1. As políticas de segurança:
    a. **Definem requisitos e regras para a proteção dos recursos de uma organização.**
    b. São constituídas pelas leis que definem o âmbito do crime informático
    c. São uma coisa de políticos e polícias. Que não tem nada a ver com segurança e redes e sistemas informáticos
    d. São as tecnologias que permitem implementar um determinado objetivo de segurança

2. O conceito de domínio de segurança:
    a. Agrega pessoas com conhecimento ou tarefas semelhantes
    b. Refere-se a um conjunto de políticas
    c. Refere-se a um conjunto de controlos
    d. **É útil para gerir a segurança de forma agregada**

3. Numa perspetiva de segurança, considera-se que os utilizadores comuns:
    a. Investem continuamente na estratégia de segurança dos seus sistemas
    b. São capazes de calcular o risco das suas atividades informáticas
    c. São recetivos a implementar políticas rígidas de segurança da informação
    d. Necessitam de formação específica na área da segurança informática

4. Identifique umas das principais fontes de vulnerabilidades:
    a. Comunicações Internas
    b. CVEs
    c. Erros de hardware
    d. Usuários

5. Qual das seguintes afirmações é verdadeira?
    a. O uso de criptografia garante a segurança de um sistema
    b. Um ataque do dia zero explora vulnerabilidades descobertas hoje
    c. O custo da segurança aplicada deve ser superior ao impacto de um ataque
    d. A defesa contra ataques passa em grande medida pela eliminação de vulnerabilidades

6. Identifique uma das principais fontes de vulnerabilidades em sistemas informáticos:
    a. Comunicações não controladas
    b. Comunicações conhecidas
    c. Administradores
    d. Fornecedores

7. A gestão de vulnerabilidades de uma aplicação, efetuada pelo seu autor:
    a. Não é realizada de forma privada
    b. Existe durante todo o ciclo de vida da aplicação
    c. Diz respeito aos comportamentos dos utilizadores
    d. Apenas se aplica a aplicações críticas

8. Identifique uma das dimensões principais a considerar numa estratégia de segurança:
    a. As pessoas
    b. O treino
    c. As vulnerabilidades
    d. As políticas

9. Em relação à faceta ofensiva da segurança, assinale a correta:
    a. Diz respeito ao software, mas não aos processos
    b. Consiste em ofender pessoas
    c. É de evitar, pois corresponde a atividades ilegais
    d. É usada pelos cibercriminosos

10. O OWASP Top 10 consiste:
    a. Nas 10 vulnerabilidades mais populares em sistemas atuais
    b. Nas 10 vulnerabilidades mais importantes para o desenvolvimento de sistemas
    c. Nos 10 mecanismos mais relevantes a implementar
    d. Nas 10 fontes de vulnerabilidades mais populares em sistemas atuais

11. Que medidas endereçam maioritariamente vulnerabilidades conhecidas?
    a. Reconhecimento
    b. Legais
    c. Ataque
    d. Ilusão

12. Um ataque Meet-in-the-Middle:
    a. Permite intercetar a negociação de chaves com Diffie-Hellman
    b. Permite encontrar a chave numa cifra dupla com dificuldade inferior à esperada
    c. Aplica-se a algoritmos que usem EDE com K1=K2 ou K2=K3
    d. É um ataque de roubo de chaves assimétricas

13. Uma cifra híbrida consiste em:
    a. Um mecanismo para aumento de performance no uso prático de chaves assimétricas
    b. Cifrar um texto com uma chave assimétrica aleatória, que é cifrada com a chave pública do destinatário
    c. Utilizar uma qualquer combinação de algoritmos de cifra
    d. Realizar uma cifra com controlo de integridade

14. Qual é a abordagem das "Jóias da Coroa" em segurança da informação?
    a. É uma estratégia de publicar a coleção de joias mais valiosa da organização utilizando medidas de segurança cibernética
    b. É um método para proteger moedas digitais contra ataques cibernéticos
    c. Ela concentra-se na salvaguarda dos principais ativos que são essenciais para a operação de uma organização
    d. É um termo usado no Centro de Operações de Segurança (Security Operations Center, SOC) para descrever incidentes com classificação de alto valor

15. No contexto das cifras, uma Substitution Box:
    a. **Aplica o conceito da confusão**
    b. Deve ser evitada na construção de algoritmos seguros
    c. Deve manter bits de controlo que permitam reverter (decifrar) a mensagem
    d. Deve ser usada apenas uma vez em cada cifra

16. O conceito de confusão, indicado por Shannon, significa
    a. **Que existe uma relação complexa entre a saída do algoritmo e as suas entradas**
    b. Que não é possível perceber o algoritmo porque o mesmo não está completamente descrito
    c. Que o algoritmo tem partes obscuras
    d. Que o resultado de um algoritmo não depende dos dados de entrada

17. Qual das cifras seguintes não existe:
    a. Cifras contínuas simétricas
    b. **Cifras contínuas assimétricas**
    c. Cifras por bloco assimétricas
    d. Cifras de Vernam

18. Qual dos seguintes modos de cifra não permite um acesso aleatório uniforme na decifra? (considere que não há pré- computação)
    a. **ECB (Electronic Code Book)**
    b. GCM (Galois/Counter Mode)
    c. CFB (Cipher FeedBack)
    d. OFB (Output FeedBack)

19. Qual dos seguintes modos de cifra não cria uma cifra contínua (stream) a partir de um algoritmo de cifra por blocos?
    a. OFB (Output FeedBack)
    b. **ECB (Electronic Code Book)**
    c. CFB (Cipher FeedBack)
    d. GCM (Galois/Counter Mode)

20. Para enviar uma mensagem confidencial a um destinatário, usando criptografia assimétrica, o remetente deve:
    a. Cifrar a mensagem usando cifra híbrida com uma chave simétrica aleatória e a chave privada do destinatário
    b. Cifrar a mensagem usando uma cifra contínua ou por blocos com a chave pública do destinatário
    c. **Cifrar a mensagem usando uma síntese da sua (remetente/originador) chave pública**
    d. Cifrar a mensagem usando cifra híbrida com uma chave simétrica aleatória e a chave pública do destinatário

21. Para enviar uma mensagem confidencial a um destinatário, usando criptografia assimétrica, o remetente deve:
    a. Cifrar a mensagem usando uma síntese da sua (remetente/originador) chave privada
    b. Cifrar a mensagem usando a chave privada do destinatário
    c. Cifrar a mensagem usando uma síntese da sua (remetente/originador) chave pública
    d. Cifrar a mensagem usando a chave pública do destinatário

22. O mecanismo de negociação de chaves Diffie-Hellman
    a. É robusto contra atacantes ativos
    b. É vulnerável a ataques de Man In the Middle
    c. Implementa um mecanismo de cifra híbrida
    d. É vulnerável a ataques de dicionário

23. Uma cifra assimétrica:
    a. Tipicamente possui blocos de 32 bytes
    b. Faz uso de pares de chaves
    c. É tipicamente mais rápida que uma cifra simétrica
    d. Suporta vários modos de cifra com feedback

24. Qual dos seguintes modos de cifra não permite paralelizar a decifra?
    a. ECB
    b. OFB
    c. CBC
    d. GCM

25. Qual dos seguintes modos de cifra permite paralelizar a decifra?
    a. CFB
    b. GCM
    c. CBC
    d. CTR

```
permite paralelização
- ECB
- CTR

pode ou não permitir
- GCM
- OFB

não permite paralelização
- CBC
- CFB
```

26. Quando se usa cifra tripla é normal usar o modo EDE (Encrypt, Decrypt and Encrypt). Porquê?
    a. Porque permite que decifra possa anular uma cifra, resultando numa única cifra simples
    b. Porque caso se usasse 3 cifras seria mais simples descobrir as 3 chaves
    c. Porque aumenta a robustez da cifra, sem impacto de performance
    d. Porque usar uma decifra entre cifras aumenta muito a confusão do processo de cifra

27. As técnicas de branqueamento em cifras:
    a. Aumentam a difusão de uma cifra
    b. Aplicam chaves ao texto e/ou criptograma com XOR
    c. Anonimizam os dados depois de decifrados
    d. Removem a maioria dos padrões do texto, mesmo usando uma chave fixa

28. Ao utilizar o mecanismo PBKFD2, que informação deve ser privada?
    a. A dimensão do resultado
    b. A senha
    c. O Pseudo Random Generator
    d. O tamanho dos blocos

29. Os mecanismos de derivação de chaves, como o PBKDF2, são importantes para:
    a. Reduzir o custo da utilização de cifras por blocos
    b. Aumentar a performance dos sistemas de autenticação
    c. Reduzir o universo de pesquisa da passe
    d. Aumentar o custo de ataques por força bruta

30. Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é verdadeira?
    a. Essa propriedade não é relevante para a robustez dos processos de criação e validação de assinaturas digitais
    b. Se for reduzida, representa um risco caso a função seja usada num MIC
    c. É definida apenas pela dimensão do resultado da função, de acordo com o paradoxo do aniversário
    d. Se for reduzida, uma entidade terceira poderá produzir um texto alternativo compatível com a assinatura de outro texto

31. No cálculo de um MAC, qual dos seguintes tipos de funções é normalmente usado?
    a. Funções de cifra com excipiente
    b. Cifras simétricas contínuas
    c. Cifras simétricas por bloco
    d. Cifras de Vernam

32. Uma assinatura digital de uma mensagem:
    a. Permite que terceiros verifiquem a identidade de quem a envia numa rede
    b. Impede que o recetor aceite uma mensagem adulterada depois de assinada
    c. Garante a identidade de quem a envia numa rede
    d. Garante a identidade de quem a recebe

33. Uma assinatura digital de uma mensagem:
    a. Garante a identidade de quem a envia numa rede
    b. Tipicamente será maior do que um MAC (Message Authentication Code) da mesma
    c. Permite que terceiros verifiquem a identidade de quem a envia numa rede
    d. Não tem qualquer vantagem em relação a uma autenticação com um MAC (Message Authentication Code)

34. Um dos objetivos das assinaturas digitais é o não-repúdio, que consiste em:
    a. Impedir a negação da criação de uma assinatura digital
    b. Impedir o acesso não autorizado ao conteúdo das mensagens/documentos
    c. Forçar o uso de smartcards na geração de assinaturas
    d. Impedir que uma entidade negue a autoria de um documento de texto

35. Para se verificar uma assinatura digital de um documento é preciso:
    a. A chave pública do verificador
    b. A identidade do assinante
    c. A chave pública do assinante
    d. O certificado de chave pública do verificador

36. A assinatura digital de um documento:
    a. Impede que o documento possa ser compreendido por quem não estiver autorizado
    b. Pode ser copiada para outro documento desde que o assinante seja o mesmo
    c. Garante que é possível detetar qualquer adulteração do mesmo após a sua assinatura
    d. Pode, em certos casos, ser realizada com uma chave simétrica

37. Uma assinatura digital de uma mensagem usando RSA:
    a. Obriga a que cada mensagem contenha sempre o certificado de chave pública do assinante
    b. Garante a identidade de quem a recebe
    c. Não tem qualquer vantagem em relação a uma autenticação com um MAC (Message Authentication Code)
    d. Não garante a sua confidencialidade

38. Em qual dos seguintes casos é possível um utente realizar uma verificação incompleta, mas válida, de uma cadeia de certificação?
    a. Existe confiança na Entidade Certificadora (CA) raiz do caminho de certificação
    b. A validação via OCSP (Online Certificate Status Protocol) devolve indicação de que o certificado é válido
    c. Não é de todo possível
    d. O certificado de uma Entidade Certificadora (CA) intermédia foi revogado após a data do certificado por ela assinado

39. Uma Entidade Certificadora raiz é confiável porque:
    a. O software que faz a validação de uma cadeia de certificação o considera confiável
    b. Certifica muitas outras Entidades Certificadoras
    c. Ninguém certifica o seu certificado
    d. Tem um certificado autoassinado

40. Tendo em conta o período de validade de um certificado, qual destas afirmações é verdadeira?
    a. Não é uma informação obrigatória nos certificados
    b. Pode ser estendido pela respetiva Entidade Certificadora
    c. Não permite que o certificado seja usado fora desse período
    d. Serve para limitar, no tempo, o uso da correspondente chave privada

41. Tendo em conta o período de validade de um certificado, qual destas afirmações é verdadeira?
    a. Pode ser encurtado caso seja revogado
    b. Não permite que o certificado seja usado fora desse período
    c. Impede que a chave privada possa ser usada fora desse período
    d. Pode ser estendido pela respetiva Entidade Certificadora

42. Em que caso é possível um utente verificar uma cadeia de certificação, sem efetivamente verificar todos os certificados da cadeia?
    a. Não existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação
    b. Existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação
    c. O certificado não está listado na CRL (Certificate Revocation List)
    d. A data do certificado é válida

43. Em que caso é possível um utente verificar uma cadeia de certificação, sem efetivamente verificar todos os certificados da cadeia?
    a. Existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação
    b. Não existe uma Entidade Certificadora (CA) intermédia confiável no caminho de certificação
    c. Não é de todo possível. É necessário validar todos os certificados
    d. A data do certificado é válida

44. Tendo em conta o uso de CRL (Certificate Revocation List), qual destas afirmações é verdadeira?
    a. As CRL indicam a identidade dos sujeitos afetos aos certificados revogados
    b. A localização da CRL de uma Entidade Certificadora faz parte de todos os certificados que ela revogar
    c. As CRL delta incluem certificados expirados, mas as CRL base não
    d. Quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

45. Tendo em conta o uso de CRL (Certificate Revocation List), qual destas afirmações é verdadeira?
    a. As CRL delta constituem uma validação de integridade das CRL base
    b. As CRL base devem ser obtidas em conjunto com as CRL delta
    c. As CRL delta devem ser consultadas a cada acesso remoto
    d. Quando uma lista base é emitida, importa obrigatoriamente a lista delta imediatamente anterior

46. Tendo em conta o uso de CRL (Certificate Revocation List), qual destas afirmações é verdadeira?
    a. Num determinado instante só existe uma lista base e delta ativas por Entidade Certificadora
    b. As CRL delta devem ser consultadas a cada acesso remoto
    c. As CRL indicam a identidade dos sujeitos afetos aos certificados revogados
    d. As CRL delta incluem certificados expirados, mas as CRL base não

47. No funcionamento de uma PKI (Public Key Infrastruture), como se procede à criação de um certificado assinado por uma Entidade Certificadora (CA)?
    a. Envia-se um Certificate Signing Request para a CA, que devolve um certificado assinado
    b. Envia-se um certificado auto assinado para a CA. que devolve um certificado assinado pela CA
    c. Envia-se a chave pública e nome (Subject) para a CA, que devolve um certificado assinado
    d. Envia-se o par de chaves para a CA, que devolve um certificado assinado

48. Um processo de autenticação serve essencialmente para:
    a. Provar que estamos a interagir com uma entidade que possui um dado atributo, objeto, ou conhecimento
    b. Obter um atributo, objeto ou conhecimento
    c. Controlar o acesso de indivíduos
    d. Determinar as intenções de um indivíduo

49. Relativamente à autenticação com desafio e resposta:
    a. Não permite uma fácil implementação do protocolo de autenticação mútua.
    b. Não pode ser utilizada em combinação com smart-cards.
    c. Pode ser utilizada em autenticações unidirecionais.
    d. É fundamental que os desafios apresentados a uma mesma credencial nunca se repitam.

50. Relativamente à autenticação de utentes com desafio resposta e pares de chaves assimétricas:
    a. Quem se autentica deve cifrar a resposta com a chave pública do autenticador.
    b. Quem se autentica deve apresentar a sua chave privada.
    c. A utilização de certificados de chave pública pode fornecer os mecanismos de identificação de quem se autentica.
    d. A validação das credenciais obriga à pré-partilha da chave pública do autenticador.

51. Relativamente à autenticação por apresentação de senha direta memorável:
    a. O sal serve para aumentar a dimensão das senhas.
    b. É vulnerável a ataques por dicionário.
    c. Os utentes memorizam senhas complexas com facilidade.
    d. Se o administrador definir a necessidade de senhas de 256 bits aleatórias, o processo torna-se seguro.

52. Relativamente à autenticação no SSH (Secure Shell):
    a. Usa sempre segredos partilhados entre utentes e servidor.
    b. Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor.
    c. Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).
    d. É da responsabilidade do servidor SSH forçar a utilização de segredos complexos.

53. Relativamente à autenticação usando TLS (Transport Layer Security):
    a. Não protege a integridade da informação.
    b. Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS).
    c. O cliente pode escolher livremente quais as credenciais que usa na sua autenticação.
    d. É vulnerável a ataques por dicionário.

54. Relativamente à autenticação usando TLS (Transport Layer Security):
    a. É vulnerável a ataques por dicionário
    b. Usa métodos de cifra considerados inseguros
    c. O cliente pode escolher livremente quais as credenciais que usa na sua autenticação
    d. Serve para garantir a negociação de uma chave de sessão entre os interlocutores corretos

55. Relativamente à autenticação no GSM (Global System for Mobile Communications):
    a. Baseia-se no conhecimento mútuo (utente e rede) de um PIN.
    b. O desafio enviado pela rede é baseado no PIN.
    c. A função de transformação do desafio apresentado pela rede é universal e realizada pelos terminais móveis.
    d. É imune a ataques com dicionário.

56. Relativamente à autenticação de utentes com S/Key:
    a. Permite que para o mesmo utente, a mesma senha produza senhas descartáveis diferentes para sistemas diferentes.
    b. As senhas descartáveis são geradas mentalmente a partir de uma senha.
    c. Usa pares de chaves assimétricas como credenciais.
    d. É um protocolo de autenticação mútua.

57. Relativamente à autenticação biométrica de utentes:
    a. Facilita a transferência de credenciais entre utentes.
    b. É um método de autenticação ideal quando se tem muitos utentes.
    c. É um método de autenticação universal (não exclui pessoas).
    d. Pode dar origem a falsos negativos, mas estes não são perigosos.

58. Na autenticação de utentes do sistema Linux:
    a. O processo de autenticação não suporta múltiplos fatores.
    b. A senha é armazenada no disco, depois de validada pelo TPM.
    c. O administrador pode alterar o método de armazenamento das credenciais.
    d. O ficheiro /etc/shadow possui um backup do ficheiro /etc/passwd

59. Considerando a autenticação de utentes em Smartphones:
    a. O Trusted Execution Environment é um ambiente seguro implementado pelo cartão SIM.
    b. As chaves são fornecidas às aplicações pelas componentes do TEE para validação.
    c. O reconhecimento facial é considerado robusto.
    d. A exploração de canais paralelos pode ser um problema para autenticação com PIN.

60. Qual dos seguintes protocolos de autenticação é vulnerável a ataques com dicionário?
    a. TTLS.
    b. RSA SecurID.
    c. SSH.
    d. Linux (com pam_unix).

61. No Linux, relativamente ao comando sudo, qual das seguintes afirmações é falsa?
    a. É um comando que serve para concretizar elevações de privilégios pontuais, logo útil para concretizar políticas de privilégio mínimo
    b. Pode ser utilizado por qualquer utilizador para o fim a que o mesmo se destina
    c. É um comando cujo ficheiro possui o bit Set-UID ativo e cujo dono é root
    d. Permite que os comandos realizados para fins de administração sejam registados em nome de quem os executou

62. No Linux, relativamente à chamada ao sistema chroot, qual das seguintes afirmações é verdadeira?
    a. A alteração da diretoria raiz de cada processo é uma operação privilegiada, logo só está acessível ao ad- ministrador
    b. O facto de existir sempre uma diretoria, na raiz do sistema de ficheiros de um processo permite que o mesmo aceda à hierarquia acima dessa raiz
    c. A alteração da diretoria raiz de um processo tem por objetivo a restrição da visibilidade que o processo tem da hierarquia total de ficheiros do sistema
    d. Com este mecanismo os ficheiros de uma pasta tornam-se acessíveis pelo utilizador root

63. No controlo de acesso baseado em papeis (Role-Based Access Control, RBAC), a capacidade de revisão de emparelhamentos utilizador-papel não permite:
    a. **Detetar os emparelhamentos que possuem um determinado direito**
    b. Que se verifique que papeis tem um utilizador
    c. Que se verifique que utilizadores possuem um papel
    d. Que se obtenha todas as relações que existem entre utilizadores e papeis

64. Qual dos seguintes modelos de controlo de acesso controla a confidencialidade em fluxos de informação?
    a. Biba
    b. RBAC (Role-Based Access Control)
    c. DAC (Discretionary Access Control)
    d. **Bell-LaPadulla**

65. O controlo de acesso baseado em papeis (Role-Based Access Control, RBAC) (escolha a resposta errada):
    a. Associa papeis (ou funções) a sessões iniciadas por utentes
    b. **É um sistema de proteção adequado a sistemas onde é inviável proteger objetos individualmente**
    c. Associa direitos a papéis (ou funções)
    d. É um conceito equivalente à proteção por grupos

66. Em relação às cópias de segurança ao nível do sistema de ficheiros, que afirmação é correta?
    a. Permitem utilizar mecanismos de duplicação de blocos.
    b. Garantem integridade do estado de cada ficheiro.
    c. Não garantem integridade do estado global dos ficheiros.
    d. **Não garantem integridade do estado de cada ficheiro.**

67. Relativamente ao método dos backups incrementais do sistema de ficheiros, qual das afirmações é verdadeira?
    a. A adição de novos dados é feita considerando o último backup completo.
    b. A longo prazo, o carácter incremental deste método irá resultar na utilização de mais espaço do que backups completos.
    c. **A recuperação de dados é mais complexa que em outros métodos.**
    d. Permite salvaguardar versões incrementais e globalmente consistentes de bases de dados.

68. Num sistema RAID 1 com N discos, qual a situação limite, após o qual existirá perda de informação?
    a. **Avaria de N-1 discos.**
    b. Avaria de apenas um disco (qualquer).
    c. Avaria de 3 discos.
    d. Avaria de 2 discos.

69. Num sistema RAID 0 com N discos, qual a situação limite, após o qual existirá perda de informação?
    a. A avaria de qualquer disco implica sempre a perda de informação.
    b. Avaria de todos os N discos.
    c. Avaria de ambos os discos com as somas de controlo (paridade).
    d. Avaria de N-1 discos.

70. Num sistema RAID 4 com N discos, qual a situação limite, após o qual existirá perda de informação?
    a. Avaria de todos os N discos.
    b. Avaria do disco que contém as somas de controlo e um outro qualquer.
    c. Avaria de qualquer disco, exceto o que contém as somas de controlo (paridade).
    d. Avaria de 1 disco (qualquer).

71. Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?
    a. RAID 6
    b. RAID 0
    c. RAID 1
    d. RAID 0+1

72. Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?
    a. RAID 1.
    b. RAID 0+1
    c. RAID 6.
    d. RAID 5.