1ª Questão (Ref.: 202306927012)

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

2ª Questão (Ref.: 202306930007)

Os malwares executam ações danosas, programadas e desenvolvidas para esse fim em um computador. Abaixo, apresentam-se diversas formas de infectar ou comprometer um computador através de códigos maliciosos, exceto:

- ☒ pelo encaminhamento de arquivos .txt pela interface de rede do computador.
- ☐ pela execução automática de mídias removíveis infectadas.
- ☐ pela exploração de vulnerabilidades existentes nos programas instalados.
- ☐ pelo acesso a páginas web maliciosas, utilizando navegadores vulneráveis.
- ☐ pela execução de arquivos previamente infectados.

3ª Questão (Ref.: 202307303509)

Qual é a relação existente entre a norma ISO/IEC 27001:2013 e o Anexo L da ISO?

- ☐ A primeira versão do Anexo L foi em 2000, como um rascunho a ser adotado pelas organizações que queriam modificar suas normas internas
- ☐ O Anexo L é uma norma universal da ISO para qualquer tipo de gestão
- ☒ Houve o alinhamento da norma ISO/IEC 27001:2013 com as diretrizes do Anexo L para padronização das definições e estruturas de diferentes sistemas de gestão ISO
- ☐ O Anexo L define a estrutura e as definições mandatórias independentemente da disciplina abordada, da norma ISO/IEC 27001:2013
- ☐ Não existe obrigatoriedade da norma ISO/IEC 27001:2013 seguir as diretivas definidas no Anexo L

4ª Questão (Ref.: 202307316949)

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 27002:2013
- [ ] ABNT NBR ISO/IEC 20000-1:2011
- [ ] ABNT NBR ISO 9001:2008
- [ ] ABNT NBR ISO 14001:2004
- [x] ABNT NBR ISO/IEC 27001:2013

5ª Questão (Ref.: 202307255104)

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

- [x] 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.
- [ ] Não registrar tentativas de logon sem sucesso, de modo a evitar o armazenamento de dados desnecessário.
- [ ] Permitir que o usuário possa realizar tentativas de entrada no sistema até que ele consiga fazer o logon.
- [ ] Data e hora de todas as tentativas de logon com sucesso.
- [ ] 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.

6ª Questão (Ref.: 202307269052)

"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 de acesso discricionário (DAC).
- [ ] Controle de acesso obrigatório (MAC).
- [ ] Controle de acesso segregado (SAC).
- [ ] Controle de acesso total (TAC).
- [x] Controle baseado em papéis (RBAC).

7ª Questão (Ref.: 202307269232)

Selecione a opção que se enquadra em um dos motivos pelos quais o Plano de Continuidade de Negócios (PCN) pode precisar ser ajustado:

- [ ] As funções e responsabilidades são bem definidas.
- [x] Mudança nas funções e membros da equipe de continuidade de negócios.
- [ ] A organização precisa fazer mudanças para demonstrar aos seus usuários e clientes que está se atualizando constantemente.
- [ ] Surgiu uma nova metodologia no mercado e, portanto, deve ser implementada imediatamente nas estratégias atuais.
- [ ] A avaliação e o teste das estratégias são eficazes.

8ª Questão (Ref.: 202307296130)

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 contêm.
- ☐ se todas as afirmativas ajudam a proteger tais equipamentos e os dados que contêm.
- ☐ se somente as afirmativas II e III ajudam a proteger tais equipamentos e os dados que contêm.
- ☐ se somente as afirmativas I e II ajudam a proteger tais equipamentos e os dados que contêm.
- ☒ se somente as afirmativas I, II e III ajudam a proteger tais equipamentos e os dados que contêm.

9ª Questão (Ref.: 202307277138)

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

10ª Questão (Ref.: 202307255319)

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 *backup* 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:

- ☒ Mitigação do risco.
- ☐ Aceitação do risco.
- ☐ Especificação do risco.
- ☐ Transferência do risco.
- ☐ Eliminação do risco.