1

Marcar para revisão

As regras de firewall são componentes essenciais na segurança de redes e sistemas, atuando como um filtro entre uma rede interna segura e redes externas potencialmente inseguras, como a Internet.
Qual das seguintes políticas é mais comumente recomendada no mercado quando se trata de regras de firewalls?

A Negar todos por padrão, sem exceções.

B Aceitar por padrão, negar por exceção.

C Autorizar todos por padrão, restringir alguns.

D Aceitar todos por padrão, negar alguns.

E Negar por padrão, autorizar explicitamente.

2

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 Falhas na confidencialidade dos dados.

B Problemas na disponibilidade da informação.

C Violações de não repúdio.

D Falha na integridade dos dados.

E Ausência de autenticidade dos dados.

3

Marcar para revisão

Considere que uma equipe esteja trabalhando num software web com severas restrições de segurança. Além dos desenvolvedores e analistas, essa equipe conta com profissionais especialistas em segurança que têm, entre outras atribuições, a responsabilidade de realizar a revisão dos códigos a fim de evitar vulnerabilidades. Se durante a etapa de desenvolvimento um revisor da equipe de segurança detectar uma vulnerabilidade, é sua responsabilidade:

A Corrigir o problema e relatar a vulnerabilidade à equipe de segurança.

B Corrigir a vulnerabilidade, contatando os desenvolvedores que programaram o trecho de código vulnerável.

C Separar a vulnerabilidade, tratando o código com erro como mais um problema que requer correção.

D Separar a vulnerabilidade e alertar a equipe de segurança para que o problema seja resolvido.

E Isolar o problema e solicitar que a equipe de desenvolvimento corrija a vulnerabilidade imediatamente.

4

Marcar para revisão

(UFES/2014) O termo "Engenharia Social" é comumente utilizado para se referir a técnicas utilizadas por pessoas mal-intencionadas que abusam de relações sociais para conseguir informações sigilosas ou acesso a sistemas. Dos cenários abaixo, NÃO caracteriza um caso de Engenharia Social o que está descrito em

A Após fornecer seu endereço de e-mail em um site para se cadastrar, você recebe uma mensagem de e-mail desse site pedindo que você clique em um link para confirmar o seu cadastro.

B Uma pessoa liga para você, identifica-se como sendo de uma empresa prestadora de serviços (ex.: de telefonia), explica que há um problema no seu cadastro e pede que você informe vários dados pessoais, como nome completo, endereço, etc.

C Você recebe um e-mail indicando que acaba de ser sorteado com um prêmio e instruindo-o a acessar um determinado site e preencher o cadastro para coletar o seu prêmio.

D Em um ambiente de trabalho, uma pessoa liga, identifica-se como administrador dos sistemas da empresa e solicita que você siga uma série de passos, incluindo acesso a sites na internet e instalação de softwares, para melhorar o desempenho da sua máquina.

E Você recebe um e-mail alertando sobre um novo vírus muito perigoso e orientando-o a procurar por determinado arquivo em seu sistema e, caso ele exista, excluí-lo imediatamente e repassar a mensagem a todos os seus conhecidos.

5

Marcar para revisão

Assinale a assertiva que **NÃO** representa um dos benefícios para a adoção da norma ABNT NBR ISO/IEC 27001:2013 por uma organização:

A Participação da gerência na Segurança da Informação

B Mecanismo para minimizar o fracasso do sistema

C Fornece segurança a todas as partes interessadas

D Isola recursos com outros sistemas de gerenciamento

E Oportunidade de identificar e eliminar fraquezas

6

Marcar para revisão

(TRE-TO/2006 - Adaptada) Entre as medidas técnicas utilizadas no processo de proteção de dados, estão o uso de criptografia para garantir a confidencialidade das informações, o controle de acesso para limitar quem pode acessar os dados e em que condições, e a realização de backups regulares para garantir a disponibilidade dos dados em caso de falhas ou desastres. Nesse sentido, assinale a opção correta a respeito de criptografia.

A Na criptografia assimétrica, é utilizada uma única chave para cifração e decifração.

B Um dos pontos fortes dos sistemas de criptografia simétrica é a facilidade da distribuição da chave aos seus usuários.

C Na criptografia assimétrica, são utilizadas duas chaves, uma pública e uma privada, sendo uma especificamente utilizada para cifrar e a outra, para decifrar.

D A criptografia simétrica provê sigilo, integridade e autenticidade dos dados cifrados.

E A criptografia assimétrica provê sigilo, integridade, autenticidade e não-repúdio dos dados cifrados.

7

Marcar para revisão

A gestão de riscos de segurança da informação é um processo fundamental para proteger ativos de informação contra ameaças e vulnerabilidades que podem comprometer a confidencialidade, integridade e disponibilidade dos dados. Ela envolve a identificação, avaliação, tratamento e monitoramento dos riscos de segurança da informação em uma organização.

O que são riscos residuais na gestão de riscos de segurança da informação?

A Riscos que foram totalmente eliminados.

B Riscos que não foram identificados.

C Riscos que foram aceitos pela organização.

D Riscos que foram transferidos para terceiros.

E Riscos que não podem ser tratados.

8

Marcar para revisão

Diante da importância do Planejamento de Continuidade de Negócios (PCN) para garantir a resiliência das organizações diante de cenários adversos, é crucial compreender os instrumentos utilizados para sua implementação
Marque a alternativa que indica o instrumento mais utilizado para a implementação do PCN.

A SWOT (Strengths, Weaknesses, Opportunities, Threats - Forças, Fraquezas, Oportunidades e Ameaças).

B ROI (Return on Investment - Retorno sobre o Investimento).

C BSC (Balanced Scorecard - Indicadores Balanceados de Desempenho).

D PDCA (Plan, Do, Check, Act - Planejar, Fazer, Verificar, Agir).

E CRM (Customer Relationship Management - Gestão de Relacionamento com o Cliente).

9

Marcar para revisão

Na questão que avalia conhecimento de informática, a menos que seja explicitamente informado o contrário, considere que: todos os programas mencionados estejam em configuração-padrão, em português; o mouse esteja configurado para pessoas destras; expressões como clicar, clique simples e clique duplo refiram-se a cliques com o botão esquerdo do mouse; e teclar corresponda à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Considere também que não haja restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados. Assinale a alternativa que apresenta procedimento de segurança da informação que pode ser adotado pelas organizações.

A Conceder aos funcionários o acesso completo aos sistemas e à rede (intranet) da organização

B Descartar o inventário dos ativos, caso a organização possua

C Não envolver a direção com a segurança da informação, tendo em vista que ela já possui diversas outras atribuições

D Realizar, periodicamente, análises de riscos, com o objetivo de contemplar as mudanças nos requisitos de segurança da informação

E Direcionar os funcionários apenas para o exercício de suas funções diárias; pois treinamentos em segurança da informação ou outros eventos relacionados devem ser evitados

10

Marcar para revisão

(FCC/2012 - Adaptada) Códigos maliciosos (malwares) são programas que objetivam executar ações danosas e atividades maliciosas em um computador. Neste contexto encontram-se bots e botnets, sobre os quais é correto afirmar:

A — Botnet é um software malicioso de monitoramento de rede que tem a função de furtar dados que transitam pela rede e, normalmente, tornar a rede indisponível disparando uma grande carga de dados direcionados ao servidor da rede.

B — Bot é um programa que dispõe de mecanismos de comunicação com o invasor e possui um processo de infecção e propagação igual ao do vírus, ou seja, não é capaz de se propagar automaticamente.

C — A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer exclusivamente via redes do tipo P2P. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.

D — Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos, coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante.

E — Um computador infectado por um bot costuma ser chamado de attack base, pois serve de base para o atacante estabelecer suas ações maliciosas. Também pode ser chamado de spam host, pois o bot instalado tem o objetivo de enviar infinitamente spams para a caixa de e-mail de quem é vítima do ataque.

00 hora : **47** min : **25** seg

Ocultar

Questão **1** de 10

1 2 3 4 5

6 7 8 9 10

○ Em branco **(10)**