1

Marcar para revisão

A informação é estruturação e organização dos dados. Assim, os dados constituem a matéria prima da informação. Dentro dos aspectos da segurança da informação que exigem atenção são: confidencialidade, integridade e disponibilidade. A respeito da:
I - Na confidencialidade, as informações serão acessadas por quem tiver a devida autorização.
II - Na integridade, a informação que chega ao receptor pode não ser a que foi enviada pelo emissor.
III - Disponibilidade, as informações podem ser acessadas por sistemas autorizados para tal fim.
Podemos considerar como corretas:

A II e III.

B I e III.

C I apenas.

D III apenas.

E I, II, III.

2

Marcar para revisão

Em relação à segurança da informação e aos controles de acesso físico e lógico, considere:
I. Se um usuário não mais faz parte da lista de um grupo de acesso aos recursos de processamento da informação, é certo que o grupo seja extinto com a criação de um novo, contendo os usuários remanescentes.
II. Direitos de acesso (físicos e lógicos) que não foram aprovados para um novo trabalho devem ser retirados ou adaptados, incluindo chaves e qualquer tipo de identificação que associe a pessoa ao novo projeto.
III. O acesso às áreas em que são processadas ou armazenadas informações sensíveis deve ser controlado e restrito às pessoas autorizadas, preferencialmente por controles de autenticação, por exemplo, cartão de controle de acesso mais PIN (personal identification number).
Está correto o que se afirma em

A I e II, apenas.

B I, II e III.

C II e III, apenas.

D III, apenas.

E I e III, apenas.

3

Marcar para revisão

É um tipo de malware feito para extorquir dinheiro de sua vítima. Esse tipo de ciberataque irá criptografar os arquivos do usuário e exigir um pagamento para que seja enviada a solução de descriptografia dos dados da vítima. O scareware é seu tipo mais comum e usa táticas ameaçadoras ou intimidadoras para induzir as vítimas a pagar.
O texto se refere ao:

A Spam

B Botnet

C Spyware

D DDoS

E Ransomware

4

Marcar para revisão

(FCC/2010) Sobre segurança da informação, considere:
I. Ameaça: algo que possa provocar danos à segurança da informação, prejudicar as ações da empresa e sua sustentação no negócio, mediante a exploração de uma determinada vulnerabilidade.
II. Vulnerabilidade: é medida pela probabilidade de uma ameaça acontecer e o dano potencial à empresa.
III. Risco: ponto pelo qual alguém pode ser atacado, molestado ou ter suas informações corrompidas.
Está correto o que consta APENAS em

A II e III

B I e III

C I

D III

E I e II

5

Marcar para revisão

A Norma ISO/IEC 27001 é uma das normas mais reconhecidas internacionalmente para a gestão da segurança da informação.

Qual é o principal objetivo da Norma ISO/IEC 27001?

A Estabelecer diretrizes para o descarte seguro de dados organizacionais.

B Fornecer um padrão para comunicações de rede seguras.

C Definir padrões para testes de penetração cibernética.

D Criar uma estrutura para treinamento em segurança cibernética.

E Prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI).

6

Marcar para revisão

O sistema de backup de missão crítica é também chamado de ambiente de:

A *Personal Identification Number.*

B *Disaster Recovery.*

C *Daily Backup.*

D *Personal Unblocking Key.*

E *Ransomware*.

7

Marcar para revisão

O sistema de monitoramento de *nobreak* detectou uma variação na tensão elétrica na entrada dos aparelhos, mas essa variação não foi o suficiente para causar danos aos equipamentos de computação a eles conectados.

Conforme os termos relacionados à segurança da informação, o que ocorreu pode ser classificado como:

A Variação

B Dano

C Eletricidade

D Tensionamento

B Evento

8

Marcar para revisão

Ter um Plano de Continuidade de Negócios (PCN) robusto é fundamental para empresas de todos os tamanhos, pois ajuda a mitigar riscos, proteger ativos críticos, manter a confiança dos clientes e garantir a sobrevivência do negócio.

Qual é o principal objetivo do Plano de Continuidade de Negócios (PCN)?

A Desenvolver planos de vendas.

B Identificar as causas naturais de desastres.

C Identificar as vulnerabilidades dos sistemas de TI.

D Identificar estratégias de marketing.

B Garantir a recuperação e a continuidade das operações em caso de desastres.

9

Marcar para revisão

A segurança da informação refere-se à prática de prevenir o acesso não autorizado, uso, divulgação, interrupção, modificação, inspeção, gravação ou destruição de informações.
Qual problema de segurança é destacado nos exemplos de laptops levados para manutenção e discos rígidos de segunda mão comprados na Internet, como por exemplo, no eBay?

A Violações de não repúdio.

B Falha na integridade dos dados.

C Ausência de autenticidade dos dados.

D Falhas na confidencialidade dos dados.

E Problemas na disponibilidade da informação.

10

Marcar para revisão

(FEPESE/2017) Identifique abaixo as afirmativas verdadeiras (V) e as falsas (F) sobre Negação de Serviço (DoS e DDoS):
( ) Negação de serviço, ou DoS (Denial of Service) é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.
( ) Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial of Service).
( ) O principal objetivo dos ataques de Negação de Serviço (DoS e DDoS) é invadir e coletar informações do alvo.
( ) Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de botnets.
Assinale a alternativa que indica a sequência correta, de cima para baixo.

A V F F F

B V F F V

C F V V F

B V V F V

E F F V F

00 hora : 49 min : 09 seg

Ocultar

Questão 1 de 10

1 2 3 4 5
6 7 8 9 10

○ Em branco **(10)**