DEI-ISEP	**Administração de Sistemas Informáticos – Época Especial**	Data: 2009/10/06 Pág. 1/2

Número: _____ Nome: _____

A duração máxima do teste é de 45 minutos.

I

Indique neste grupo as afirmações verdadeiras. Cada afirmação pode ter mais do que uma resposta correcta. Duas opções erradas anulam uma opção correcta

Algumas considerações importantes a ter em conta na definição de uma politica de Segurança Informática numa organização são...

☐ Uma correcta definição dos ataques possíveis, tendo em conta os factores humanos

☐ Implementação de uma linha de defesa contra intrusão com múltiplos firewalls..

☐ Assegurar que todos os elementos do departamento de informática são envolvidos na definição dessa politica, independentemente dos elementos dos outros sectores da organização.

☐ Nenhuma das anteriores está correcta

Nos sistemas informáticos, as falhas ...

☐ Nunca podem ser provocadas pelos utilizadores.

☐ De confidencialidade podem ser combatidas com cópias de segurança.

☐ Podem ter menores consequências se existirem cópias de segurança actualizadas.

☐ De energia podem ser totalmente resolvidas por uma UPS com bateria.

☐ Devem ser imperceptiveis quando existe tolerância a falhas.

☐ Incluem situações de tempo de resposta elevado para um serviço de rede.

A criptografia simétrica ...

☐ utiliza a mesma chave para cifrar e decifrar

☐ facilita a distribuição de chaves públicas.

☐ consegue ser mais rápida do que a de chave pública.

☐ usada actualmente emprega chaves com 64 bits.

☐ não pode usar chaves com mais do que 128 bits.

☐ não é suficientemente segura para as aplicações actuais.

O algoritmo ...

☐ RC4 é um algoritmo de cifragem de chave pública.

☐ de cifragem RC5 suporta vários comprimentos de chave.

☐ DES suporta chaves de 128 bits.

☐ MD5 é um algoritmo de cifragem simétrica.

☐ 3DES usa 3 chaves DES distintas.

As chaves públicas RSA podem ser usadas para ...

☐ produzir uma assinatura digital.

☐ verificar a origem de uma mensagem.

☐ produzir um "hash code".

☐ produzir um "checksum" criptográfico.

☐ cifrar usando criptografia simétrica.

☐ cifrar mensagens para garantir a confidencialidade.

A distribuição de chaves ...

☐ é muito mais simples para as chaves públicas.

☐ por "puzzles" é muito usada na actualidade.

☐ secretas pode ser feita usando certificados de chave pública.

☐ públicas tem de garantir a confidencialidade das mesmas.

☐ secretas pode ser feita por correio electrónico.

☐ secretas pode ser realizada durante a autenticação do utilizador.

As assinaturas digitais ...

☐ não garantem a integridade/origem de um documento.

☐ apenas podem ser verificadas pelo emissor.

☐ servem propositos diferentes das assinaturas manuais.

☐ devem impossibilitar a negação de autoria.

☐ devem garantir a confidencialidade.

☐ mais usadas actualmente aplicam criptografia de chave pública.

Pode-se definir "precedencia IP" como ...

☐ Protocolo usado os tipos de filas numa interface de output para a definição do QoS

☐ Utilização dos 3 bits mais significativos do campo TOS num header IP, para marcar um pacote IP

☐ Metodologia de sinalização entre um host e uma aplicação num servidor, para garantir um determinado nível de largura de banda para o acesso a essa aplicação.

☐ Metodologia para evitar a congestão de uma interface sob o TCP

☐ Nenhuma das anteriores está correcta

Configuração IKE:

☐ Sobre o Cisco IOS implementa mecanismos para criar automática e dinamicamente chaves expiradas.

☐ Requer a utilização de chaves públicas emitidas por uma autoridade pública de certificação

☐ Usa as SAs estabelecidas pelo IPSec para autenticar entre si os dois peers IPSec que necessitam de estabelecer uma comunicação segura.

☐ Nenhuma das anteriores está correcta