

Estácio: Alunos x +

simulado.estacio.br/alunos/

**1ª Questão** (Ref: 202007053445)

Um Técnico Judiciário está analisando as características de diversas pragas virtuais (malwares) para proceder à instalação de antivírus adequado. Dentre as características específicas por ele analisadas, estão:

I. Programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Um exemplo é um programa que se recebe ou se obtém de sites na internet e que parece ser inofensivo. Tal programa geralmente consiste em um único arquivo e necessita ser explicitamente executado para que seja instalado no computador.

II. Programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes que exploram vulnerabilidades existentes nos programas instalados no computador. Após incluído, ele é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.

III. Programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia. O atacante exige pagamento de resgate para restabelecer o acesso ao usuário.

As descrições acima são, correta e respectivamente, correspondentes a:

- ☐ vírus, spyware e rootkit.
- ☐ spyware, cavalo de troia (trojan) e ransomware.
- ☒ cavalo de troia (trojan), backdoor e ransomware.
- ☐ worm, backdoor e vírus.
- ☐ bot, rootkit e cavalo de troia (trojan).

**2ª Questão** (Ref: 202007030431)

A notícia divulgada na imprensa e identificada por uma analista de TI como sendo um ataque de malware

Pesquisar

25°C Ensolarado 11:58 05/06/2023

Estácio: Alunos x +

simulado.estacio.br/alunos/

**8ª Questão** (Ref: 202007422563)

O roubo ou a perda de laptops é atualmente um dos piores problemas para a segurança da informação corporativa. A respeito da segurança da informação em ambientes e equipamentos, considere as afirmativas a seguir.

I. Realizar o inventário de todos os laptops, de forma que possam ser identificados caso sejam recuperados.

II. Criptografar todos os dados sensíveis.

III. Proteger o BIOS com senha.

IV. Em viagens aéreas, enviar o laptop separadamente com a bagagem.

Assinale:

☐ se somente as afirmativas I e IV ajudam a proteger tais equipamentos e os dados que contém.

☒ se somente as afirmativas I, II e III ajudam a proteger tais equipamentos e os dados que contém.

☐ se somente as afirmativas I e II ajudam a proteger tais equipamentos e os dados que contém.

☐ se todas as afirmativas ajudam a proteger tais equipamentos e os dados que contém.

☐ se somente as afirmativas II e III ajudam a proteger tais equipamentos e os dados que contém.

---

**9ª Questão** (Ref: 202007403571)

Sobre Firewall, Firewall Pessoal e Antivírus, são feitas as seguintes afirmações:

I. Um Firewall é um software ou hardware que verifica informações provenientes da rede/internet ou do computador e toma ações como bloquear ou liberar a passagem dessas informações.

II. Um Firewall Pessoal é um software que é executado apenas em servidores para proteger os dados do servidor contra hackers/vírus.

III. Antivírus e Firewall têm a mesma funcionalidade, diferenciando-se apenas na forma como tomam as ações. O antivírus impede o vírus de entrar no computador, bloqueando portas. Já o firewall apaga vírus que entram, por exemplo, por pendrive.

Pesquisar

25°C Ensolarado 11:59 05/06/2023

Estácio: Alunos x +

simulado.estacio.br/alunos/

**9ª Questão** (Ref.: 202007403371)

Sobre Firewall, Firewall Pessoal e Antivírus, são feitas as seguintes afirmações:

I. Um Firewall é um software ou hardware que verifica informações provenientes da rede/internet ou do computador e toma ações como bloquear ou liberar a passagem dessas informações.

II. Um Firewall Pessoal é um software que é executado apenas em servidores para proteger os dados do servidor contra hackers/vírus.

III. Antivírus e Firewall têm a mesma funcionalidade, diferenciando-se apenas na forma como tomam as ações. O antivírus impede o vírus de entrar no computador, bloqueando portas. Já o firewall apaga vírus que entraram, por exemplo, por pendrive.

IV. Antivírus são softwares projetados para identificar, analisar e eliminar softwares maliciosos e vírus de computador. Geralmente utilizam base de dados de definição de vírus para ajudar na identificação desses nos computadores.

Em relação a estas afirmações, assinale a alternativa correta:

- ☐ Somente a afirmação IV está correta.
- ☐ Somente as afirmações II, III e IV estão corretas.
- ☒ Somente as afirmações I e IV estão corretas.
- ☐ Somente a afirmação I está correta.
- ☐ Somente as afirmações I, II e IV estão corretas.

**10ª Questão** (Ref.: 202007381752)

Pedro trabalha na área que cuida da segurança da informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de *backupp* para tentar garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor *backup* de forma redundante.

Em sua avaliação, a estratégia utilizada por Pedro para tratar o risco é considerada:

- ☐ Transferência do risco.
- ☒ Mitigação do risco.
- ☐ Evitação do risco.

Pesquisar

25°C Ensolarado 11:59 05/06/2023

Estácio: Alunos x +

simulado.estacio.br/alunos/

2ª Questão (Ref: 202007050431)

A notícia divulgada na imprensa e identificada por uma analista de TI como sendo um ataque de malware corretamente relatado é:

- ☐ O funcionário teve um software, com capacidade de interceptar e registrar o que foi digitado por ele, instalado sem seu conhecimento. O backdoor enviou os dados digitados para um PC remoto controlado pelo invasor. Com isso, suas senhas de acesso aos documentos confidenciais do escritório de advocacia foram capturadas.
- ☐ Após o ataque de backdoor, o CIO recebeu um e-mail de cibercriminosos que dizia: "Invadimos seu servidor e bloqueamos seus documentos. Pague 15.000 euros em moeda virtual para recuperá-los. Mas, para provar que podemos recuperar seus arquivos, liberaremos dois documentos de sua escolha".
- ☒ O funcionário da empresa verificou no Gerenciador de Tarefas do Windows e o processo não estava lá. O malware fez com que o arquivo malicioso desaparecesse da listagem. Para conseguir essa invisibilidade, os rootkits normalmente grampelam funções do Windows, podendo ser instalados como drivers.
- ☐ O ransomware, conhecido como Gazer, vem sendo utilizado ativamente em ataques com o objetivo de espionar governos e diplomatas. O trojan utiliza métodos avançados para se esconder por longos períodos, facilitando o roubo de informações. A sua propagação é feita por meio de campanhas de phishing.
- ☐ Quase 1 milhão de usuários da web ficaram sem conexão na Alemanha devido a um ataque do adware Mirai. Essa versão do Mirai, ao invés de abrir os roteadores, configurando os administradores com senhas padrão, consegue infectar mais aparelhos a partir da execução de códigos remotos.

3ª Questão (Ref: 202007443382)

Qual norma técnica possui o seguinte título: "Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos"?

- ☐ ABNT NBR ISO/IEC 20000-1:2011
- ☐ ABNT NBR ISO 14001:2004
- ☐ ABNT NBR ISO/IEC 27002:2013
- ☒ ABNT NBR ISO/IEC 27001:2013
- ☐ ABNT NBR ISO 9001:2008

Pesquisar

25°C Ensolarado 11:59 05/06/2023



Estácio: Alunos x +

simulado.estacio.br/alunos/

**4ª Questão** (Ref: 202007440377)

A cláusula do Anexo L, cuja norma ISO/IEC 27001:2013 é alinhada, que trata do estabelecimento dos resultados desejados do sistema de gestão, é:

- ☐ Escopo
- ☐ Suporte
- ☒ Referência normativa
- ☐ Liderança
- ☐ Termos e definições

**5ª Questão** (Ref: 202007381537)

Selecione a opção que contenha apenas itens necessários para que um processo de logon seja considerado eficiente:

- ☐ Auxiliar o usuário sobre a correção de erros no logon, para facilitar a entrada do mesmo no sistema e, desse modo, aumentar a sua produtividade.
- ☒ Informar que o computador só deve ser acessado por pessoas autorizadas e evitar identificar o sistema ou suas aplicações até que o processo de logon esteja completamente concluído.
- ☐ Permitir que o usuário possa realizar tentativas de entrada no sistema até que ele consiga fazer o logon.
- ☐ Não registrar tentativas de logon sem sucesso, de modo a evitar o armazenamento de dados desnecessário.
- ☐ Data e hora de todas as tentativas de logon com sucesso.

**6ª Questão** (Ref: 202007395485)

"O acesso é atribuído pelo administrador do sistema e é estritamente baseado na função do sujeito dentro da família ou organização e a maioria dos privilégios se baseia nas limitações definidas pelas responsabilidades do trabalho". Selecione a opção que corresponde a esse tipo de controle de acesso:

- ☒ Controle baseado em papéis (RBAC).
- ☐ Controle de acesso segregado (SAC).

Pesquisar

25°C Ensolarado 11:59 05/06/2023

Estácio: Alunos x +

simulado.estacio.br/alunos/

6ª Questão (Ref: 202007392452)

"O acesso é atribuído pelo administrador do sistema e é estritamente baseado na função do sujeito dentro da família ou organização e a maioria dos privilégios se baseia nas limitações definidas pelas responsabilidades do trabalho". Selecione a opção que corresponde a esse tipo de controle de acesso:

- ☒ Controle baseado em papéis (RBAC).
- ☐ Controle de acesso segregado (SAC).
- ☐ Controle de acesso discricionário (DAC).
- ☐ Controle de acesso obrigatório (MAC).
- ☐ Controle de acesso total (TAC).

7ª Questão (Ref: 202007393062)

Em relação ao ciclo básico de atividades recomendado pela NBR 15999 para a realização de um bom Plano de Continuidade de Negócios (PCN) e que segue o modelo PDCA, selecione a etapa na qual serão implementadas as estratégias de prevenção e de mitigação:

- ☐ Definição de Melhores Estratégias.
- ☐ Análise de Impacto de Negócios.
- ☐ Testes e Simulações.
- ☐ Documentação de Planos.
- ☒ Mapeamento de Negócios.

8ª Questão (Ref: 202007422563)

O roubo ou a perda de laptops é atualmente um dos piores problemas para a segurança da informação corporativa, respeito da segurança da informação em ambientes e equipamentos, considere as afirmativas a seguir.

I. Realizar o inventário de todos os laptops, de forma que possam ser identificados caso sejam recuperados.

II. Colocar em funcionamento todos os dispositivos de segurança.

OneDrive

Captura de tela salva

A captura de tela foi adicionada ao OneDrive.

Pesquisar

25°C Ensolarado 11:59 05/06/2023