

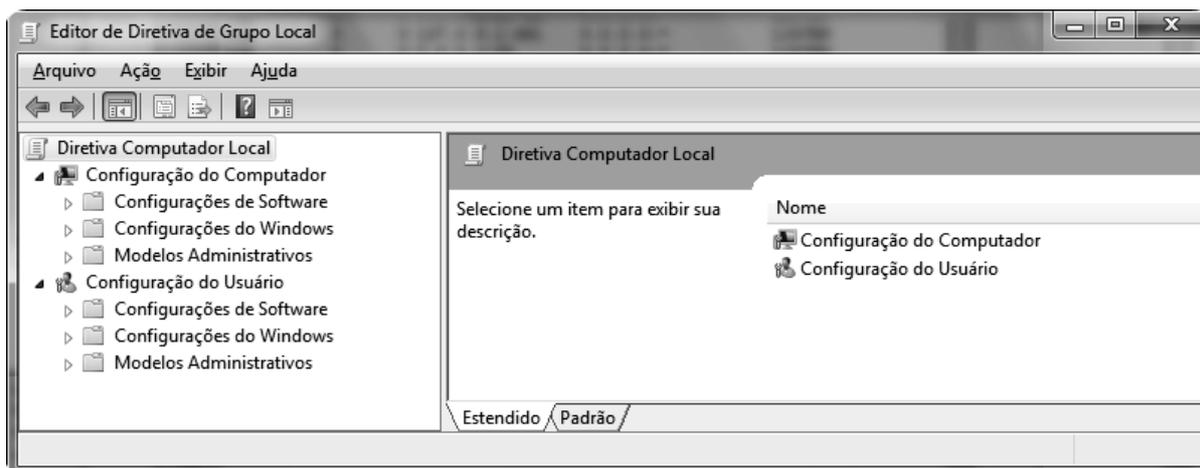
CONHECIMENTOS ESPECÍFICOS

Active Internet connections (servers and established)

| Proto | Recv-Q | Send-Q | Local Address | foreign Address | State |
|-------|--------|--------|-----------------|-----------------|--------|
| tcp | 0 | 0 | 0.0.0.0:5666 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:49574 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:903 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:10024 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:10025 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:3310 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:53487 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:111 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:1556 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:1557 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:13782 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 127.0.0.1:631 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:25 | 0.0.0.0:* | LISTEN |
| tcp | 0 | 0 | 0.0.0.0:13724 | 0.0.0.0:* | LISTEN |
| . | . | . | . | . | . |
| . | . | . | . | . | . |
| . | . | . | . | . | . |

Considerando os dados acima, que foram coletados em uma máquina e mostram o *status* de alguns serviços em um sistema operacional CentOS 5.8 ou superior, com configuração padrão em relação aos serviços, julgue os itens a seguir.

- 51 Um servidor HTTP está em funcionamento nesse sistema.
- 52 O servidor CUPS, utilizado para serviços de impressão, está em funcionamento na máquina em questão.
- 53 O comando `netstat -nap` permite ao administrador ver quais são os processos relacionados com cada conexão em aberto nesse sistema operacional.



A figura acima representa a tela de edição de diretivas de grupo local em um sistema operacional Windows 7 Enterprise (gpedit.msc) em rede local. Julgue os próximos itens, relativos à interface mostrada na figura e ao gpedit.msc.

- 54 Por meio do gpedit.msc, é possível configurar programas que poderão ser executados logo após o usuário fazer *logon* na máquina.
- 55 Nessa interface, é possível fazer configurações personalizadas para o uso de atualizações do Windows (Windows *update*) e direcionar o sistema em questão para um servidor de atualizações interno em uma rede local.
- 56 O gpedit.msc permite alterar configurações de *logon* do Windows.

Em códigos de programas, é muito comum o uso de estruturas condicionais para que determinado código seja executado mediante o atendimento de determinada condição. Julgue os itens que se seguem, a respeito dessas estruturas.

- 57 Na linguagem C, a estrutura `for` realiza basicamente a seguinte sequência: primeiro, uma variável é inicializada; segundo, uma condição é checada; se a condição é satisfeita, então um trecho de código é executado e, em seguida, a variável é incrementada ou decrementada segundo a declaração do código; então, a condição é checada novamente e o ciclo se repete enquanto a condição `for` for satisfeita.
- 58 A estrutura `while` é um tipo de *loop* em que o código nela contido será executado até que a condição especificada de parada seja satisfeita.
- 59 Em estruturas do tipo `case`, a execução de código ocorre somente no caso de determinada condição especificada na estrutura ter sido satisfeita.

```
1 #!/bin/bash
2 if [[ $ EUID -ne 0 ]]; then
3 echo "Not Permitted" 2>&1
4 exit 1
5 else
6 mount /dev/sda1 /mnt/dev1
7 fi
```

Acerca do trecho de código acima, julgue os itens subsequentes.

- 60 Caso a condição de execução seja satisfeita, o sistema montará um DVD com partição 1 no diretório `/dev/sda1`.
- 61 O código de programa na linha 1 determina que o sistema use o interpretador `bash`.
- 62 O trecho de código na linha 2 verifica se o usuário é *root* do sistema.

A respeito da instalação do sistema de gerenciamento de banco de dados (SGBD) Postgree SQL 9.1 em sistemas Linux, que necessita ser feita manualmente em alguns casos, julgue os itens a seguir.

- 63 É impossível fazer a instalação do Postgree SQL com suporte ao protocolo LDAP.
- 64 Para uma instalação básica, após a verificação de alguns requisitos básicos e a descompactação do pacote de *software*, o comando `./configure` deve ser executado no diretório em que o *software* tiver sido descompactado.
- 65 Quando se utiliza um compilador GNU Make, os comandos `gmake`, `gmake check` e `gmake install` são utilizados, respectivamente, para se compilar o sistema, fazer a checagem do sistema e instalar o sistema com a configuração padrão. Para executar o comando `gmake check`, o usuário deverá ter privilégios de superusuário.

Julgue os itens seguintes, referentes a segurança física e segurança lógica de sistemas.

- 66 A segurança lógica é responsável por medidas de controle que permitam que usuários e sistemas acessem informação que esteja explicitamente permitida. Nesse sentido, as etapas de autenticação e autorização são consideradas práticas inadequadas de segurança lógica.
- 67 No processo de identificação de categorias de funcionários em uma organização, é considerada boa prática de segurança física a adoção de mecanismos de identificação que sejam capazes de distinguir funcionários de visitantes e categorias diferenciadas de funcionários, por meio do uso de dispositivos de identificação com uso de sistema de cores.

A respeito de sistemas de criptografia e tipos de criptografia utilizados em sistemas de segurança de rede, julgue os itens a seguir.

- 68 A criptografia simétrica é específica para conexões de rede não monitoradas. Uma desvantagem dessa técnica de criptografia é o fato de que, por meio de um ataque de CBC (*cypher block chaining*), um atacante pode extrair dados legíveis de uma conexão de rede interceptada.
- 69 Se um usuário A quiser enviar uma mensagem cifrada unicamente para um usuário B, sem que outros usuários sejam capazes de decifrá-la, um mecanismo de cifra adequado nesse caso envolverá o uso de criptografia de chave pública ou assimétrica.
- 70 O algoritmo AES (*advanced encryption standard*) permite, entre outras funcionalidades, a utilização de cifras assimétricas durante o uso de uma sessão SSL/TLS.

Com relação a sistemas antivírus e *malwares*, em geral, julgue os próximos itens.

- 71 Um mesmo vírus de computador é capaz de infectar várias máquinas. Uma estação de trabalho, normalmente, pode conter vários vírus diferentes e aptos a serem executados ao mesmo tempo.
- 72 Uma característica dos vírus de computador do tipo *worm* é a sua incapacidade de se disseminar autonomamente: eles necessitam da intervenção de um usuário que os execute e, só assim, se propagam e infectam outros usuários.

Julgue os itens a seguir, relativos a sistemas de detecção de intrusão (IDS).

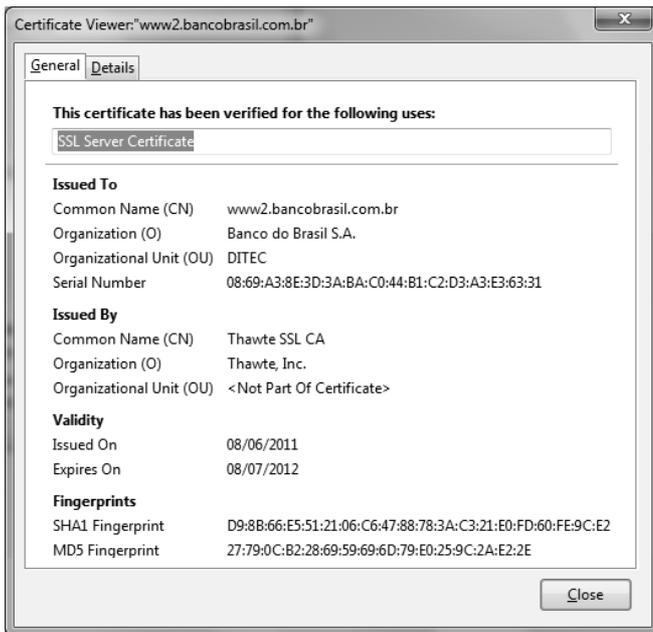
- 73 Em IDS, um falso negativo é uma situação que caracteriza que um sistema não está sob ataque.
- 74 Um IDS, diferentemente de um *firewall*, é capaz de reagir e enviar solicitação de desconexão quando detecta alguma anomalia de tráfego na rede.
- 75 No IDS, erros do tipo falso positivo podem levar usuários a ignorar a saída dos dados porque tratam ações legítimas como tentativas de invasão.

Julgue os itens que se seguem com base na norma ISO 27001, que estabelece um conjunto de diretrizes e práticas de segurança da informação.

- 76 Um evento de segurança da informação é uma ocorrência em um sistema, serviço ou rede que pode violar a política de segurança da informação ou causar falha de controles.
- 77 Os requisitos especificados nas seções de 4 a 8 da referida norma podem ser ignorados em casos de conformidade com o que a norma estabelece.

Em segurança da informação, um risco é um evento ou uma condição incerta que pode causar algum dano a um sistema de informação ou até à própria organização como um todo. Com referência à avaliação de riscos, julgue os próximos itens.

- 78 Em uma organização, a identificação de vulnerabilidades é uma atividade importante, que deve ser realizada em conjunto com a avaliação de riscos.
- 79 Em avaliação de riscos, os riscos podem ser analisados de acordo com sua probabilidade de acontecimento e com os possíveis impactos que eles podem causar.



A figura acima ilustra o certificado digital de Internet banking do sítio do Banco do Brasil. Considerando esse certificado, julgue os itens a seguir.

- 80 Os campos CN, O, OU são comuns em certificados digitais. Além desses campos, outros campos adicionais podem ser utilizados, desde que sejam observadas as devidas restrições de uso dos campos.
- 81 A assinatura digital produzida mediante o uso do algoritmo MD5 gera uma saída de 16 bytes.
- 82 Assinaturas SHA1 para certificados de 1.024 bits terminam com a sequência hexadecimal 9C:E2. Portanto, a chave pública do certificado mostrado na figura é de 1.024 bits.

Julgue os seguintes itens, referentes a modelo relacional de banco de dados e teoria de SGBDs.

- 83 A regra de integridade referencial estabelece que, se um conjunto de atributos *CE* for de uma chave estrangeira de uma relação *X* que faça referência a uma relação *S*, que tenha por chave primária *CA*, então, para toda tupla *N* com extensão de *S*, os valores para o conjunto de atributos de *CA* da tupla *N* serão nulos.
- 84 A regra de integridade de uma chave primária estabelece que, se um conjunto de atributos denominado *CA* for a chave primária de uma relação *X*, então a extensão de *X* não poderá ter, em nenhum momento, duas tuplas com a mesma combinação de valores para os atributos de *CA*.

Uma organização que possui baixa maturidade em gerenciamento de serviços de tecnologia da informação (TI) decidiu adotar algumas práticas preconizadas pelo modelo ITIL e, para isso, definiu uma estratégia de curto prazo, com foco no uso do modelo ITIL versão 2, priorizando os seguintes processos: *service desk*, gerenciamento de incidentes, gerenciamento de problemas e gerenciamento de configuração.

Tendo como referência a situação hipotética acima, julgue os itens a seguir, relativos à estratégia adotada pela organização.

- 85 Os processos priorizados pela organização são definidos e especificados detalhadamente na documentação oficial do ITIL versão 2. A partir da implementação desses processos, a organização deve se adaptar à estrutura de tarefas padronizadas nessa norma.
- 86 Os processos prioritários definidos pela organização não incluem os processos do grupo de processos de entrega de serviços do ITIL versão 2.
- 87 A estratégia adotada pela organização não poderá acarretar aumento da maturidade de gerenciamento de serviços de TI no curto prazo, visto que, nessa estratégia, é considerada apenas parte dos processos do ciclo de suporte de serviços.
- 88 O gerenciamento de configuração — que serve de base para todas as outras práticas definidas no modelo ITIL versão 2 — consiste em prática adequada para a situação hipotética em tela, pois, caso não seja realizada, a implementação dos demais processos será bastante complexa.

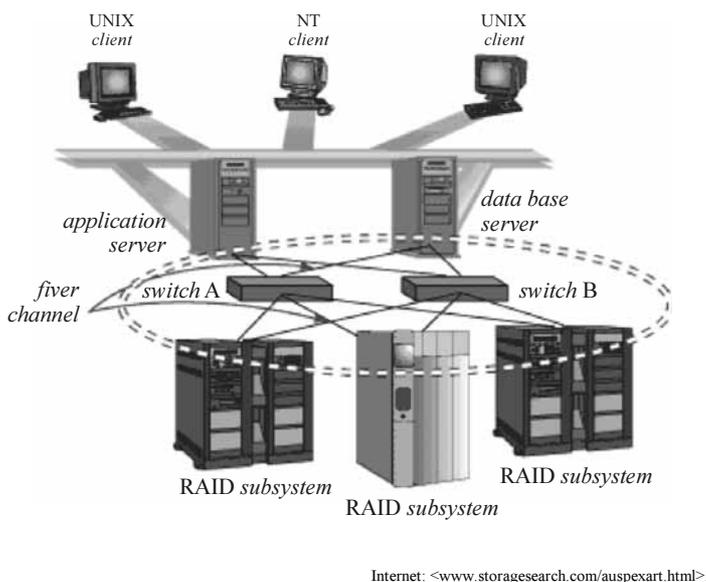
Em ambientes de *datacenters* bancários, é comum a coexistência de recursos de *hardware* considerados de plataforma baixa e os de plataforma alta. Acerca das razões técnicas que causam essa coexistência, julgue os itens seguintes.

- 89 Ambientes de plataforma baixa podem ser implementados, indiferentemente, por meio das plataformas RISC ou CISC.
- 90 Servidores de plataforma baixa com arquitetura RISC têm sido a principal escolha para implementação de servidores de aplicação em portais corporativos e de Internet banking.
- 91 *Mainframe* está presente nesses ambientes, em virtude de consistir em solução tecnológica com uso demonstrado para cargas de trabalho definidas por elevado número de transações concorrentes, com requisitos de alta disponibilidade e confiabilidade.

Com o advento da World Wide Web (WWW) e da Internet, muitas tecnologias utilizadas em ambientes bancários passaram a ter como base os padrões de codificação da informação definidos e empregados nessas redes. Com relação a esses padrões, julgue os itens que se seguem.

- 92 O protocolo IBM 3270 não é aderente ao modelo WWW.
- 93 XML consiste em um padrão de representação de informação extensível que, por isso, pode ser usado para representar tanto informação estruturada como não estruturada.

Figura para os itens de 94 a 101.



Com base na arquitetura de infraestrutura de armazenamento de dados (*storage*) corporativa representada na figura, bem como nos conceitos e tecnologias relativos a armazenamento de dados, julgue os próximos itens.

- 94 A infraestrutura representada na figura acima pode constituir uma representação para a implementação de um *storage area network* (SAN).
- 95 Em virtude de os *switches* não estarem interconectados entre si na configuração acima, a arquitetura representada é incapaz de utilizar *inter switch link* (ISL) ou entroncamento (*trunk*).
- 96 Zoneamento de *fiber channel* é usado para tornar os diversos discos virtuais (LUNs) acessíveis a todos os dispositivos conectados a uma SAN.
- 97 Fitotecas são adicionadas à arquitetura em tela por meio de interfaces SAN implementadas na rede *fiber channel*, com o objetivo de tornar os dados armazenados em fita disponíveis a todos os dispositivos conectados à SAN, do mesmo modo que os sistemas de armazenamento em disco.
- 98 Na configuração mostrada na figura acima, os *switches* que implementam a rede *fiber channel* podem ser considerados como *fiber channel directors*.

Considerando que, na figura apresentada, o sistema de armazenamento de discos empregue a tecnologia RAID (*redundant array of independent/inexpensive drives*), comumente presente nesse tipo de sistema, julgue os itens subsecutivos.

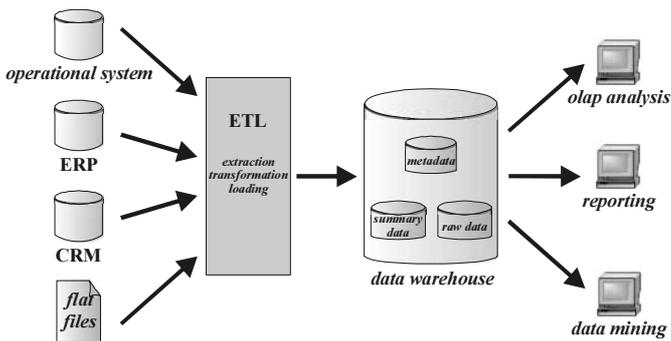
- 99 As tecnologias RAID proporcionam aumento do desempenho do acesso a disco, em decorrência da distribuição de blocos de dados em estrias (*stripes*), por meio de discos diferentes, que podem ser acessados concorrentemente.
- 100 Em tecnologia RAID 5, são usados dados redundantes que possibilitam a recuperação de dados caso um dos discos do arranjo falhe. Essa tecnologia, no entanto, não permite a recuperação de dados caso haja falha simultânea de dois discos que contenham blocos de dados de um mesmo arquivo.
- 101 A tecnologia RAID 0 pressupõe a existência de dois ou mais discos configurados com dados distribuídos redundantemente entre eles, de modo que, caso um dos discos do arranjo falhe, as configurações RAID 0 introduzem um mecanismo eficiente de proteção contra perda de dados.

As tecnologias de virtualização de servidores trouxeram uma série de benefícios aos ambientes de TI corporativos, sendo tecnologias estruturantes em *datacenters* modernos. Entre os produtos disponíveis para a implementação de virtualização de servidores, incluem-se os produtos das famílias VMWARE e XEN. Acerca desses produtos e de suas características, julgue os itens a seguir.

- 102 A tecnologia de virtualização VMWARE permite a configuração de máquinas virtuais (VMs) em configuração de *cluster* de alta disponibilidade, de modo que, quando um servidor físico do *cluster* falha, as máquinas virtuais que executavam no servidor são migradas automaticamente para outro servidor do *cluster*.
- 103 As tecnologias de virtualização VMWARE e XEN distribuem *cores* de processamento e memória de um servidor físico entre as máquinas virtuais instaladas nesse servidor, devendo o número de máquinas virtuais criadas em um servidor físico limitar-se ao número de *cores* de processamento existentes no servidor, já que cada máquina virtual deve ter, pelo menos, um *core* de processamento alocado.
- 104 Para se compararem os produtos VMWARE e XEN, podem-se avaliar as especificações técnicas do *hypervisor* utilizado mediante as seguintes características: tipo de sistema operacional convidado suportado, número de máquinas virtuais e de CPUs virtuais suportados (taxa de consolidação), número máximo de CPUs virtuais e tamanho máximo de memória RAM por máquina virtual.
- 105 Máquinas virtuais são criadas a partir de imagens de máquinas virtuais, que são arquivos binários contendo uma imagem de disco do sistema operacional convidado. Um dos padrões de indústria para essas imagens consiste no *open virtualization format* (OVD), que possibilita a interoperabilidade e que é suportado pela tecnologia XEN, mas não é suportado pelos produtos VMWARE, que utilizam um formato de imagens proprietário.

A coexistência de ambientes de plataforma alta e de plataforma baixa resulta em desafios tecnológicos para integração de plataformas. Com relação a essa integração, julgue os itens seguintes.

- 106 A plataforma baixa é a plataforma *de facto* para processamento de *back-end*, enquanto a plataforma alta faz a implementação de processamento de *front-end*.
- 107 Uma técnica comumente usada para a integração consiste na migração de aplicações de plataforma alta para plataforma baixa, e vice-versa.
- 108 Aplicações legadas que rodam em plataforma alta podem ser expostas como serviço e integradas em aplicações desenvolvidas para plataforma baixa, mediante uma abordagem de arquitetura orientada a serviço (SOA).



Internet: <www.infoescola.com/informatica/data-warehouse>

Considerando a figura acima, que representa um esquema básico do processo de desenvolvimento de um armazém de dados (*data warehouse*), julgue os itens que se seguem.

- 109 A exploração de dados com OLAP requer a extração da informação original para um *data warehouse*, conforme ilustrado na figura, e não pode ser realizada diretamente em bases de dados relacionais.
- 110 O processo de extração, transformação e carga (ETL) ilustrado permite extrair dados de diversas fontes de dados e migrá-los para o *data warehouse*, mantendo sua estrutura e normalização originais.
- 111 Os modelos de dados usados no *data warehouse* são frequentemente constituídos por modelos dimensionais, em que um mesmo dado pode ser fisicamente gravado mais de uma vez. Entre as razões de esses modelos serem utilizados, destaca-se o aumento do desempenho em consultas a grandes volumes de dados associados a realizações de uma dimensão do modelo.

Acerca de arquiteturas computacionais para processamento de alto desempenho e alta disponibilidade, julgue os próximos itens.

- 112 No modelo de computação em *grid*, diversos nodos de processamento são coordenados para operarem como se fossem um único sistema, por meio de técnicas de compartilhamento de memória secundária.
- 113 *Clusters* computacionais podem ser utilizados para criar sistemas de computação que agreguem as propriedades de alta capacidade de processamento (desempenho) e alta disponibilidade. Para a constituição desses sistemas, são geralmente utilizados recursos de *hardware* cuja configuração básica e desempenho sejam semelhantes, pois isso facilita o projeto da função de distribuição de carga e controle de disponibilidade.

Servidores de aplicação são elementos comuns na arquitetura de implantação de sistemas e aplicações com base em tecnologia *web*. Atualmente, existe uma grande variedade de servidores de aplicação que suportam diferentes *frameworks* de desenvolvimento de *software*. A respeito dos servidores de aplicação utilizados no mercado corporativo, julgue os itens subsecutivos.

- 114 O IBM Web Sphere Application Server suporta diversos servidores *web* comumente disponíveis, como, por exemplo, o Apache Web Server e o IIS.
- 115 O IIS da Microsoft é um servidor *web* concebido para ser utilizado com o *framework* NET e, por isso, requer *software* adicional para executar aplicações com base em *framework* J2EE.
- 116 Os servidores de aplicação Tomcat e JBoss são concebidos para operar nativamente com o *framework* de desenvolvimento J2EE, além de possuírem suporte para diversos sistemas gerenciadores de bancos de dados, tais como SQL Server, Oracle, DB2 e PostgreSQL.
- 117 Servidores de aplicação são elementos da gerência de configuração de um ambiente corporativo, em virtude de serem diretamente associados à arquitetura de aplicações com base em tecnologia *web*. Entretanto, a versão do *software* servidor de aplicação usado não consiste em informação comumente coletada no banco de dados de gerência de configuração, pois esses sistemas desempenham o mesmo papel arquitetural.

A seguir, apresenta-se trecho de uma política de *backup* de dados corporativa.

- Dados armazenados no SGBD corporativo: *backup* incremental diário (segunda a sexta-feira) e dados do *backup* localizados *on-site*; *backup* completo semanal (sábado) e dados do *backup* localizados *off-site*.
- Caixas de correio eletrônico (*exchange*): *backup* completo diário (segunda a sexta-feira) e dados do *backup* localizados *on-site*; *backup* completo semanal (sábado) e dados do *backup* localizados *off-site*.
- Imagens de máquinas virtuais: *backup* completo (todas as terças e quintas-feiras) e dados localizados *on-site*.

Com base nessa política, julgue os itens a seguir.

- 118 Uma política adequada de *backup* deve explicitar o suporte que será utilizado e o procedimento que será adotado para a guarda das mídias usadas no *backup* e para o seu transporte de *on-site* para *off-site*. Essas informações, contudo, não estão explícitas no trecho da política em questão.
- 119 *Backups* realizados com base na referida política não podem ser usados, como estratégia de recuperação de desastres, em eventos que comprometam totalmente os recursos do sítio de processamento.
- 120 Em face das informações acima, é correto afirmar que a periodicidade do *backup* de imagens de máquinas virtuais é inadequada, pois essas são normalmente alteradas diariamente.