro da sala de equipamentos para que os técnicos e administradores da rede monitorem e gerenciem o sistema.

86 Em ambiente de redes, designa-se por UTP um cabo de par trançado que faz a distribuição vertical de conexões (*up twisted pair*).

87 Monomodo e multimodo são os dois tipos de fibras ópticas utilizados em comunicação. As fibras multimodo têm a vantagem de poderem cobrir maiores distâncias sem o uso de repetidores, sendo, portanto, as mais empregadas.

Uma infra-estrutura de chaves públicas (ICP) é um conjunto de instrumentos de segurança que permite usuários de uma rede, em princípio insegura, executarem transações de forma segura, por meio do uso de um par de chaves criptográficas (pública e privada) fornecido por uma autoridade confiável. A ICP também provê certificados digitais que podem identificar indivíduos, máquinas e processos. Acerca desse assunto, julgue os itens a seguir.

88 O padrão X.509 V3 permite a adição de campos (extensões) personalizados aos certificados emitidos, como, por exemplo, limitações para o uso do certificado. Dessa forma, é possível restringir a finalidade com que os certificados serão utilizados por aplicações às quais eles venham a ser apresentados.

89 É possível estabelecer uma ICP sem o uso de uma autoridade confiável para a emissão de certificados, sendo a confiança distribuída por meio de uma cadeia de confiança, em que cada usuário pode assinar a chave pública de outro usuário declarando ali o grau de confiança que deposita nessa associação (usuário/chave).

90 O protocolo SSL (*secure sockets layer*), desenvolvido pela Netscape, e o protocolo TLS (*transport layer security*), baseado no SSL e padronizado pelo IETF, são largamente empregados por aplicações cliente/servidor na Internet para o gerenciamento de comunicações seguras utilizando certificados digitais padrão X.509. Esses protocolos oferecem diversos serviços para aplicações em rede, incluindo o de assinatura digital de mensagens.

91 A ICP-Brasil é a infra-estrutura de chaves públicas do governo brasileiro. A política de certificados vigente nessa ICP prevê a emissão de 8 tipos de certificados, sendo 4 para assinatura digital e 4 para sigilo.

92 Certificados digitais têm normalmente um prazo de validade associado, além de poderem ser revogados por diversos motivos. Uma vez que um certificado tenha perdido sua validade, por tempo ou revogação, as chaves por ele certificadas devem ser destruídas, para evitar que possam ser utilizadas de forma fraudulenta.

93 Usualmente, cada usuário de uma PKI necessita de 2 pares de chaves, um para assinatura/conferência e outro para cifração/decifração. Tal necessidade deriva do fato de que a chave privativa para decifração pode necessitar ser copiada para fins de *backup*, mas a chave privativa de assinatura somente pode ser de conhecimento único do próprio usuário, não podendo as duas, nesse caso, serem as mesmas.

94 Um dos problemas gerenciais de uma autoridade certificadora (AC) é o da emissão de uma lista de certificados revogados (LCR). Essa lista deve conter a identificação de todos os certificados que tenham sido revogados por qualquer motivo e deve estar disponível em tempo hábil para consulta por um cliente, sob o risco de um usuário malicioso poder fraudar uma operação. Para reduzir ao mínimo esse risco, foi criado o protocolo LDAP (*lightweigth directory access protocol*), que permite um acesso rápido à base de dados do LCR.

Com referência à auditoria de sistemas computacionais, julgue os itens seguintes.

95 Para que uma auditoria, em geral, tenha sucesso, é imprescindível que seja realizada por uma entidade externa à instituição, a fim de manter independência.

96 Um elemento fundamental para uma auditoria bem feita são as entrevistas com as pessoas relacionadas ao sistema auditado, tais como operadores, programadores, gerentes etc.

97 Ferramentas de apoio a auditoria ou CAATs (*computer assisted audit techniques*) são recursos computacionais usados para facilitar o trabalho de auditoria em sistemas computacionais, tais como ferramentas para extração de dados por amostragem de bancos de dados e *port scanners*.

98 Auditoria envolve a coleta de uma massa de dados a partir de várias fontes. De uma forma geral, dados coletados a partir de documentos arquivados ou obtidos de pessoas físicas devem ser verificados quanto à confiabilidade como evidências. No entanto, dados obtidos diretamente do sistema, como, por exemplo, registros de *log*, são confiáveis por natureza.

99 Entre os pontos gerais a serem normalmente verificados em uma auditoria de sistemas computacionais, incluem-se a política de documentação, a segregação de funções e a existência de um plano de contingência.

A utilização de sistemas de detecção de intrusão ou *intrusion detection systems* (IDS) é uma das formas de se prevenir o sucesso de ataques a um sistema de informações. De acordo com os princípios e técnicas de IDS, julgue os itens a seguir.

100 A utilização de um *firewall* como *gateway* para conexão com o ambiente externo de uma rede torna prescindível o uso de IDS específicos, uma vez que *firewalls* normalmente possuem mecanismos de detecção e bloqueio de ataques à rede.

101 Sistemas de detecção de instrusão enquadram-se em duas categorias: baseados em rede (*network based*) e baseados em *host*. Os primeiros monitoram todo o tráfego em um segmento de rede, procurando por assinaturas que evidenciem uma atividade suspeita, e os demais monitoram a atividade em um *host* específico. Um IDS baseado em rede tende a ser mais complexo e caro, estando sujeito a gerar falsos alarmes com maior freqüência.

102 Uma forma comum de detecção de intrusão é a análise de anomalias estatísticas no sistema, tais como taxa de utilização de CPU e atividade de discos. A desvantagem desses métodos é que não detectam ataques oriundos da rede interna da organização perpetrados por usuários legítimos.

103 Um método de detecção de intrusão é o uso de *honeypots* (potes de mel), que consiste em instalar na rede computadores e sub-redes fictícias inteiras especialmente configurados e maqueados como altamente interessantes (para o atacante). Quando um intruso penetrar na rede, ele será atraído para o *honeypot*, onde se pode monitorá-lo e aprender seus métodos antes que ataque o sistema real.

Com relação a normas e padrões correntes acerca de segurança de sistemas, julgue os itens subseqüentes.

104 A norma ISO-17799, assim como a versão nacional da ABNT NBR-17799, são originárias da norma inglesa BS-7799, que se constitui, basicamente, em um conjunto de recomendações para a gestão da segurança da informação dentro do ambiente de uma organização.

105 A norma FIPS 140-2, estabelecida pelo NIST (*National Institute of Standards and Technology*) dos Estados Unidos da América (EUA), estabelece requisitos de segurança para módulos criptográficos. Essa norma prevê 4 níveis de segurança crescentes e oferece critérios de teste para algoritmos e funções criptográficas de forma a permitir a um desenvolvedor de um módulo o projeto ou a escolha de algoritmos criptográficos apropriados para o nível de segurança pretendido.

106 *Common criteria* — resultado do esforço de organizações de segurança dos EUA, Canadá e alguns países europeus — foi adotada pela ISO (*International Standards Organization*) como a norma internacional ISO 15408. Essa norma estabelece uma metodologia de definição de requisitos de segurança de um produto para avaliar e atribuir uma classificação à segurança de produtos e para gerar toda a documentação que comprove a aplicação desses critérios.

107 Limitações do espaço de endereçamento e também questões de segurança levaram ao desenvolvimento de um novo padrão para o protocolo de rede na Internet, que recebeu a identificação IPv6. O conjunto de serviços de segurança oferecido nessa nova versão do IP, conhecida como IPSec, foi projetado para aplicabilidade tanto na nova versão quanto na versão atual do IP, IPv4.

108 *Request for comments* (RFC) é um tipo de documento formal gerado pelo *Internet Engineering Task Force* (IETF), o qual pode ser apenas para informação ou uma proposta de padronização para a qual se solicita comentários da comunidade interessada. A proposição de novas RFCs é função de especialistas associados à Internet Society por meio do Internet Architecture Board (IAB).

109 O algoritmo de *hashing* SHA-1 (*secure hash algorithm*), largamente utilizado em aplicações de segurança, é um algoritmo padrão da Internet, estabelecido por meio de uma RFC denominada *secure hash standard*.

110 PKIX é a denominação de um grupo de trabalho do IETF criado com o propósito de desenvolver padrões para dar suporte às aplicações na Internet utilizando uma PKI baseada no padrão X.509. As RFCs que definem os protocolos CMP (*certificate management protocol*), OCSP (*online certificate status protocol*) e TSP (*time-stamp protocol*) são frutos do trabalho desse grupo.

A former head of German counter-intelligence recently confided: “The best piece of intelligence is the one that only I possess.” That spymaster’s emphasis on exclusivity and withholding information even from his friends is, alas, the watchword among intelligence chiefs worldwide. And it threatens to undermine efforts to globalize the hunt for terrorists and their bad works.

Timely and credible intelligence — often the merest scrap — can be as decisive in foiling[1] terrorist plotting as any police action, cruise missile, or bomb. That’s why the American Congress and the White House are focused on improving information sharing between the CIA and FBI. But the debate has so far overlooked another chronic intelligence failure: the inadequacy of the CIA’s liaison with other intelligence services.

One reason for urgent reform is that even though the United States far outstrips other countries in its technical intelligence gathering, many other nations often have better human intelligence, or *humint* — real live spies.

[1]foil – to prevent (someone or something) from being successful.

Robert Gerald Livingston. Internet: <http://www.ndol.org/ndol_ci.cfm?kaid=450004&subid=900020&contentid=250680> (with adaptations).

Based on the text above, judge the following items.

111 The best piece of information is not supposed to be available to anyone.

112 The word “one” (ℓ.2) is a numeral.

113 Chiefs agree to the principle that intelligence can only be passed on to some special friends all over the world.

114 The word “threatens” (ℓ.5) can be correctly replaced by **menaces**.

115 Believable and opportune intelligence can decisively replace the action of the police, even cruise missiles, and bombs.

116 The CIA and FBI are yet to establish a process of information interchange.

117 The USA surpasses other countries in terms of technical intelligence collection.

The job of the intelligence officer is to identify those strands that are worth pursuing and then to pursue them until either they are resolved, or they start to look flaky and not worth pursuing, or there is nothing more that can usefully be done. It is a risk-management process. The number of potential leads that can be followed is virtually infinite. On the other hand, covert investigation is extremely resource-intensive and impinges[1] on the human rights of the subject. The threshold[2] for such investigations is therefore high and the number of investigations necessarily limited. Consequently many potential leads have to be discounted. Decisions on which leads to pursue are vital, but are also complex and rich in judgement.

[1] impinge – to have an effect on (something) often causing problems by limiting it in some way.

[2] threshold – a point or level at which something begins or starts to take effect.

Michael Herman. Internet: <http://www.csis-scrs.gc.ca/eng/comment/com83_e.html> (with adaptations).

Based on the text above, judge the items below.

118 It can be deduced that not every piece of information is worth pursuing.

119 In the text, “On the other hand” (ℓ.7) means **out of hand**.

120 In the text, “therefore” (ℓ.10) means **consequently**.

PROVA DISCURSIVA

- Nesta prova — que vale **cinco pontos** —, faça o que se pede, usando a página correspondente do presente caderno para rascunho. Em seguida, transcreva o texto para a folha de **TEXTO DEFINITIVO**, no local apropriado, pois **não serão avaliados fragmentos de texto escritos em locais indevidos**.
- Qualquer fragmento de texto além da extensão máxima de **trinta** linhas será desconsiderado.

ATENÇÃO! Na folha de **texto definitivo**, identifique-se apenas no cabeçalho, pois **não será avaliado** texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.

O sistema de inteligência artificial criado por brasileiros para o Conselho de Segurança da Organização das Nações Unidas (ONU) — chamado de Olimpo — foi selecionado em um universo de 762 outros trabalhos, de todas as partes do mundo, pelo comitê científico da 5.ª Conferência Internacional de Sistemas de Informação de Empresas.

A metodologia empregada chama-se Pesquisa Contextual Estruturada e usa um sistema de extração de informação de textos combinado com a técnica de inteligência artificial conhecida como raciocínio baseado em casos (RBC). Permite fazer buscas rápidas em textos de documentos com base no conhecimento e não apenas em palavras-chave.

Isso quer dizer que, mesmo que o documento não contenha a palavra digitada na pergunta feita pelo usuário, a busca será feita, com base no conceito contido naquela palavra ou em idéias semelhantes a ela.

De acordo com Hugo Hoeschl, coordenador do trabalho, "é estratégico o Brasil ser detentor de uma tecnologia tão forte, com denso reconhecimento internacional, desenvolvida especialmente para ser aplicada em segurança". Por sua rapidez e precisão, o sistema de busca "é importante para todos os organismos da ONU e fornecerá significativos benefícios para a solução de conflitos internacionais".

Liana John. Internet: <http://www.estadao.com.br/ciencia/noticias/2003/jan/07/79.htm> (com adaptações).

A origem remota da Atividade de Inteligência no Brasil, outrora denominada Atividade de Informações, ocorreu com o advento do Conselho de Defesa Nacional, mediante o Decreto n.º 17.999, de 29 de novembro de 1927. Esse Conselho, constituído pelo presidente da República e pelos ministros de Estado, tinha por destinação, entre outras, a tarefa de "coordenar a produção de conhecimentos sobre questões de ordem financeira, econômica, bélica e moral referentes à defesa da Pátria". Como fica claro na missão, interessava ao governo a produção de informações com finalidade precípua de defender a Pátria, isto é, informações vinculadas a interesses estratégicos de segurança do Estado.

Internet: <http://www.abin.gov.br/abin/historico.jsp>.

Considerando que as idéias apresentadas nos textos acima têm caráter unicamente motivador, redija um texto dissertativo, posicionando-se acerca do seguinte tema.

A INFORMAÇÃO COMO FATOR ESTRATÉGICO DE SEGURANÇA

RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	