CONHECIMENTOS ESPECÍFICOS

Acerca da ISO 38500 e do COBIT 5, julgue os itens subsequentes.

51 A ISO 38500 aponta como princípios, entre outros, a responsabilidade e a aquisição. O primeiro versa sobre indivíduos dentro da organização, que compreendem e aceitam suas responsabilidades com respeito ao fornecimento e à demanda de TI. O segundo diz respeito à aquisição realizada por razões válidas, embasadas em análise apropriada e contínua.

52 O COBIT 5 descreve um modelo único e integrado de princípios que permite governar e gerir a TI de forma holística para toda a organização, o que abrange todas as áreas responsáveis pelas funções de TI e considera tanto os interesses internos quanto os interesses externos relacionados à TI.

A respeito de gerenciamento de serviços, julgue os próximos itens.

53 A classificação dos processos na ISO/IEC 20000 compreende entrega de serviços, controle, liberação, resolução e relacionamento. O processo de gerenciamento de segurança da informação é classificado como de entrega.

54 No ITIL, o gerenciamento de continuidade de negócio é responsável por garantir que os serviços de TI atendam às necessidades atuais e futuras do negócio dentro do orçamento planejado, e por gerenciar a redução de riscos a um nível aceitável.

Em relação a gerenciamento de projetos com base no PMBOK 5, julgue os itens a seguir.

55 O controle do cronograma abrange a monitoração do andamento das atividades do projeto com vistas a atualizar seu progresso, que, no caso de utilização de um método ágil de desenvolvimento, abrange a repriorização do plano de trabalho restante (*backlog*).

56 Os processos de iniciação, entre eles, o desenvolvimento do termo de abertura do projeto, devem ser realizados no padrão tático-estratégico e embutidos no nível de controle do projeto, visto que, antes de se iniciar o projeto, há a necessidade de que os requisitos de alto nível sejam elucidados e o controle macro do projeto seja realizado também por parte dos gestores da organização.

Julgue os itens seguintes a respeito da IN n.º 4 MPOG/SLTI e da Resolução CNJ n.º 182.

57 De acordo com a Resolução CNJ n.º 182, o planejamento das contratações de solução de TI e comunicação incluirá as seguintes fases: análise de viabilidade da contratação, análise dos aspectos técnicos da solução e análise dos aspectos administrativos da contratação.

58 De acordo com a IN n.º 4 MPOG/SLTI, a gestão de processos de TI, que inclui a gestão de segurança da informação, não poderá ser objeto de contratação, salvo se aprovado pela autoridade máxima do órgão ou entidade, e desde que esteja sob supervisão exclusiva de servidores do órgão ou entidade.

Julgue o item a seguir com relação à norma ISO 27005.

59 A ISO 27005, que estabelece guias de referência para gerenciamento de risco em segurança da informação, é aplicável na maior parte das organizações, com exceção das agências de governo.

Julgue os itens seguintes, relativos à política de segurança da informação e comunicações (POSIC).

60 Uma POSIC pode ser complementada por normas e procedimentos que a referenciem, o que propicia a criação de um corpo normativo.

61 A POSIC de uma organização deve estabelecer critérios para determinar competências e responsabilidades relacionadas à segurança da informação, bem como ser constantemente revista e atualizada.

No que se refere à gestão de continuidade de negócio (GCN), julgue os itens subsequentes.

62 Cabe à GCN identificar, quantificar e priorizar os riscos aos produtos e aos serviços fundamentais para uma organização; a análise de risco reconhece as prioridades que farão a organização cumprir constantemente suas obrigações, mesmo diante de um incidente ou de uma situação de crise.

63 Em uma visão de GCN, sistemas, processos e pessoas envolvidas nas atividades da organização devem ser mapeados. Na visão da GCN não é necessário fazer levantamento de possíveis ameaças e análise de risco, já que isso é objetivo de outras áreas da segurança da informação.

Na área de gerenciamento de incidentes de segurança da informação, é comum a formação de equipes de tratamento e resposta a incidentes de redes. Acerca desse assunto, julgue os itens subsecutivos.

64 Ao se estabelecer a visão proposta pela equipe de resposta a incidentes, é importante que esta seja comunicada a outros indivíduos da organização para fins de contribuição mútua. Essa circunstância permite identificar, antes da implementação, problemas organizacionais ou no processo da equipe de resposta a incidentes.

65 As equipes de resposta a incidentes são normalmente constituídas por especialistas em segurança da informação e por administradores de sistemas e de redes. No entanto, outros profissionais com perfis técnicos e administrativos poderão, indistintamente, integrar essas equipes.

Julgue os itens a seguir com relação ao gerenciamento de contas de usuários no Linux e no Windows 2012 Server R2.

66 Em versões modernas do Linux, o arquivo `/etc/shadow` armazena as senhas criptografadas e as informações adicionais sobre as senhas dos usuários.

67 O Linux apresenta restrição de mecanismos de bloqueio de acesso a arquivo de senha `passwd`. Assim, qualquer usuário pode ler esse arquivo e verificar os nomes de usuários.

68 No Windows 2012 Server R2, os dados dos usuários do (AD) *Active Directory* ficam armazenados em um gerenciador de banco de dados do SQL Server. Logo o administrador do SQL Server também tem poderes administrativos sobre o domínio AD.

Em geral, um *buffer overflow* se caracteriza por permitir a sobrescrita de espaços de memória utilizados por um processo, o que pode ser realizado intencionalmente ou não. A esse respeito, julgue os itens que se seguem.

69 Uma vez que o uso de *buffer overflow* é considerado genérico em segurança da informação, ele é independente da arquitetura do processador.

70 O seguinte trecho de código não é passível de um ataque *buffer overflow*.

```
#include <stdio.h>
#include <string.h>

  void fun1(void)
  {
       char arg2[10];
       gets(arg2);
       printf("%s\n", arg2);
  }
int main(void)
  {
       printf("Isso pode?\n");
       fun1();
       printf("Sim, pode...\n");
       return 0;
  }
```

O termo APT (*advanced persistent threat*) é utilizado em segurança da informação para descrever ameaças cibernéticas através de técnicas de coleta de informações que tenham valor para o atacante. Acerca desse assunto, julgue os itens subsequentes.

71 APTs podem utilizar diversos protocolos de rede para transmitir ou receber informações do ponto de comando e controle do *malware*. Normalmente esse tráfego é construído pelo atacante para parecer um tráfego de rede legítimo.

72 Em geral, uma APT não é detectada por antivírus ou por *softwares* IDS firmados em assinaturas.

73 Os *rootkits*, que normalmente são encontrados em APTs, não somente podem esconder a existência de certos processos ou programas de métodos normais de detecção mas também permitir uso contínuo com acesso privilegiado a determinado recurso.

Julgue os itens seguintes, a respeito do HTTPS e das técnicas de proteção que envolvem o uso do protocolo TLS.

74 A técnica de compressão não é recomendada ao se utilizar a versão 2 do HTTP sobre o protocolo TLS 1.2.

75 Na implementação do HTTP versão 2 sobre o protocolo TLS 1.2, é mandatório desabilitar a renegociação da conexão.

76 No HTTP, a técnica geral do controle de fluxo garante que não haja interferência entre as conexões independentes. Entretanto essa técnica foi abandonada na versão 2 do HTTP, que criou o conceito de `WINDOW_UPDATE` *frame*.

Considerando que um *firewall* seja utilizado com o IPTABLES configurado corretamente e com a quantidade adequada de interfaces, julgue os itens subsecutivos.

77 A execução do código mostrado a seguir provocará o bloqueio do tráfego de saída do ICMP do tipo `echo-request`.

```
iptables –A OUTPUT -p icmp --icmp-type echo-request
-j DROP
```

78 O comando mostrado a seguir redireciona uma conexão TCP da porta `5000` para a porta `22`.

```
iptables -t nat -A PREROUTING -p tcp --dport
22 -j REDIRECT --to-ports 5000
```

Acerca dos modos de funcionamento do SELinux, julgue os próximos itens.

79 No modo *Permissive*, o SELinux estará habilitado, mas apenas gera alarmes e *log* das ações no sistema.

80 O modo de funcionamento *Enforcing*, que não é o padrão do SELinux, nega acesso a recursos e impede o *log* das ações realizadas no sistema.

A respeito da configuração e da administração de sistemas gerenciadores de bancos de dados (SGBD) e de produtos a eles relacionados, julgue os itens a seguir.

81 Apenas instalações autônomas de SQL Server permitem o uso de servidor de arquivos SMB como opção de armazenamento.

82 No PostgreSQL, mesmo usando-se o parâmetro de configuração `listen_address = '*'`, é possível controlar os usuários que poderão se conectar ao banco de dados.

83 No PostgreSQL, mudanças nas configurações de memória compartilhada exigem que o banco de dados seja totalmente reiniciado.

84 A ocorrência de falha em uma instância do DB2 PureScale exige a interferência do administrador do banco de dados para que os recursos sejam reiniciados, devendo a forma de notificação da falha ser configurada pelo administrador.

85 Na instalação do DB2 PureScale em Linux, se um usuário existente for selecionado como proprietário de instância do DB2, ele deverá existir com o mesmo UID em todos os *hosts*.

86 Se, na modificação de determinada instância existente de SQL Server, for realizada a instalação de componentes de replicação, será necessário reiniciar o agente de SQL Server.

Julgue os itens subsequentes, relativos a projetos de bancos de dados.

87 Durante a normalização de tabelas, devem ser priorizadas as decomposições sem perdas que levam a projeções independentes.

88 Qualquer atributo de uma tabela representada na terceira forma normal pode ser alterado sem que ocorra interferência nos demais atributos.

No que se refere à organização de arquivos e métodos de acesso a bancos de dados, julgue os próximos itens.

89 O acesso direto a registros será eficiente ao se usar funções *hash*, visto que essas funções garantem uma relação unívoca entre o registro e a sua localização física.

90 A utilização de árvores-B+ para implementar acesso indexado a registros é eficiente quando se trata de aplicação em que a operação predominante é a inclusão de novos registros.

91 As vantagens dos arquivos *hash* incluem a otimização no uso do espaço físico em disco.

A respeito de tipos de bancos de dados, julgue os itens que se seguem.

92 A capacidade de estender tipos de dados básicos é uma das características dos bancos de dados objeto relacional.

93 Sistemas de bancos de dados classificados como NoSQL permitem a inserção de dados sem que haja um esquema predefinido.

A respeito de *tunning* de bancos de dados, julgue os itens subsecutivos.

94 O uso de *correlated subquery* aumenta o desempenho na execução de consultas a bancos de dados.

95 Ao se realizar o *tunning* de um PostgreSQL, o valor atribuído à variável `effective_cache_size` pode influenciar o uso adequado de índices durante a execução de consultas.

Acerca de subsistemas de armazenamento de dados e de compartilhamento de arquivos, julgue os itens que se seguem.

96 O CIFS, protocolo usado em uma NAS para o compartilhamento de arquivos, exige o uso de serviço auxiliar para evitar que um usuário sobrescreva o trabalho dos demais usuários em determinado arquivo.

97 A implementação de RAID via *software* apresenta desempenho inferior se comparada à implementação de RAID via *hardware*.

98 Os fatores que interferem no desempenho de uma NAS incluem o serviço de autenticação utilizado, o número de retransmissões realizadas devido a erros e o tempo despendido para acessar um arquivo em um dispositivo NAS.

Julgue os próximos itens, relativos à computação na nuvem.

99 Em provedor que fornece serviço como IaaS (*infrastructure-as-a-service*), o consumidor consegue configurar o sistema operacional utilizado pela nuvem.

100 A possibilidade de monitorar e controlar os recursos utilizados na computação na nuvem proporciona maior transparência tanto para o provedor quanto para o consumidor do serviço.

Julgue os itens a seguir, relativos a sistemas de arquivos e tecnologias de becape.

101 Usando-se a ferramenta RSync para se executar o comando `rsync –av--delete /original/ /backup/`, uma cópia dos arquivos do diretório `/original/` será armazenada no diretório `/backup/`, e os arquivos previamente copiados para o diretório `/backup/` e apagados no diretório `/original/` serão apagados também no diretório `/backup/`.

102 Para aumentar o desempenho do NTFS, recomenda-se a utilização da técnica de *journaling*, que grava, em um *log*, as operações que serão executadas no sistema de arquivos antes mesmo de suas execuções.

Considerando que as partes A e B se comuniquem de forma confidencial usando criptografia simétrica, de modo que ambas as partes cifrem suas mensagens antes de enviá-las, julgue os itens seguintes, relativos a criptografia.

103 A parte A pode usar as mensagens cifradas pela parte B para provar a autenticidade dessas mensagens para terceiros.

104 As partes A e B compartilham a mesma chave criptográfica, também denominada chave secreta.

105 AES e 3DES são exemplos de algoritmos criptográficos que podem ser usados pelas partes A e B.

Acerca dos servidores de aplicação JEE e Red Hat JBoss, julgue os itens subsequentes.

106 É possível executar múltiplas instâncias *standalone* do Red Hat JBoss em uma máquina que suporta apenas um endereço de rede.

107 Por meio da interface de gerenciamento CLI do Red Hat JBoss, o comando `deploy aplicacao.war` permite implantar uma aplicação cujo *deployment* esteja em `aplicacao.war` em um servidor *standalone*.

108 GlassFish e TomCat são exemplos de servidores de aplicação JEE que suportam a tecnologia EJB.

Julgue os próximos itens, relativos ao VMWare.

109 O VMWare, embora aumente a produtividade, não possibilita reduzir custos de TI em uma organização.

110 O VMWare é útil em ambientes de suporte devido ao fato de permitir a execução simultânea de diferentes sistemas operacionais em uma única máquina física.

Com relação às disposições do Regimento Interno (RI) do Tribunal de Justiça do Distrito Federal e dos Territórios (TJDFT), julgue os itens a seguir.

111 Caso um advogado impetre pedido de *habeas corpus* no TJDFT em favor de um cliente seu e a referida medida for concedida, a decisão será cumprida, independentemente de acórdão.

112 Se um servidor da justiça do Distrito Federal (DF) cometer infração disciplinar cuja penalidade, após processo disciplinar, seja a demissão, a autoridade responsável para aplicá-la será o corregedor da justiça.

113 Se um desembargador afastar-se de suas funções por um período de quarenta dias, o presidente do TJDFT designará um juiz de direito substituto de segundo grau para substituí-lo, o que vinculará esse juiz aos processos que lhe possam ser distribuídos durante o período da substituição.

114 O presidente e o vice-presidente do tribunal e o corregedor da justiça integram o Conselho Especial do TJDFT; os demais desembargadores integrantes desse conselho são eleitos pelo Tribunal Pleno.

Ainda com base no RI do TJDFT, julgue os itens que se seguem.

115 Se secretário de governo do DF cometer crime comum no período em que exerce a função, ele será processado e julgado originariamente pelo Tribunal Pleno do TJDFT.

116 O corregedor da justiça do TJDFT integra o Conselho da Magistratura, logo pode exercer, nesse conselho, as funções de relator e de revisor.

Acerca da organização judiciária do DF e dos territórios, julgue os itens a seguir.

117 Um quinto dos cargos de desembargador devem ser preenchidos por membros do Ministério Público do Distrito Federal e Territórios e por advogados em efetivo exercício da profissão.

118 Ação de indenização por acidente de trabalho ajuizada por servidor contra o DF deverá ser processada e julgada por uma das varas de fazenda pública.

119 O TJDFT tem competência originária para processar e julgar o governador e o vice-governador do DF em crimes comuns e de responsabilidade.

120 Cabe aos juízes de direito aplicar penalidades disciplinares a servidores que lhes sejam subordinados, desde que a pena não exceda a trinta dias de suspensão.

Espaço livre