Estácio

EMMELLY ALVES PORTELA
202303329156 POLO RIACHO FUNDO II - BRASÍLIA - DF

Voltar

Avaliação AV

avalie seus conhecimentos

Disc.: DGT0288 - INTRODUÇÃO À SEGUR
Aluno: EMMELLY ALVES PORTELA
Prof.: SAMUEL ZANFERDINI OLIVA

Período: 2023.1 EAD (GT)
Matr.: 202303329156
Turma: 9005

Lupa

VERIFICAR E ENCAMINHAR

Prezado(a) Aluno(a),

Responda a todas as questões com atenção. Somente clique no botão **FINALIZAR PROVA** ao ter certeza de que respondeu a todas as questões e que não precisará mais alterá-las.

A prova será SEM consulta. O aluno poderá fazer uso, durante a prova, de uma folha em branco, para rascunho. Nesta folha não será permitido qualquer tipo de anotação prévia, cabendo ao aplicador, nestes casos, recolher a folha de rascunho do aluno.

Valor da prova: 10 pontos.

1 ponto

1. 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:

(Ref.: 202308273393)

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

1 ponto

2. 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?

(Ref.: 202308273397)

- (●) Apenas II e III.
- ( ) Apenas III e IV.
- ( ) Apenas I e II.
- ( ) Apenas II, III e IV.
- ( ) I, II, III e IV.

1 ponto

3. Um funcionário estava passando na sala de equipamentos de computação quando esbarrou em um servidor web que estava posicionado no canto de uma mesa e o derrubou no chão, parando a operação do mesmo.

Segundo a norma ABNT NBR ISO/IEC 27002:2013, o responsável pela segurança do servidor deixou de colocar em prática o controle relacionado à:

(Ref.: 202308660332)

- ( ) Acordo de confidencialidade
- ( ) Gerenciamento de senha de usuário
- ( ) Segregação de funções
- ( ) Inventário dos ativos
- (●) Localização e proteção do equipamento

1 ponto

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

(Ref.: 202308660335)

- ( ) ABNT NBR ISO 14001:2004
- ( ) ABNT NBR ISO/IEC 27002:2013
- (●) ABNT NBR ISO/IEC 27001:2013
- ( ) ABNT NBR ISO 9001:2008
- ( ) ABNT NBR ISO/IEC 20000-1:2011

1 ponto

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

(Ref.: 202308598490)

- (●) 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.
- ( ) 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.

- ○ 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.

1 ponto

6. **(FGV - Técnico do Ministério Público - Tecnologia da Informação - 2018)**

Assinale o instrumento tecnológico que permite a identificação segura do autor de uma mensagem ou documento em uma rede de computadores:

(Ref.: 202308598499)

- ○ Cartão inteligente.
- ○ Biometria.
- ◉ Certificado digital.
- ○ Token de segurança.
- ○ PIN.

1 ponto

7. 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:

(Ref.: 202308610015)

- ○ Análise de Impacto de Negócios.
- ○ Documentação de Planos.
- ○ Mapeamento de Negócios.
- ○ Testes e Simulações.
- ◉ Definição de Melhores Estratégias.

1 ponto

8. 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:

(Ref.: 202308620524)

- ○ Somente as afirmações I, II e IV estão corretas.
- ○ 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.

1 ponto

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

(Ref.: 202308639521)

- ◉ 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.
- ○ Em análises de riscos, é necessário levar em conta os possíveis ataques que podem ocorrer, contudo desconsideram-se os possíveis efeitos desses ataques.
- ○ Como medida de segurança corretiva utilizam-se firewalls e criptografia.
- ○ Como medida de segurança preventiva utilizam-se controle de acesso lógico e sessão de autenticação.
- ○ As medidas de segurança dividem-se em dois tipos: as preventivas e as corretivas.

1 ponto

10. A empresa Major atua no segmento de hospedagem de sites. Ela adotou um SGR, mas não levou em consideração um fornecedor de suprimentos de peças de computador.

Esse fornecedor não possui contrato de prestação de serviços por tempo determinado, e a Major faz contratos por demanda. Esse elemento (fornecedor) é classificado como:

(Ref.: 202308610024)

- ○ Indivíduo
- ○ Parte analisada
- ○ Comprador
- ◉ Parte interessada
- ○ Contratante

VERIFICAR E ENCAMINHAR

Não respondida Não gravada Gravada