Considere os excertos seguintes, contendo o resultado do comando `ls -l` e um fragmento do `/etc/group`, respetivamente. Utilize a informação destes excertos para responder às questões que fazem referência ao mesmo.

```
$ ls -l
drwxr--r--  6 student ssi     192  Mar 5  10:02  utils
-rw-r--r--  1 teacher admin  2782  Feb 20 13:50  file.txt
-rw-rw-r--  1 student ssi    1692  Feb 20 13:50  script.sh

$ cat /etc/group
admin:x:998:teacher
ssi:x:999:teacher,student,hector
```

Grupo I

(7,5 Valores)

Neste grupo, uma resposta incorreta implica uma penalização. Contudo, uma eventual penalização não afeta a avaliação das questões dos restantes grupos. Não há lugar a penalização no caso de não responder a qualquer questão.

Questão 1 *Numa política de controlo de acesso discricionário (DAC) os processos que executam em nome de um utilizador só podem aceder aos recursos do próprio.*

Questão 2 *Numa política de controlo de acesso mandatório (MAC) é o administrador quem define as permissões associados aos recursos dos utilizadores.*

Questão 3 *As políticas de controlo de acesso baseado em papeis (RBAC) são computacionalmente mais exigentes do que as baseadas em atributos.*

Questão 4 *Em Linux, para um processo realizar uma operação sobre um ficheiro tem de ter permissão de leitura em todas as diretorias que é necessário atravessar para o alcançar.*

Questão 5 *Em sistemas operativos como o Unix e o Linux, a flag de set-user-id permite que um programa seja executado com um utilizador efetivo igual ao do dono do ficheiro.*

Questão 6 *Em Linux, o comando* `sudo` *utiliza a flag set-user-id para permitir a executar a um utilizador normal a execução de comandos como utilizador* `root`.

Questão 7 *A representação octal do conjunto de permissões* `-rw-r-r-` *é 533.*

Questão 8 *Considere o excerto do início da página. O comando* `chmod exec script.sh` *torna o ficheiro especificado executável.*

Questão 9 Considere o excerto do início da página. O utilizador `teacher` possui permissões de leitura, escrita e execução sobre o ficheiro `script.sh`.

Questão 10 Considere o excerto do início da página. Relativamente à diretoria `utils`, o utilizador `hector` é capaz de mudar para essa diretoria.

Grupo II

(7,5 Valores)

Nas questões deste grupo, uma resposta incorreta penaliza a pontuação dentro da mesma questão. Uma questão sem resposta não implica penalização.

Questão 11 Uma *cifra autenticada* combina as seguintes técnicas criptográficas:

- [A] uma cifra simétrica com uma cifra assimétrica
- [B] uma cifra simétrica com um MAC
- [C] uma cifra simétrica com uma assinatura digital
- [D] uma cifra assimétrica com uma assinatura digital
- [E] nenhuma das opções anteriores

Questão 12 Numa *Função de Hash Criptográfica*

[A] é sempre viável encontrar mensagens distintas que são mapeadas num mesmo valor de hash

[B] para um qualquer valor de hash, não deve ser possível encontrar uma mensagem que mapeie nesse valor

[C] existem mensagens para as quais não é viável o cálculo do respectivo valor de hash

[D] não existem nunca duas mensagens distintas com o mesmo valor de hash

[E] *Nenhuma das respostas apresentadas está correta.*

Questão 13 Um *Message Authentication Code (MAC)* garante a(s) seguinte(s) propriedade(s):

[A] não repúdio

[B] anonimato

[C] confidencialidade

[D] integridade

[E] *Nenhuma das respostas apresentadas está correta.*

Questão 14 O algoritmo *ChaCha20*, utilizado nas sessões TP, é uma

[A] cifra sequencial

[B] cifra autenticada

[C] cifra por blocos

[D] cifra simétrica

[E] *Nenhuma das respostas apresentadas está correta.*

Questão 15 Um certificado X509:

[A] pressupõe uma relação de confiança na entidade responsável pela sua emissão

[B] permite associar uma chave pública à entidade detentora da respectiva chave privada

[C] atesta que uma técnica criptográfica oferece protecção para a(s) propriedade(s) de segurança descriminada(s) nesse certificado

[D] é utilizado para garantir a confidencialidade das chaves públicas

[E] *Nenhuma das respostas apresentadas está correta.*

Questão 16 Quais dos seguintes atributos é normal encontrar-se num certificado X509

[A] periodo de validade

[B] chave privada do titular

[C] chave pública da entidade emissora

[D] identificaçao da entidade emissora

[E] *Nenhuma das respostas apresentadas está correta.*

Questão 17 Numa assinatura digital

[A] garante-se a confidencialidade e integridade da mensagem

[B] a chave pública é requerida ao gerar a assinatura

[C] garante-se a autenticidade do emissor

[D] a chave pública é requerida ao verificar a assinatura

[E] *Nenhuma das respostas apresentadas está correta.*

Questão 18 Numa cifra de chave pública

[A] é necessária a chave pública para "cifrar"

[B] garante-se a autenticidade do emissor

[C] é necessária a chave pública para "decifrar"

[D] garante-se a confidencialidade e integridade da mensagem

[E] *Nenhuma das respostas apresentadas está correta.*

Grupo III *(5 valores)*

Questão 19 No projecto TP1 foi enunciado o seguinte requisito:

> *Os clientes, ao receberem uma mensagem, devem poder verificar que a mensagem foi efectivamente enviada pelo* `<SENDER>` *especificado e a si dirigida.*

Apresente o desenho de uma solução criptográfica que permita responder a esse requisito. Fundamente a sua resposta, detalhando em particular o papel dos certificados de chave pública na solução proposta.

Questão 20 Recorde o enunciado do segundo trabalho prático e considere a proposta de uma solução que envolva um ou mais processos "demónio". Identifique **razões concretas** que **justifiquem** que algum dos processos possa/deva executar como `root`.