Instituto Superior de Engenharia do Porto – Licenciatura em Engenharia Informática – Administração de Sistemas (ASIST) – 2018/2019

Exame Final – Época Normal – 16 de janeiro de 2019 – 14:30

Prova a realizar sem recurso a consulta ou calculadora – Duração: 90 minutos

Número: _____ **Nome:** _____

1ª Parte (60%) – Para cada uma das afirmações assinale com: **V** – caso a considere **totalmente verdadeira** ou **F** – caso a considere **total ou parcialmente falsa**
Se quiser anular uma resposta, rasure a mesma. Caso queira responder de novo coloque a resposta após a resposta anulada. **Se não tiver a certeza não responda, uma resposta errada anula meia resposta certa.**

1. O administrador de sistemas é responsável pela validação das cópias de segurança, mesmo que não seja ele a efetuá-las V
2. Apesar da virtualização de *hardware* diminuir os custos sistemas, os custos de operação e complexidade mantém-se ..... F
3. Uma SAN FCIP é diretamente compatível com outra SAN iFCP ..... F
4. Em termos de RTO, há vantagem do *mirroring* síncrono face ao assíncrono ..... F
5. O SLA (*Service Level Agreement*) define os critérios de segurança dos sistemas V
6. A probabilidade de falha pode ser nula caso se recorra à redundância V
7. Com redundância o MTBF (*Mean Time Between Failures*) pode ser igual ao MTTF (*Mean Time To Fail*) V
8. Um sistema Fail Soft é aquele onde a degradação do SLA é prolongada mas não significativa ..... F
9. Se um sistema for alimentado por uma UPS, é sempre *Fault Tolerant* ..... F
10. O sistema RAID pode conter um SPOF (*Single Point Of Failure*) V
11. Em termos de RPO (*Recovery Point Objective*) a estratégia de cópia diferencial é igual à incremental ..... F
12. Em termos de RTO (*Recovery Time Objective*) a estratégia de cópia diferencial é igual à incremental V
13. Para garantir a confidencialidade pode-se utilizar criptografia irreversível ..... F
14. Uma vantagem da criptografia simétrica é garantir a autenticidade do emissor, mas complica a troca de segredos ..... F
15. A criptografia assimétrica nunca é periódica ..... F
16. Para a segurança dos dados, é suficiente que a sua comunicação entre sistemas seja criptografada ..... F
17. Um sistema AAA (*Authentication, Authorization, Accounting*) contém obrigatoriamente quatro constituintes V
18. O PDP (*Policy Decision Point*) pode coexistir com o PIP (*Policy Information Point*) num sistema RADIUS ..... F
19. Face ao RGPD (*Regulamento Geral de Proteção de Dados*) um sistema AAA é suficiente V
20. Num sistema LDAP (*Lightweight Directory Access Protocol*) um objeto pode pertencer a várias classes estruturais ..... F
21. Num sistema LDAP (*Lightweight Directory Access Protocol*) um objeto pode pertencer a várias classes auxiliares V
22. No LDAP um DN (*Distinguished Name*) é único mas um RDN (*Relative Distinguished Name*) pode ser repetido V
23. O Kerberos trabalha apenas com chaves cifras assimétricas ..... F
24. Como constituintes do Kerberos temos o AS (*Authentication Server*) e o TGS (*Ticket Granting Service*) V
25. O TGS (*Ticket Granting Service*) não necessita possuir uma chave partilhada com o AS (*Authentication Server*) ..... F
26. A primeira mensagem numa comunicação Kerberos é sempre não encriptada ..... F
27. No Kerberos pode haver uma relação de um KDC (*Kerberos Distribution Center*) para mais do que um *realm* ..... F
28. Para que um *principal* possa utilizar serviços de outro *realm*, necessita sempre de se autenticar nele ..... F
29. Um *realm* Kerberos possui sempre um SPOF (*Single Point Of Failure*) V
30. Caso a segurança seja mais importante que o desempenho, um *firewall Packet Filter* é preferível ao *Stateful* ..... F
31. Uma DMZ pode ser definida como a zona de acesso exclusivamente externo da rede V
32. A utilização de VLAN (*Virtual LAN*) impossibilita o *sniffing* ..... F
33. Um *firewall Packet Filter* permite bloquear ataques à disponibilidade ..... F
34. É responsabilidade do Administrador de Sistemas dificultar os ataques *IP Spoofing* criando regras que inibam a chegada de pacotes com endereços de origem iguais aos internos, mas para os pacotes que saem da rede não é importante ..... F
35. O *Man-In-The-Middle* usurpando a identidade do servidor DNS só é possível se o atacante estiver na rede interna ..... F
36. Na configuração de uma VPN (*Virtual Private Network*) o MTU (*Maximum Transmission Unit*) da ligação física é indiferente .... F
37. Para garantir o uso do PMTUD (*Path MTU Discovery*) torna-se necessária a existência de regras adicionais na *firewall* .... F
38. O modo **tunnel** do IPsec é mais vantajoso do que o modo **transport** se a desempenho é importante ..... F
39. Não é possível usar apenas o ESP (*Encapsulating Security Payload*) e garantir apenas a autenticidade e integridade V

40. Uma ligação IPsec com AH (*Authentication Header*) e ESP (*Encapsulating Security Payload*) obriga à criação de quatro SA (*Security Association*) V

41. Uma ligação IPsec com IKE (*Internet Key Exchange*) obriga à criação de duas SA (*Security Association*) ..... F

42. O tempo de vida do TLS *Handshake Protocol* é sempre esgotado antes de novos mecanismos de cifra serem negociados.. F

43. O *overhead* de uma comunicação diminui se a diferença **(informação total transmitida – informação útil)** aumenta …… F

44. O LFI (*Link Fragmentation and Interleaving*) possibilita que os pacotes de maior prioridade não sejam afetados pelos pacotes de menor prioridade em ligações de baixo débito V

45. O TCP implementa um controlo de congestionamento baseado no RTO (*Retransmission Time Out*) e no RTT (*Rount-Trip Time*) V

46. No protocolo da janela deslizante, o tamanho da janela inicial é definido pelo recetor, mas depois é o emissor que o define .... F

47. O RED (*Random Early Detection*) só descarta pacotes de baixa prioridade ..... F

48. A marcação dos bits de prioridade ocorre apenas e só no nó de origem, nunca no percurso ..... F

49. Em qualquer implementação de *Soft QoS* o número de filas de saída é sempre fixo ..... F

50. O *Hard QoS* é preferível ao *Soft QoS* se há um tipo de tráfego prioritário V

2ª Parte (40%) – **Para cada questão responda apenas no espaço disponível. Respostas fora desse espaço serão ignoradas.**

1. **Indique e justifique três funções do administrador de sistemas** (**10%**)

- Gerenciamento de recursos: o administrador de sistemas é responsável por garantir que os recursos do sistema, como CPU, memória, armazenamento e rede, estão a funcionar corretamente e estão disponíveis para os utilizadores.

- Segurança: o administrador de sistemas é responsável por garantir que os dados e informações armazenadas no sistema estão seguras e protegidas contra ameaças externas, como ataques cibernéticos.

- Suporte técnico: o administrador de sistemas é responsável por fornecer suporte técnico aos utilizadores do sistema, resolvendo problemas e garantindo que o sistema está a funcionar corretamente. Isso inclui solucionar problemas de hardware e software, instalar atualizações e corrigir bugs.

2. Explique a influência do RPO (*Recovery Point Objective*) e do RTO (*Recovery Time Objective*) no BCP (*BusinessContinuity Plan*) (10%)

O RPO (Recovery Point Objective) é o ponto de recuperação desejado para um sistema ou processo em caso de desastre. Determina a quantidade de dados ou informações que podem ser perdidos sem prejudicar significativamente o negócio. Por exemplo, se o RPO é de 24 horas, significa que BCP deve garantir a recuperação dos dados até 24 horas antes da falha.

Já o RTO (Recovery Time Objective) é o tempo máximo esperado para recuperar um sistema ou processo após uma falha. Determina quanto tempo o negócio pode ficar sem acesso a um determinado sistema ou processo antes que isso cause danos significativos. Por exemplo, se o RTO é de 8 horas, significa que o BCP deve garantir que o sistema ou processo esteja a funcionar novamente em até 8 horas após a falha.

Ambos, RPO e RTO, são importantes para o BCP (Business Continuity Plan), pois ajudam a identificar os requisitos de recuperação e a estabelecer metas realistas para a recuperação dos sistemas e processos críticos em caso de desastre. Ao definir RPO e RTO, é possível estabelecer uma estratégia de recuperação de desastres e implementar medidas para garantir a continuidade dos negócios.

3. Explique a diferença entre o DRP (*Disaster Recovery Plan*) e o Plano de Contingência (10%)

O Disaster Recovery Plan (DRP) é um plano de recuperação de desastres que descreve as ações a serem tomadas para recuperar rapidamente os sistemas e dados críticos de uma empresa após um desastre. Geralmente inclui procedimentos detalhados para a recuperação de hardware, software, dados e comunicações.

Já o Plano de Contingência é um plano geral que descreve as ações a serem tomadas em caso de emergência. Pode incluir medidas para lidar com desastres naturais, falhas de sistemas, interrupções de negócios e outros eventos inesperados. Geralmente inclui procedimentos de comunicação,designação de responsabilidades e outras medidas para garantir a continuidade dos negócios.

Em resumo, o DRP é uma parte específica do Plano de Contingência, onde é descrito como recuperar os sistemas e dados críticos de uma empresa após um desastre, enquanto o Plano de Contingência é um plano geral que abrange todos os aspectos de contingência de uma empresa.

4. **Explique as diferenças entre o *Custom Queuing* e o *Fair Queuing*, indicando para cada um deles uma situação práticaem que seja aconselhada a utilização dessa técnica (10%)**

Custom Queuing e Fair Queuing são técnicas de gerenciamento de fluxo de rede que visam garantir uma distribuição justa e eficiente dos recursos de rede.

Custom Queuing (CQ) é uma técnica que permite aos administradores de rede criar regras específicas para classificar e priorizar pacotes de acordo com critérios pré-definidos. Isso permite que os administradores de rede possam garantir que certos tipos de tráfego, como voz e vídeo, tenham prioridade sobre outros tipos de tráfego, como dados. Uma situação em que a utilização do CQ seria aconselhada seria em uma rede corporativa onde é importante garantir que aplicativos críticos, como sistemas de telefonia, tenham prioridade sobre outros tipos de tráfego de rede.

Fair Queuing (FQ) é uma técnica que divide o tráfego em fluxos e garante que cada fluxo receba um número igual de pacotes em um determinado período de tempo. Isso garante que nenhum fluxo receba mais recursos do que outro e evita a sobrecarga de certos fluxos. Uma situação em que a utilização do FQ seria aconselhada seria em uma rede de provedor de serviços onde é importante garantir que todos os clientes tenham acesso igualitário aos recursos de rede.