1ª Questão (Ref.: 202308619926)

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:

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

2ª Questão (Ref.: 202308622925)

Em relação a códigos maliciosos (malwares), analise as assertivas a seguir:

I. Vírus é uma categoria de malware que pode ser infectado através de pen drives e outros dispositivos, porém não pode ser propagado por e-mail.

II. Um worm é capaz de se propagar automaticamente em redes de computadores e não se propaga por meio da inclusão de cópias de si mesmo em outros programas.

III. Um computador denominado zumbi é aquele que pode ser controlado remotamente, sem o conhecimento do seu dono.

IV. Spyware é um programa que pode ser utilizado apenas de forma maliciosa, não sendo permitida a utilização de forma legítima.

Quais estão corretas?

- ☐ Apenas III e IV.
- ☐ Apenas I e II.
- ☒ Apenas II e III.
- ☐ Apenas II, III e IV.
- ☐ I, II, III e IV.

3ª Questão (Ref.: 202309009863)

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

4ª Questão (Ref.: 202309006858)

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:

- [ ] Suporte
- [ ] Liderança
- [ ] Termos e definições
- [x] Referência normativa
- [ ] Escopo

5ª Questão (Ref.: 202308959345)

Uma forma de se proteger em relação aos vírus é através do uso de programas antivírus que procuram por padrões para detectar e eliminá-los. Cada vírus tem uma estratégia para tentar evitar sua identificação. Selecione a opção que apresenta o vírus que faz o antivírus acreditar que o programa mal-intencionado está em outro lugar que não seja a sua localização real.

- [ ] Cavalo de Troia.
- [ ] Vírus *stealth*.
- [x] Vírus blindado.
- [ ] Polimórfico.
- [ ] Mutante.

5ª Questão (Ref.: 202308959345)

Uma forma de se proteger em relação aos vírus é através do uso de programas antivírus que procuram por padrões para detectar e eliminá-los. Cada vírus tem uma estratégia para tentar evitar sua identificação. Selecione a opção que apresenta o vírus que faz o antivírus acreditar que o programa mal-intencionado está em outro lugar que não seja a sua localização real.

- ☐ Cavalo de Troia.
- ☐ Vírus *stealth*.
- ☒ Vírus blindado.
- ☐ Polimórfico.
- ☐ Mutante.

6ª Questão (Ref.: 202308961960)

Crime cibernético é todo crime executado on-line e inclui, por exemplo, o roubo de informações no meio virtual. Uma recomendação correta de segurança aos usuários da internet para se proteger contra a variedade de crimes cibernéticos é:

- ☐ Manter os softwares atualizados, exceto os sistemas operacionais, pois esses já possuem mecanismos de segurança como *firewall*, antivírus e *antispyware*.
- ☐ Usar a mesma senha (composta por letras maiúsculas e minúsculas, números e símbolos) em todos os sites com conteúdo de acesso restrito, mantendo essa senha protegida em um aplicativo de gerenciamento de senhas.
- ☒ Gerenciar as configurações de mídias sociais para manter a maior parte das informações pessoais e privadas bloqueadas.
- ☐ Proteger a rede *wireless* com senha que utiliza criptografia *Wired Equivalent Privacy* - WEP ou com uma *Virtual Protect Network* - VPN.
- ☐ Usar uma suíte de segurança para a internet com serviços como *firewall, blockwall* e antivírus, como o *LibreOffice Security Suit*.

7ª Questão (Ref.: 202308962146)

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

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

8ª Questão (Ref.: 202308978447)

Considere os seguintes controles da política de segurança estabelecida em uma empresa:

I. Controlar o acesso de pessoas às áreas em que se encontram os servidores computacionais da empresa.

II. Bloquear acesso dos funcionários para sites inseguros da internet.

III. Instalar Firewall para controlar os acessos externos para a rede local da empresa.

Os controles mencionados são, respectivamente, tipificados como de Segurança

- ☐ Física, Física e Lógica.
- ☒ Física, Lógica e Física.
- ☐ Física, Lógica e Lógica.
- ☐ Lógica, Lógica e Física.
- ☐ Lógica, Lógica e Lógica.

9ª Questão (Ref.: 202308989049)

Assinale a opção correta a respeito de segurança da informação, análise de riscos e medidas de segurança física e lógica.

- ☐ Como medida de segurança preventiva utilizam-se controle de acesso lógico e sessão de autenticação.
- ☐ Como medida de segurança corretiva utilizam-se firewalls e criptografia.
- ☒ Analisar riscos consiste em enumerar todos os tipos de risco, quais desses riscos expõem a informação e quais as consequências dessa exposição, bem como enumerar todas as possibilidades de perda direta e indireta.
- ☐ As medidas de segurança dividem-se em dois tipos: as preventivas e as corretivas.
- ☐ Em análises de riscos, é necessário levar em conta os possíveis ataques que podem ocorrer, contudo desconsideram-se os possíveis efeitos desses ataques.

10ª Questão (Ref.: 202308936928)

Uma microempresa possui um *nobreak* convencional para seus computadores. Ele se situa em uma região com muita instabilidade no fornecimento de energia elétrica.

Na fase de processo de avaliação de riscos de seu sistema de GR, a probabilidade de faltar energia elétrica por mais tempo do que o *nobreak* é capaz de suportar em termos de fornecimento de energia, desligando seus computadores, foi categorizada como um risco sem tratamento. Esse risco é denominado:

- ☐ Criterioso.
- ☐ Perceptivo.
- ☒ Residual.
- ☐ Comunicativo.
- ☐ Contextual.