

 <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova <b>Teste Modelo</b>	Ano letivo	Data
	Curso <b>Segurança Informática em Redes e Comunicações</b>	Hora	
	Unidade Curricular <b>Segurança Informática</b>	Duração <b>01h50</b>	

#### Observações

- Sem consulta de documentação.

#### Cotações

Grupo I – Questão 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 – 0,70 Valores cada.

Grupo II – Questão 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 – 0,75 Valores cada.

Grupo III (apenas para quem não tem nota em AC) – Questão1 – 1,50 Valores, Questão2 – 1,25 Valores, Questão3 – 1,25 Valores, Questão4 – 1,50 Valores

## GRUPO I

Em cada questão deste grupo existem duas respostas corretas. Assinale-as indicando as respetivas alíneas. No caso de assinalar mais de duas respostas, apenas serão consideradas as duas primeiras. Cada alínea correta tem a cotação de 0,35 valores (num total de 0,70 valores por questão). Cada alínea errada desconta, na cotação, 0,15 valores (num total de 0,30 valores por questão). A cotação mínima deste grupo é 0 (zero).

### 1. Quais os princípios fundamentais de criptografia?

- a) Redundância.
- b) Atualidade / Evitar reutilização de mensagens.
- c) Criptografia simétrica.
- d) Criptografia assimétrica.
- e) Chaves privadas
- f) Chaves públicas

### 2. No processo de Cifra de Vigenère...

- a) ... o tamanho do texto é limitado a 28 caracteres.
- b) ... consiste na escrita de uma chave como cabeçalho da grelha, seguida da mensagem escrita por linhas.
- c) ... a mensagem é cifrada com uma chave alfabética.
- d) ... caso a quantidade de caracteres da chave for menor que o tamanho de caracteres da mensagem, a chave será repetida até ambas terem a mesma quantidade de caracteres.
- e) ... o tamanho do texto é limitado a 64 caracteres.
- f) ... a mensagem é cifrada com o bastão de Licurgo.

(previsão de 10 questões de escolha múltipla)

## GRUPO II

Para cada uma das afirmações apresentadas neste grupo, indique se é Verdadeira ou Falsa.

Cada resposta correta tem a cotação de 0,75 valores. Cada resposta errada desconta, na cotação, 0,30 valores. A cotação mínima deste grupo é 0 (zero).

1. O Role Based Access Control (RBAC) é uma abordagem alternativa, nas políticas de acesso, para controlo de acesso obrigatório e controlo de acesso discricionário. ✓

2. A mensagem, "AENDR AEDAH OUAAO QRIHX TSONA", encriptada com cifra de transposição de colunas e chave "CAEBDC", tem como mensagem original "O ATAQUE SERA NO DIA D NA HORA H". F

(previsão de 10 questões de V ou F)

## GRUPO III

1. Construa o texto base (linhas orientadoras) para o documento das políticas de segurança desta organização.

(previsão de 4 questões de desenvolvimento)