1- Como age o spear-phishing?

* **Link via e-mail.**
* Repassando e-mail.
* Pescando na canoa.
* Nenhuma das alternativas.

2- Qual proteção primária do computador para evitar invasões?

* Antivirus
* **Firewall**
* Wifi
* Roteador

3- O que é DDO’s?

* **Tipo de ataque cibernetico.**
* Tipo de defesa cibernetica.
* Metodo de prevenção.
* Sistema operacional.

4- Para que serve a Autenticação?

* Verificar se uma entidade é realmente o que diz ser.
* Proteger as informações contra alterações não autorizadas.
* Evitar que uma entidade negue que foi ela quem executou determinada ação.
* **Permitir que uma entidade se identifique.**

5- Não é uma boa medida contra virus

* Instalar um bom programa anti-vírus.
* Sempre verificar os disquetes ou CDs antes de utilizá-los.
* Não executar aplicativos desconhecidos.
* **Manter sempre a conexão do computador com a rede local, pois esta é sempre livre de vírus.**

6- Qual o método mais eficaz, dentre as opções, para obter segurança da rede?

* Treinamento da equipe em criptografia e banco de dados.
* Treinamento de frameworks de governança de TI, como COBIT e ITIL.
* Compra de firewall e proxy especializados para a rede.
* **Tecnologias, materiais e treinamento das pessoas.**

7- Qual a forma mais segura de manter sua privacidade dos seus dados?

* Criptografia.
* **Não utilizar uma rede de dados.**
* Chaves de segurança e bloqueio de fontes externas.
* Uso de sistema de autenticação de acesso.

8- Port Scanner, Protocol Analyzer e Honeypots/Honeynets são ferramentas utilizadas no processo de:

* Ameaças iminentes.
* Análise de processos.
* **Análise de risco.**
* Análise de capacidade.

9- Um sistema de segurança de intervenção preemptiva é caracterizado por:

* Atrasar ameaças.
* **Agir no momento exato de um ataque.**
* Recuperar o sistema para um estado aceitável após um ataque.
* Operar antes de um ataque.

10- Quem invade ilegalmente um computador/rede é denominado:

* Hacker
* Scanner
* Finger
* **Cracker**

11- Qual protocolo que permite a navegação na internet segura através de criptografia?

* **HTTPS**
* HTTP
* HTML
* XHTML

12- O acesso não autorizado em uma instituição pode causar diversos danos qual medida de redução para este tipo de problema?

* Habilitar proteção por senha e bloqueio automático de tela nas estações de trabalho.
* **Utilizar filtros de conteúdo e varredura antivírus em entradas e saídas para a internet.**
* Minimizar permissões de escrita/exclusão apenas ao proprietário dos dados.
* Habilitar varreduras antivírus automáticas para CDs, DVDs e pen-drives USB.

13- O usuário, além de fornecer o seu e-mail e senha, digita um código gerado ou recebido em seu celular. Essa tecnologia é conhecida como:

* Cartão inteligente
* Certificado digital
* **Token de segurança**
* Criptografia

14- A propriedade referente à salvaguarda da exatidão e da completude da informação é conhecida como:

* Disponibilidade
* Confidencialidade
* **Integridade**
* Finalidade

15- O programa semelhante aos vírus, capaz de se propagar automaticamente pelas redes, autorreplicando-se é:

* **Worm**
* Spyware
* Backdoor
* Trojan

16- São princípios da Segurança da Informação:

* Confidencialidade, integridade e vulnerabilidade.
* Vulnerabilidade, disponibilidade e autenticidade.
* Confidencialidade, ameaça e integridade.
* **Confidencialidade, confiabilidade e integridade.**

17- Qual método primário para obtenção de dados do usuário?

* Rootkit
* **Engenharia social**
* Bot
* Worm

18- O método de acesso a serviços e recursos de rede que exigem, além de uma senha, um código de verificação específico para cada acesso chama-se:

* **Verificação em duas etapas.**
* Desafio resposta.
* Identificação alternativa.
* Autenticação assimétrica.

19- Nas moedas virtuais, o Bitcoin mitiga o problema de gastar uma mesma moeda mais de uma vez (o problema de double-spending), empregando:

* **Blockchain.**
* Criptografia simétrica centralizada.
* Criptografia assimétrica centralizada.
* Autenticação do gasto e sua validação por um comitê central.

20- O símbolo do cadeado fechado presente nos navegadores de internet significa que

* A página apresentada não pode ser alterada.
* O acesso ao sítio está bloqueado.
* **A conexão é segura.**
* O navegador fechou a conexão com o servidor.