

DEI-ISEP	Administração de Sistemas Informáticos – Exame de Época Especial	Data: 2010/09/06 Pág. 1/4
----------	---	------------------------------

Número: _____ Nome: _____

A duração máxima do teste é de 35 minutos.

I

Em cada um dos grupos seguintes assinale as afirmações verdadeiras (V) e falsas (F). São consideradas correctas as respostas “V” às afirmações verdadeiras e “F” às afirmações falsas. Duas opções erradas anulam uma opção correcta.

As funções de um Administrador de sistemas num Centro de Processamento de Dados incluem:

- ☐ Planeamento de respostas a falhas de serviços e problemas do sistema informático
- ☐ Coordenação das operações correntes dos sistemas (salvaguardas de dados, actualizações, comunicações ...)
- ☐ A responsabilidade pela elaboração de um Plano de Continuidade de Negócio da Empresa
- ☐ Supervisão e treino de operadores de sistemas

Para a redução dos custos de operação num CPD a atenção de um Administrador de Sistemas deve incidir principalmente sobre:

- ☐ Os custos de energia e de arrefecimento.
- ☐ Os custos relativos a operação, gestão e administração do CPD
- ☐ Os custos relativos à aquisição de novos servidores e equipamentos.
- ☐ A consolidação de cargas de processamento através de metodologias de virtualização

O conceito de “Continuidade de Negócio” numa empresa:

- ☐ Significa que devem ser sempre escolhidas metodologias que garantam valores de RTO de poucos minutos, no planeamento de processos de recuperação em caso de desastre.
- ☐ Implica a utilização de metodologias de replicação em tempo real para os servidores de aplicações e bases de dados críticas.
- ☐ Implica uma definição dos valores de RTO e RPO considerados adequados pelos órgãos de gestão da empresa.
- ☐ Refere-se à capacidade de uma organização recuperar de um desastre e/ou de um e pelos órgãos de gestão da empresa vento imprevisto, reiniciando e continuando as operações de negócio.
- ☐ Inclui o conceito de alta disponibilidade através da utilização de infra-estruturas de rede resistentes e tolerantes a falhas.

Uma política de segurança de uma empresa ...

- ☐ Deve fornecer um enquadramento para a implementação dos mecanismos de segurança, definir procedimentos de segurança adequados, processos de auditoria à segurança e estabelecer uma base para procedimentos legais na sequência de ataques que possa sofrer.
- ☐ Deve especificar os mecanismos de tolerância a falhas.
- ☐ Deve especificar uma infra-estrutura virtual para virtualizar um conjunto de máquinas físicas sobre rede, criando uma infra-estrutura de máquinas virtuais.
- ☐ Deve definir claramente as áreas de responsabilidade dos intervenientes das diferentes áreas de trabalho da empresa, incluindo a direcção/administração.

DEI-ISEP	Administração de Sistemas Informáticos – Exame de Época Especial	Data: 2010/09/06 Pág. 2/4
----------	---	------------------------------

Num sistema de controlo de acessos do tipo AAA ...

- ☐ As credenciais de autenticação submetidas pelo cliente ao PDP são sempre do tipo "chave partilhada" (shared-key).
- ☐ A verificação da "password" submetida pelo cliente é normalmente feita utilizando o "Password Authentication Protocol" (PAP), que nunca transmite as passwords em claro.
- ☐ A componente de contabilização da utilização de recursos tem uma importância crescente, em que por questões de segurança e de direitos de autor, a legislação é cada vez mais exigente na manutenção de registos de utilização dos recursos
- ☐ É fundamental a implementação de metodologias de monitorização da taxa de utilização de switches e placas de rede.
- ☐ Podem ser criadas metodologias de atribuição dinâmica de VLANs, em que um switch (PEP) bloqueia o acesso à rede ao utilizador, até estar concluída a autenticação. Depois configura automaticamente a porta, de acordo com a informação sobre a VLAN em que o utilizador deve ser colocado

O par chave pública/privada em criptografia assimétrica entre duas entidades A e B

- ☐ Garante a confidencialidade de uma mensagem enviada de A para B se essa mensagem for cifrada com a PrivA.
- ☐ Garante a autenticação de uma mensagem enviada de A para B se essa mensagem for cifrada com a PubB.

Considere-se que num Plano de Continuidade de Negócios de uma empresa, uma análise de impacto, para garantia de um determinado nível de continuidade de serviço definiu os seguintes índices: RTO: 6 horas; RPO: 1 hora. A empresa tem um horário de funcionamento de 2ª a 6ª, entre as 8 e as 18 horas e dispõe de um CPD alternativo.

- ☐ Uma salvaguarda total dos dados efectuada todos os dias entre as 0 e as 5 horas, com o envio diário dos suportes para o CPD alternativo, durante o horário de trabalho, para o CPD alternativo, garante o cumprimento dos dois índices.
- ☐ Uma replicação "on-line" das transacções permite cumprir os dois índices.
- ☐ Uma metodologia que implemente uma replicação dos dados alterados, para o CPD alternativo, de hora em hora, durante o horário de trabalho, garante o cumprimento dos dois índices

DEI-ISEP	Administração de Sistemas Informáticos – Exame de Época Especial	Data: 2010/09/06 Pág. 3/4
----------	---	------------------------------

II

Classifique de verdadeiras (V) ou falsas (F) as seguintes afirmações. Uma opção mal assinalada sofre um desconto adicional de meia opção correcta

1. As SANs são normalmente construídas sobre uma infra-estrutura especialmente concebida para manipular comunicações de storage_____
2. O LDAP resulta de um protocolo mais complexo especificado na norma X.500/ISO para acesso a directórios X500, onde é possível armazenar informação relativa a diversos tipos de objectos (pessoas, organizações, serviços, etc.), que pode ser partilhada por múltiplas aplicações _____
3. O RADIUS permite que dispositivos sem suporte LDAP (switches, routers, ...), possam ter acesso ao repositório de credenciais de autorização. _____
4. A criptografia de chaves publicas baseia-se na utilização de uma chave partilhada entre o emissor e o receptor e num algoritmo de encriptação como o DES ou o 3DES_____
5. A implementação do algoritmo MD5 garante protecção contra ataques do tipo “negação de serviço”_____
6. Para garantir a confidencialidade numa comunicação de dados sobre IPsec deve ser implementada uma associação de segurança AH_____
7. A definição de uma politica de Segurança Informática numa organização deve incluir a especificação de uma linha de defesa contra intrusão, que inclua múltiplos “firewalls”..... _____
8. As assinaturas digitais mais usadas actualmente aplicam criptografia de chave pública_____
9. Numa SAN com o protocolo iSCSI é possível a utilização da infra-estrutura de rede IP existente, incluindo switches, routers e adaptadores de rede_____
10. Num planeamento de um processo de continuidade de negócio o “Recovery Time Objective” (RTO) associado aos diferentes processos de negócio de uma empresa, é estabelecido durante a fase de análise do impacto de uma ruptura de continuidade no negócio e depois apresentado ao administrador de sistemas informáticos para aceitação_____
11. O “Recovery Point Objective” (RPO) define o intervalo de tempo necessário para restaurar os dados de um backup_____
12. O WRED (Weight Random Early Detection) Cria processos de sinalização entre aplicações e a rede para garantir níveis de largura de banda através da rede_____
13. O Pode-se definir “precedência IP” como um protocolo usado para definir o numero de filas numa interface de output para a definição do QoS. ... _____

DEI-ISEP	Administração de Sistemas Informáticos – Exame de Época Especial	Data: 2010/09/06 Pág. 4/4
----------	---	------------------------------

14. Um objectivo importante da monitorização de recursos de rede consiste em proporcionar informação sobre problemas em processos críticos da rede ou infra-estrutura informática _____
15. Uma correcta gestão de falhas sobre uma rede informática deve detectar e registar as falhas ocorridas e notificar os operadores de forma a que as falhas possam ser rapidamente resolvidas e que a rede continue em operação _____
16. Algumas considerações importantes para a definição de uma correcta política de segurança são:
- 16.1 Ter em conta os factores humanos _____
 - 16.2 Limitar o âmbito de acessos _____
 - 16.3 Ter apenas em conta os acessos via rede informática _____
 - 16.4 Não esquecer a segurança física _____
 - 16.5 Conhecer os pontos fracos _____
 - 16.6 Cifrar toda a informação que passa sobre a rede _____
17. A redução de custos importante que pode ser obtida em implementações SANs iSCSI tem a ver com a utilização de uma infra-estrutura standard com switches Gigabit Ethernet e routers IP. _____
18. Um TCP Offload Engine, ou "TOE Card", oferece uma alternativa a um HBA iSCSI. Um TOE descarrega as operações TCP/IP, relativas a esta interface de rede, do processador do host, libertando os ciclos de CPU para o processamento das principais aplicações correr no host. _____
19. Num processo de continuidade de negócio deve ser avaliado logo de início se os switches de backbone são redundantes _____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto
Administração de Sistemas – 2009/2010
Exame de Época de Setembro – 06/09/2010 – Prática – 2ª Parte

Número: _____ Nome: _____

Prova a realizar sem recurso a consulta. Duração: 30 minutos.

Classifique cada afirmação como verdadeira (V) ou falsa (F)

Cada resposta errada desconta meia resposta certa.

Bom trabalho.

Administração de servidores Linux

1. A tabela de partições é definida pelo fabricante do disco, nunca podendo ser alterada ____
2. Num sistema Linux o acesso a uma partição é conseguido através de uma letra de drive ____
3. A partição raiz de um sistema Linux nunca pode ser do tipo SWAP..... ____
4. As partições do disco “/dev/sdc” são identificadas por nomes começados por “/dev/sdc” ____
5. Ao contrário dos sistemas de ficheiros XFS e Reiser FS, o EXT3 é do tipo “journaling”..... ____
6. A partição SWAP deve ter capacidade igual ou superior à da partição raiz ____
7. Não é possível definir cotas diferentes em duas partições do mesmo disco ____
8. As “homes” de todos os utilizadores devem residir sempre na partição raiz ____
9. Cada utilizador pode ter um programa inicial diferente (“Shell”) ____
10. Os grupos primários nunca existem no ficheiro **/etc/group** ____
11. O comando “**usermod**” permite gerir utilizadores definidos em repositórios remotos ____
12. O ficheiro “/etc/shadow” permite manter secretos os “digest” das “passwords” ____
13. O grupo primário de um utilizador tem sempre um nome igual ao do utilizador ____
14. NIS (“Network Information Service”) é o mesmo que NSS (“Name Service Switch”) ____
15. Os utilizadores definidos em “/etc/passwd” são sempre considerados em primeiro lugar ____
16. Numa cadeia PAM se um módulo “required” falha, a cadeia vai sempre resultar em falha.... ____
17. A cadeia PAM “password” serve para autenticar utilizadores ____
18. O ficheiro “/etc/nsswitch.conf” não afecta directamente o funcionamento do PAM ____
19. As permissões 0722 são apropriadas para uma “Home Directory” ____
20. A pasta “/etc/skel/” deve ter permissões de escrita para todos os utilizadores..... ____
21. O comando “umask” serve para alterar as permissões de ficheiros existentes ____
22. Os ficheiros de arranque da shell residentes na pasta “/etc/” são os últimos a ser executados ____

23. As variáveis de ambiente são sempre propagadas aos processos filhos criados ____
24. Em partições onde os utilizadores não podem escrever, a definição de cotas é importante ____
25. O comando “quotaoff” deve ser aplicado antes de se usar o comando “quotacheck” ____
26. O comando “setquota” é a única forma de definir as cotas de um utilizador ____
27. O comando “route” não permite definir o “default route” (“default gateway”) ____
28. O comando “ip”, entre outras funcionalidades, substitui os comandos “ifconfig” e “route” .. ____
29. O comando “vconfig add eth1 200” cria uma interface de rede identificada por “eth1.200” .. ____
30. Os servidores DHCP só respondem a clientes que utilizem um sistema operativo igual ____
31. O “Internet Daemon” (inetd/xinetd) não é adequado para serviços muito solicitados ____
32. No IPTABLES, quando não há “match” com nenhuma regra, o acesso é sempre negado ____
33. O IPTABLES não permite definir regras com base no endereço de origem, apenas destino . ____
34. O tipo de script e interpretador a usar é identificado através do nome do ficheiro ____
35. A criptografia simétrica assegura automaticamente a autenticidade dos intervenientes ____
36. O “System Logger” (syslog) é o responsável pela gestão dos ficheiros “lastlog” e “wtmp” .. ____
37. O ficheiro “lastlog” deve ser consultado através do comando “lastlog” ____
38. Num sistema de cópias incrementais, deve realizar-se periodicamente uma cópia integral ... ____

Administração de servidores Windows

1. O RAID1 utiliza um mecanismo conhecido como mirror..... ____
2. O WS2008 em modo Server Core não tem suporte a virtualização. ____
3. O Hyper V no WS2008 apenas suporta virtualização de máquinas Windows..... ____
4. O WS2008 permite executar aplicações remotas sem trazer todo ambiente de trabalho ____
5. O sistema de ficheiros FAT32 usa clusters mínimos de 32Kb. ____
6. O Active Directory obedece a determinadas regras, sendo estas denominadas de Catalog ____
7. No Active Directory um site é um conjunto de controladores de domínio. ____
8. No Servidor de DNS um registo do tipo A contém informação acerca de um host. ____
9. Os servidores de DHCP no WS2008 funcionam em modo stateless..... ____
10. Com os “default password requirements” activos as passwords tem no mínimo 8 caracteres. ____
11. A pasta SYSVOL armazena os ficheiros públicos do domínio. ____

Duas respostas erradas anulam uma resposta certa

Duração: 30 minutos

6 de Setembro de 2010

Número: _____

Nome: _____

1. As mensagens ICMP Redirect são enviadas apenas por um computador..... _____
2. O EIGRP calcula o melhor caminho para um destino aplicando o algoritmo de Dijkstra..... _____
3. O processo de descoberta/recuperação de vizinhos no EIGRP emprega mensagens que não provocam uma grande ocupação da largura de banda _____
4. O OSPF propaga apenas as alterações à topologia _____
5. Se nada for programado em contrário, o OSPF faz a auto-agregação das tabelas _____
6. O OSPF associa um custo (peso) a cada caminho que pode ser alterado pelo administrador..... _____
7. Um inconveniente do OSPF é que o *flooding* é propagado a todas as AS's..... _____
8. Na configuração do OSPF é necessário definir, num primeiro nível, a Área e dentro desta a *Autonomous System*..... _____
9. O OSPF só envia LSA's quando detecta uma alteração à topologia, o que implica que todos os encaminhadores com OSPF que estão na mesma área os enviam também..... _____
10. Uma desvantagem do encaminhamento dinâmico é a alta ocupação da largura de banda _____
11. Nas opções do **route-map** é possível determinar os critérios (*set*) e as acções (*match*) a efectuar..... _____
12. Para filtrar o tráfego entre várias redes podem ser usadas ACL's *standard* que filtram pacotes e protocolos..... _____
13. Uma ACL só pode ser aplicada como *inbound* ou *outbound*, nunca nos dois em simultâneo _____
14. Para especificar todos os hosts de uma rede IP classe C com 27 *network bits* numa ACL, o *wildcard* a indicar é 0.0.0.31 _____
15. Um pacote é descartado após o processamento de todas as regras de uma *crypto* ACL no caso de nenhuma delas ter sido satisfeita..... _____
16. As ACL's configuradas num dispositivo ficam de imediato aplicadas a todas as interfaces activas do mesmo _____
17. Se para um dispositivo pretendermos permitir qualquer tipo de tráfego num dado interface, devemos aplicar-lhe uma ACL com essa indicação..... _____
18. O único critério usado para testar um pacote numa ACL *extended* é o endereço destino..... _____
19. Se um pacote não fizer o *match* com nenhuma regra de uma ACL é enviado pelo dispositivo para o *default route* _____
20. Caso exista, a regra do *default route* numa tabela estática tem que ser obrigatoriamente a última _____

21. Se uma ACL contiver apenas a linha **access-list 10 deny host 196.27.12.8** e for aplicada no sentido *outbound* significa que apenas ao host com o endereço IP indicado é negado o envio de pacotes _____
22. A aplicação *outbound* de uma ACL a uma interface implica a análise de todo o tráfego que sai por esse interface _____
23. Numa tabela NAT dinâmica, todos os endereços internos são automaticamente incluídos na tabela mesmo que não acedam ao exterior _____
24. A segurança informática pode ser classificada em quatro grandes grupos: Autenticidade, Integridade, Confidencialidade e Privacidade..... _____
25. A autenticidade versa a confiança na exactidão e fiabilidade do sistema _____
26. A autenticidade pode ser obtida por um processo de autenticação do utilizador _____
27. O NAT pode ser aplicado para balanceamento de carga, aplicando-se-lhe um princípio de round-robin ou de maior capacidade individual de cada sistema _____
28. O algoritmo Round Robin do NAT tem em atenção a capacidade de cada servidor interno _____
29. A criptografia unidireccional é utilizada para cifrar mensagens que circulam entre dois sistemas _____
30. O algoritmo DES tem uma chave de 56 bits se excluirmos os de paridade..... _____
31. O sistema Kerberos contém obrigatoriamente um TGS e pode conter um AS..... _____
32. Uma associação de segurança IPsec só pode ser limitada numa base de volume transferido _____
33. A diferença entre o AH e o ESP é que o segundo verifica a integridade e confidencialidade da mensagem _____
34. A aplicação de métodos criptográficos a um grande volume de informação é eficiente se for em modo contínuo _____
35. O BGP é um protocolo *classfull*..... _____
36. Uma DMZ é sempre a zona mais acessível pelo exterior da rede..... _____
37. O IPsec tem dois modos de funcionamento e dois protocolos de segurança, só se podendo aplicar um modo e um protocolo em cada momento..... _____
38. Se a ACL **access-list 101 permit ip 194.27.16.20 0.0.0.5 any** endereçar redes *classfull* da classe C, os sistemas internos abrangidos por ela são 4 (quatro), um dos quais é o que tem o endereço IP 194.27.16.23 _____
39. Podemos ter IPsec sem IKE, mas o inverso não é verdade _____