# Lista 08 - Auditoria de Sistemas

*Professor:* Fábio Engel de Camargo
*Disciplina:* Segurança em Tecnologia da Informação
*Meio para entrega:* Moodle

1. Qual dos seguintes é um exemplo de um nível de permissividade?

   **a)** Prudente
   **b)** Permissivo
   **c)** Paranóico
   **d)** Promíscuo
   **e)** Todas as alternativas anteriores

2. Uma auditoria examina se os controles de segurança são apropriados, estão instalados corretamente e são/estão _____.

   **a)** Atualizados
   **b)** Cuidando de seu objetivo
   **c)** Autorizados
   **d)** Econômicos

3. Uma _____ é um padrão usado para medir quão efetivo seu sistema é em relação a expectativas do setor.

   **a)** Objetivo de controle
   **b)** Configuração
   **c)** Padrão de referência (*benchmark*)
   **d)** Política

4. Atividades de pós-auditoria incluem qual das seguintes?

   **a)** Apresentar descobertas à gerência
   **b)** Analisar dados
   **c)** Entrevistas de saída
   **d)** Análise de descobertas do auditor
   **e)** Todas as alternativas anteriores

5. _____ é usado quando não é tão crítico detectar e responder a incidentes imediatamente.

**a)** Monitoramento que não seja em tempo real

**b)** Um controle de acesso lógico

**c)** Monitoramento em tempo real

**d)** Nenhuma das alternativas anteriores

6. Uma plataforma comum para capturar e analisar entradas de histórico é _____.

**a)** Sistema de detecção de intrusos (IDS)

**b)** Honeypot

**c)** Informação de Segurança e Gerenciamento de Evento (SIEM - Security Information and Event Management)

**d)** HIPAA

7. Em métodos _____., o IDS compara tráfego atual com padrões de atividade consistente com aqueles de uma intrusão de rede conhecida via casamento de padrão e casamento de estado.

**a)** Baseados em assinatura

**b)** Baseados em anomalia

**c)** De varredura heurística

**d)** Todas as alternativas anteriores

8. Isolamento de computador é o isolamento de redes internas e o estabelecimento de um(a) _____.

**a)** HIDS

**b)** DMZ

**c)** IDS

**d)** IPS

9. A análise do sistemas para descobrir o máximo possível sobre a organização, seus sistemas e redes é conhecida como _____.

**a)** Teste de penetração

**b)** Teste de vulnerabilidade

**c)** Mapeamento de rede

**d)** Reconhecimento