1

Marcar para revisão

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:

A Se somente as afirmativas II e III ajudam a proteger tais equipamentos e os dados que contêm.

B Se somente as afirmativas I e II ajudam a proteger tais equipamentos e os dados que contêm.

C Se todas as afirmativas ajudam a proteger tais equipamentos e os dados que contêm.

D Se somente as afirmativas I e IV ajudam a proteger tais equipamentos e os dados que contêm.

E Se somente as afirmativas I, II e III ajudam a proteger tais equipamentos e os dados que contêm.

2

Marcar para revisão

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

A As medidas de segurança dividem-se em dois tipos: as preventivas e as corretivas.

B Em análises de riscos, é necessário levar em conta os possíveis ataques que podem ocorrer, contudo desconsideram-se os possíveis efeitos desses ataques.

C Como medida de segurança corretiva utilizam-se firewalls e criptografia.

D Como medida de segurança preventiva utilizam-se controle de acesso lógico e sessão de autenticação.

E 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.

3

Marcar para revisão

(FCC/2009 - Adaptada) Engenharia social é uma técnica utilizada por pessoas mal-intencionadas e podem ocorrer em várias formas. Nesse amplo contexto, engenharia social é um método de ataque que explora vulnerabilidades, provocando riscos de

A boatos espalhados pela Internet.

B quebras de privacidade dos usuários.

C criptoanálises de senhas.

D códigos maliciosos nos computadores.

E fraudes contra os usuários.

4

Marcar para revisão

Na segurança da informação, a fragilidade de um ativo ou grupo de ativos, que pode ser explorada por uma ou mais ameaças, é chamada de:

A Desastre.

B Vulnerabilidade.

C Ameaça.

D Incidente de segurança da informação.

E Risco.

5

Marcar para revisão

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

A Não existe obrigatoriedade da norma ISO/IEC 27001:2013 seguir as diretivas definidas no Anexo L.

B O Anexo L é uma norma universal da ISO para qualquer tipo de gestão.

C 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.

D A primeira versão do Anexo L foi em 2000, como um rascunho a ser adotado pelas organizações que queriam modificar suas normas internas.

E O Anexo L define a estrutura e as definições mandatórias independentemente da disciplina abordada, da norma ISO/IEC 27001:2013.

6

Marcar para revisão

As informações podem ser armazenadas em diversos formatos, como em papel, em mídias digitais, em dispositivos móveis, em redes de computadores, entre outros. Para criar uma senha segura é recomendável que os colaboradores observem qual instrução?

A Informar a senha a terceiros como forma de redundância.

B O usuário deve utilizar apenas letras ou números.

C Sempre utilizar a mesma senha para todas as contas.

D Não se deve alterar as senhas com frequência.

E As senhas devem ter, pelo menos, oito caracteres.

7 Marcar para revisão

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:

A Residual.

B Perceptivo.

C Criterioso.

D Contextual.

E Comunicativo.

8 Marcar para revisão

Em relação à biblioteca ITIL (*Information Technology Infrastructure Library*), selecione a opção correta:

A Junto com o plano de recuperação de desastres, tem um papel reativo quando ocorrem problemas.

B Não pode ser aplicada em nenhum aspecto do plano de continuidade dos negócios.

C É aplicada apenas no plano de continuidade dos negócios.

D Aborda todas as necessidades dos negócios da empresa.

E Concentra-se no alinhamento de serviços de TI com as necessidades dos negócios.

9 Marcar para revisão

Suponha que uma entidade R (remetente) deseja enviar uma mensagem m para outra entidade D (destinatário) utilizando a internet. Para se comunicarem, R e D utilizam criptografia de chave pública. R+ e R- são as chaves pública e privada de R, respectivamente, e D+ e D- são as chaves pública e privada de D, respectivamente.
A partir dessa situação, avalie o que se afirma.
I - Se R utilizar D+ para criptografar m, então D poderá utilizar D- para decriptar m.
II - Se R utilizar R+ para criptografar m, então D poderá utilizar D- para decriptar m.
III - Se R utilizar R- para criptografar m, então D poderá utilizar R+ para decriptar m.
IV - Se R utilizar D- para criptografar m, então D poderá utilizar R+ para decriptar m.
Está correto apenas o que se afirma em:

A II e IV.

B II e III.

C III e IV.

D I e IV.

E I e III.

10 Marcar para revisão

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:

A Pelo encaminhamento de arquivos .txt pela interface de rede do computador.

B Pela execução de arquivos previamente infectados.

C Pelo acesso a páginas web maliciosas, utilizando navegadores vulneráveis.

D Pela execução automática de mídias removíveis infectadas.

E Pela exploração de vulnerabilidades existentes nos programas instalados.

00 hora : 49 min : 29 seg

Ocultar

Questão 1 de 10

1 2 3 4 5
6 7 8 9 10

○ Em branco **(10)**