

U.C. 21181

Segurança em Redes e Computadores

15 de fevereiro de 2019

-- INSTRUÇÕES --

- O estudante deverá responder à prova na folha de ponto e preencher o cabeçalho e todos os espaços reservados à sua identificação, com letra legível.
- Sempre que não utilize o enunciado da prova para resposta, poderá ficar na posse do mesmo.
- Verifique no momento da entrega da(s) folha(s) de ponto se todas as páginas estão rubricadas pelo vigilante. Caso necessite de mais do que uma folha de ponto, deverá numerá-las no canto superior direito.
- Em hipótese alguma serão aceites folhas de ponto dobradas ou danificadas.
- Exclui-se, para efeitos de classificação, toda e qualquer resposta apresentada em folhas de rascunho.
- Os telemóveis deverão ser desligados durante toda a prova e os objectos pessoais deixados em local próprio da sala de exame.
- A prova termina com a palavra **FIM**. Verifique o seu exemplar e, caso encontre alguma anomalia, dirija-se ao professor vigilante nos primeiros 15 minutos da mesma, pois qualquer reclamação sobre defeito(s) de formatação e/ou de impressão que dificultem a leitura não será aceite depois deste período.
- Utilize unicamente tinta azul ou preta.
- Apresente os cálculos e justificações necessárias ao suporte da sua resposta. As respostas que não se encontrem adequadamente documentadas serão fortemente penalizadas.

Duração: 90 minutos

1. Indique, explicando-os, quais são os três conceitos básicos (*CIA triad*) considerados como fundamentais para a segurança informática. (1,5 valores)
2. Indique como se distingue um modelo de cifra simétrico convencional, de um sistema de cifra por chave-pública. (2 valores)
3. Indique as formas que conhece para proteção de um ficheiro de senhas de acesso (*passwords*). Dê exemplos de 3 técnicas que podem ser utilizadas para se tentar obter senhas de acesso. (1,5 valores)
4. Explique o que entende pelo termo “Cavalo-de.Tróia” (no original, em inglês, *trojan horse*), explicando sumariamente como pode funcionar. (2 valores)
5. Explique em que consiste a engenharia social, enquanto mecanismo de propagação de malware e quais as contramedidas que podem ser acionadas. (2 valores)
6. Indique, explicando, quais são os 3 objetivos de desenho de uma *firewall*. (3 valores)

FIM