A+ Alterar modo de visualização

Peso da Avaliação 1,50
Prova 47742503
Qtd. de Questões 10
Acertos/Erros 3/2
Canceladas 5
Nota 8,00

Atenção: Esta questão foi cancelada, porém a pontuação foi considerada.

1 A fase do planejamento da política de segurança necessita por parte de seus agentes, um entendimento global e abrangente sobre todos os recursos de informação, sejam eles físicos ou lógicos, para que as vulnerabilidades, pontos fracos e riscos sejam mapeados, compreendidos e tratados dentro da política. Normalmente, a visão que se tem com relação à segurança, em geral, está pautada nas ações reativas, mas que representam sérios problemas no tocante aos esforços e dispêndio financeiro, quando na busca da recuperação. Esta visão muda a partir do momento em que é criada uma política de segurança. Classifique V para as sentenças verdadeiras e F para as falsas:

( ) A abordagem proativa é essencial, mas, não depende diretamente de uma política de segurança e sim da proatividade das equipes de segurança.
( ) A abordagem proativa define claramente as responsabilidades individuais,
( ) A abordagem proativa deve facilitar o gerenciamento da segurança em toda a organização,
( ) A política proativa trata da questão da segurança das informações com a visão “Será que o sistema será atacado?”.
( ) A política proativa irá reduzir consideravelmente os custos das não conformidades.

Assinale a alternativa que apresenta a sequência CORRETA:

A V - V - F - V - F.

B F - V - V - F - V.

C F - F - V - V - V.

D V - F - F - V - V.

2 As questões da segurança da informação envolvem também recursos de hardware, que igualmente devem ser salvaguardados quanto a possíveis ações de mal uso. A destruição ou danificação destes equipamentos também devem ser pontos a considerar. As informações necessitam dos meios para suportá-las, e sua pronta recuperação deve ser possível. Portanto, se foi realizado um backup, deverá ser possível fazer o seu restore. Sobre as cópias de segurança, classifique V para as sentenças verdadeiras e F para as falsas:

( ) O conceito de volatilidade da informação se refere ao tempo que ela permanece ativa e necessária para a organização.
( ) O conceito de velocidade da informação se refere a como estas podem ser recuperadas a partir de uma mídia.
( ) Para todos os backups devem existir registros das operações envolvidas na ação de realizar a cópia. Sugere-se constar as informações da frequência, como diários, semanais, mensais e anuais.

( ) Deve-se especificar o recurso de mídia utilizado (CD, DVD, fita DAT, disquete etc.).
( ) Deve-se especificar o período de tempo em que as informações constantes na mídia devem ficar retidas para assegurar uma maior proteção ao negócio.

Assinale a alternativa que apresenta a sequência CORRETA:

A V - V - F - F - V.

B V - F - F - V - F.

C F - F - V - V - V.

D F - V - F - V - F.

Atenção: Esta questão foi cancelada, porém a pontuação foi considerada.

3 A perda de acesso às informações ou à infraestrutura de tecnologia da informação representa um risco concreto e uma ameaça para qualquer organização. É nesse enfoque que atua o plano de continuidade de negócios. O objetivo principal do plano de continuidade de negócios é manter as operações de uma organização funcionando no caso da ocorrência de um evento de falha de segurança. Com relação ao plano de continuidade de negócios, assinale a alternativa CORRETA:

A O plano de continuidade de negócios tem sua atuação restrita a processos de negócio.

B O plano de continuidade de negócios deve priorizar as operações cuja paralisação traga maior impacto para a organização.

C O plano de continuidade de negócios objetiva manter todas as operações da organização em funcionamento, no caso da ocorrência de um evento de falha de segurança.

D As atualizações no plano de continuidade de negócios ocorrem somente após um evento de falha de segurança.

Atenção: Esta questão foi cancelada, porém a pontuação foi considerada.

4 Em muitas empresas, a informação é o maior patrimônio. Diante disso, para que a organização se mantenha ativa, sem paradas ou invasões é necessária a criação de práticas organizacionais de gestão da continuidade do negócio, para que todos tenham conhecimento e para reduzir os riscos referente à segurança da informação na organização. Com base nesses documentos, classifique V para as sentenças verdadeiras e F para as falsas:

( ) O Plano de Continuidade de Negócios deve ser elaborado com o claro objetivo de contingenciar situações e incidentes de segurança que não puderem ser evitados.
( ) A empresa possuirá um plano único, chamado de Plano Global, que integra os aspectos físicos, tecnológicos ou humanos e, ainda, a preocupação com múltiplas ameaças potenciais de uma organização.
( ) O Plano de Continuidade Operacional define os procedimentos para contingenciamento dos ativos que suportam cada um dos processos de negócio.
( ) O Plano de Continuidade de Negócios, também chamado de PCO, tem como objetivo reduzir o tempo de indisponibilidade e, consequentemente, os potenciais impactos para o negócio.

Assinale a alternativa que apresenta a sequência CORRETA:

A V - F - V - V

B F - V - F - F.

C V - F - V - F.

D F - F - V - V.

5 O PCN - Plano de Continuidade de Negócios (BCP - Business Continuity Plan), com relação ao escopo das políticas de continuidade dos negócios, deve prover alternativas para o processamento de transações econômicas e financeiras das organizações em casos de falhas graves de sistemas ou desastres. Para que o plano, no caso da necessidade de uso, possa dar a garantia de eficiência desejada, deve haver ações que monitorem e testem a sua eficiência. Desta forma, podemos afirmar que:

I- A gerência deve identificar suas informações críticas, níveis de serviços necessários e o maior tempo que poderia ficar sem o sistema.
II- A gerência deve assinalar prioridades aos sistemas de informações para que possa determinar as necessidades de backup e sua periodicidade.
III- O BCP deve ser desenvolvido e documentado, além ter as manutenções atualizadas, para garantir as operações pós-desastres.
IV- São considerados objetos da contingência uma aplicação, um processo de negócio, um ambiente físico e também uma equipe de funcionários.

Assinale a alternativa CORRETA:

A As sentenças I e III estão corretas.

B As sentenças II e IV estão corretas.

C As sentenças I e II estão corretas.

D Todas as sentenças estão corretas.

Atenção: Esta questão foi cancelada, porém a pontuação foi considerada.

6 Segurança da informação significa proteger seus dados e sistemas de informação de acessos e uso não autorizados, divulgação, modificação, leitura, gravação, inspeção e destruição. O conceito de segurança da informação está ligado à confidencialidade, à integridade e à disponibilidade da informação. O conceito de segurança de processamento está ligado à disponibilidade e operação da infraestrutura computacional. Esses conceitos são complementares e asseguram a proteção e a disponibilidade das informações das organizações. O impacto da perda e/ou violação de informações para empresa é enorme e pode, em alguns casos, levá-la à falência. Com relação à segurança ambiental das informações, analise as afirmativas a seguir:

I- A parte de climatização na segurança ambiental refere-se ao bem-estar dos usuários somente na utilização do ambiente.
II- Em decorrência da necessidade do controle das condições ambientais e de confiabilidade para o sistema de condicionamento de ar, é recomendável a instalação de condicionadores do tipo compacto (self-contained) ou de central de água gelada.
III- Sistemas de detecção de incêndio e sensores automáticos, além de brigada de incêndio, devem ser

constantemente verificados e treinados.
IV- A retirada do descarte e do transporte são fatores ambientais que devem ter controles específicos, evitando que informações sejam acessadas indevidamente.

Assinale a alternativa CORRETA:

FONTE: http://efagundes.com/artigos/seguranca-da-informacao/. Acesso em: 30 out. 2018.

A As afirmativas I e IV estão corretas.

B As afirmativas I e II estão corretas.

C As afirmativas II, III e IV estão corretas.

D As afirmativas I e III estão corretas.

Atenção: Esta questão foi cancelada, porém a pontuação foi considerada.

7 Qualquer processo, regra ou metodologia necessita de atualizações e continuidade da sua manutenção, principalmente quando se fala em tecnologias da informação. Esses procedimentos são essenciais para a continuidade dos negócios e segurança dos dados e informações. A atualização e a manutenção do plano de continuidade devem ser organizadas formalmente, devem ser realizadas em períodos como uma ou duas vezes por ano. Não existe algo predefinido, pois, a cada momento que surgir a necessidade de atualizar e realizar a manutenção do plano de continuidade dos negócios, esses procedimentos devem ocorrer conforme a necessidade identificada. Segundo Ferreira e Araújo (2008), o processo de revisão do plano deve ocorrer seguindo alguns itens. Sobre esses itens, análise as seguintes opções:

I- Perda da credibilidade no mercado e irregularidades dos recursos.
II- Eventuais riscos identificados e incidentes de segurança.
III- Ocorrências de inatividade dos ativos e imagem do negócio.
IV- Vulnerabilidades encontradas e alterações na legislação.

Agora, assinale a alternativa CORRETA:

FONTE: FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de segurança da informação – guia prático para elaboração e implementação. 2. ed. revisada. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

A Somente a opção III está correta.

B Somente a opção II está correta.

C As opções I e IV estão corretas.

D As opções II e IV estão corretas.

8 Os sistemas de informação computadorizados e o acesso às dependências onde eles se encontram são em muitos casos negligenciados. Muito se ouve falar de criptografia, bloqueio, restrição de acesso e tantas outras técnicas criadas para dificultar o acesso de pessoas não autorizadas a dados sigilosos, no entanto, pouco sobre técnicas de segurança para proteger o hardware sobre o

qual esses sistemas estão funcionando. Quando o assunto é colocado em pauta, as informações não são divulgadas como deveriam. Os profissionais e usuários com pouco conhecimento de segurança em informática acabam por desacreditar da possibilidade de ocorrência de graves prejuízos para a empresa. Com relação ao acesso ao físico, assinale a alternativa INCORRETA:

FONTE: SILVA, Gilson Ferreira; SCHIMIGUEL, Juliano. Segurança em ambiente de TI: Segurança física da informação em pequenas empresas e estudo de caso em Jundiaí/SP. Revista Observatorio de la Economía Latinoamericana, Brasil, mar. 2017.

A Um firewall pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede.

B Como exemplo de uma barreira física, podemos citar uma simples parede ou até mesmo uma cerca elétrica, já na estrutura lógica, um logon em uma rede.

C Quando a empresa define um acesso físico, a segurança lógica acaba sendo desnecessária.

D Um exemplo de barreira física que limita o acesso seria uma sala-cofre ou roletas de controle de acesso físico.

9 O plano de contingência deve ser parte da política de segurança de uma organização, complementando assim, o planejamento estratégico desta. Neste documento são especificados procedimentos preestabelecidos a serem observados nas tarefas de recuperação do ambiente de sistemas e negócios, de modo a diminuir o impacto causado por incidentes que não poderão ser evitados pelas medidas de segurança em vigor. Com relação à avaliação do plano de contingência, alguns itens devem ser verificados. Sobre esses itens, analise as sentenças a seguir:

I- Deve-se verificar se os backups estão ou não atualizados e se são de fácil recuperação.
II- Deve-se verificar se a equipe de contingência está preparada caso ocorram eventualidades.
III- Deve-se verificar se os planos de contingência abrangem aspectos de integridade, confidencialidade e disponibilidade.
IV- Deve-se ter relatórios de acompanhamento para os funcionários, não há necessidade de relatórios gerenciais.

Assinale a alternativa CORRETA:

A Somente a sentença II está correta.

B As sentenças I, III e IV estão corretas.

C As sentenças II, III e IV estão corretas.

D As sentenças I, II e III estão corretas.

10 Para o sucesso da implementação do plano de contingência em uma empresa, é de suma importância que sejam observadas as funções críticas dos negócios, as quais podem estar enquadradas como de alto, médio ou baixo risco. Com esta avaliação feita, serão aplicadas as proteções mais apropriadas para cada caso. Assim, os planos de contingência de uma empresa devem garantir que:

I- Sejam suficientemente abrangentes para cobrir aspectos físicos, lógicos, de redes, de propriedades intelectuais, de pessoas, transacionais, entre outros.
II- No momento da ocorrência de algum sinistro, a equipe deve realizar o planejamento da solução e

da sua recuperação.
III- Estejam previstos testes periódicos destes planos.
IV- Na existência de backups com diversas periodicidades, somente um backup semestral precisa estar atualizado.
V- Os backups possam ser recuperados com pouca ou nenhuma dificuldade.

Assinale a alternativa CORRETA:

A As sentenças II, IV e V estão corretas.

B As sentenças I, III e V estão corretas.

C As sentenças I, II e III estão corretas.

D As sentenças I, III, IV e V estão corretas.

Imprimir