Nome: Samuel Santana Diel Data: 20 / 11 / 2023

Professora: Adriana Bastos da Costa

Disciplina: Auditoria e Segurança de Software

***Leia atentamente as instruções:***

*- A avaliação terá a duração de 1 hora.*
*- Responda as questões em WORD e poste no Blackboard.*
*- A avaliação será feita com consulta ao material da aula.*

1- Quando falamos em segurança da informação existem 3 conceitos básicos que precisam ser bem entendidos, são eles: vulnerabilidade, ameaça e falha. Baseado nos 3 conceitos, marque a opção que define cada um deles:

A) vulnerabilidade – é o que causa a parada de um serviço de TI; ameaça – é o motivo do problema; falha – é o que gera o prejuízo para a empresa

B) vulnerabilidade – é uma fraqueza no sistema; ameaça – é a exploração indevida de uma fraqueza; falha – é um incidente que afeta o serviço de TI

C) vulnerabilidade – é o que gera o prejuízo para a empresa; ameaça – é um incidente de segurança; falha – é um erro na recuperação de um backup

D) vulnerabilidade – é a exploração indevida de uma fraqueza; ameaça – é sempre causada pelo fator humano; falha – pode ser resolvida com a realização periódica de auditorias

A) vulnerabilidades – é sempre causada pelo fator humano; ameaça – pode ser resolvida com a realização periódica de auditorias; falha – está relacionada ao desenvolvimento mal feito de um software

2- Quando falamos em auditoria, vários conceitos estão envolvidos e precisam ser entendidos, tais como:

I- **Ação corretiva**
II- **Ação preventiva**
III- **Conformidade**
IV- **Constatações da auditoria**
V- **Critérios da auditoria**

Avalie a lista de explicações a seguir e marque a que corresponde ao respectivo conceito:

( ) ação para eliminar a causa de uma não conformidade potencial ou outra situação potencialmente indesejada. O objetivo aqui é a prevenção de problemas futuros
( ) resultados da avaliação das evidências obtidas ao longo do processo de auditoria, baseado nos critérios da auditoria
( ) ação para eliminar a causa de uma não conformidade identificada ou outra situação indesejada
( ) conjunto de políticas, procedimentos ou requisitos utilizados como base para a realização da auditoria
( ) atendimento a um requisito da norma que está sendo avaliada

Assinale a opção que corresponde ao correto relacionamento entre conceitos e suas explicações:

A- I, II, III, IV, V
B- V, III, I, IV, II
C- II, IV, I, V, III
D- II, V, III, I, IV
E- I, IV, III, V, II

3- A norma ISO 19011 é uma norma voltada para organizar o programa de auditorias de uma empresa, buscando organizar um conjunto de passos que devem ser seguidos para garantir a qualidade de uma auditoria. O PDCA, que é uma técnica de gestão, busca identificar pontos onde a empresa não está obtendo resultados satisfatórios, alterando esses processos de maneira gerenciada para alcançar a melhoria contínua. Avalie as asserções a seguir:

I- O passo "Implementando o Programa de Auditoria" da norma ISO 19011, está relacionado com o P – Planejar do PDCA. Pois a implementação de um programa de autoria requer planejamento, recursos e autoridade para a execução das tarefas.

ENQUANTO

II- O passo "Monitorando e Analisando Criticamente o Programa de Auditoria" da norma ISO 19011, está relacionado com o C – Checar. Pois o monitoramento do programa de auditoria ajuda a verificar se os resultados previstos com a implantação do processo estão sendo obtidos.

Marque a opção que corresponde a análise das asserções acima:

A- As duas asserções são verdadeiras
B- As duas asserções são falsas
C- A asserção I é verdadeira e a asserção II é falsa
D- A asserção I é falsa e a asserção II é verdadeira
E- As duas asserções são verdadeiras, mas não estão relacionadas com passos da ISO 19011

4- A segurança da Informação é um assunto crítico para todas as empresas, pois as consequências de um vazamento de dados pode ser algo bastante desastroso para os negócios. Avalie as afirmativas a seguir e marque com V as que forem VERDADEIRAS e com F as que forem FALSAS:

( ) Integridade - a informação acessada é completa, sem alterações ou distorções
( ) Confidencialidade – a informação deve ser acessada pelas pessoas com cargos hierárquicos mais altos.
( ) Disponibilidade – a informação deve ode ser acessada a qualquer momento pela pessoas da empresa.
( ) Criptografia - codifica texto digitalizado normal e o transforma em texto criptografado e ilegível ou em números, que são decodificados
( ) Hash - é uma metodologia de controle de acesso que embaralha os dados de forma que não sejam reconhecíveis

Assinale a alternativa que corresponde a análise correta de cada afirmação acima:

A- V F F V F
B- V F F F F
C- F V V F V
D- F V F V F
E- V F V F V

5- Um sistema de informação deve ser desenvolvido para apoiar as empresas no processamento dos dados e então, gerar conhecimento. Para que um sistema de informação seja útil e realmente apoie as empresas no seu dia a dia ele deve ser construído baseado em três dimensões, sendo elas, dimensão tecnológica, dimensão humana e dimensão organizacional. Marque a opção que relaciona corretamente a dimensão com seu objetivo:

A- **Organizacional** – a estratégia e a política definidas pelos donos da empresa determinam o modo como ela utiliza a tecnologia e os sistemas de informação; **Humana** – são pessoas que desenvolvem e usam os SI, dessa forma elas devem estar capacitadas o suficiente para desempenhar essas tarefas da melhor maneira possível; **Tecnológica** – os consultores contratados precisam conhecer as principais nuvens oferecidas no mercado, pois todos os SIs modernos precisam estar na nuvem para gerar economia para a empresa;

B- **Organizacional** – a vontade dos profissionais deve ser ouvida, pois assim podemos ter uma empresa democrática e isso determinam o modo como ela utiliza a tecnologia e os sistemas de informação; **Humana** – as pessoas contratadas já precisam conhecer o SI da empresa, para apresentar bom desempenho desde o primeiro dia de trabalho; **Tecnológica** – os SI vão além de recursos tecnológicos, mas nem por isso prescindem deles, uma boa infraestrutura de tecnologia da informação é fundamental para alcançar os resultados desejados;

C- **Organizacional** – a história da empresa, a experiência dos donos e a concorrência de mercado determinam o modo como a empresa utiliza a tecnologia e os sistemas de informação; **Humana** – as pessoas contratadas já precisam conhecer o SI da empresa, para apresentar bom desempenho desde o primeiro dia de trabalho; **Tecnológica** – os SI envolvem utilizar sempre os recursos mais modernos para garantir que a empresa sempre esteja à frente de seus concorrentes;

D- **Organizacional** – a história, a cultura e a estrutura de uma empresa determinam o modo como ela utiliza a tecnologia e os sistemas de informação; **Humana** – precisam poder alterar os SIs sempre que necessário, sem precisar de autorização, pois elas é que sabem o que precisa ser feito para gerar melhores resultados; **Tecnológica** – os SI precisam ser independentes dos recursos tecnológicos, para serem flexíveis e poderem ser alterados sempre que necessário para gerar melhores resultados financeiros;

E- **Organizacional** – a história, a cultura e a estrutura de uma empresa determinam o modo como ela utiliza a tecnologia e os sistemas de informação; **Humana** – evidentemente, são pessoas que desenvolvem e usam os SI, portanto elas devem estar capacitadas o suficiente para desempenhar essas tarefas da melhor maneira possível; **Tecnológica** – os SI vão além de recursos tecnológicos, mas nem por isso prescindem deles, uma boa infraestrutura de tecnologia da informação é fundamental para alcançar os resultados desejados;

6- O programa de auditoria precisa definir a periodicidade das auditorias, o tipo de auditoria e o escopo da auditoria. O grande objetivo é buscar a melhoria contínua através da identificação de pontos que precisam ser melhorados e pontos que precisam ser corrigidos. Dessa forma, a empresa está o tempo todo olhando para se mesma e buscando formas melhores de definir e executar seus processos. Pensando em escopo das auditorias, a auditoria de segurança é uma das auditorias mais executadas atualmente. Marque a alternativa que define corretamente o objetivo da auditoria de segurança:

A- Uma **auditoria** de **segurança** é um processo de verificação da funcionalidade de **sistemas** e de identificação de vulnerabilidades, instabilidades e falhas que facilitam ou propiciam invasões hacker, erros de execução e outros problemas.

B- Uma **auditoria** de **segurança** é um processo de atualização dos meios de controle de acesso aos **sistemas** e de identificação de formas diferentes de implantar criptografia em todos os dados sensíveis, minimizando assim a chance de invasões hackers.

C- Uma **auditoria** de **segurança** é um processo de mobilização e conscientização dos colaboradores da empresa em relação aos problemas mais comuns identificados nos mercados e nos concorrentes, de forma a prevenir novos ataques.

D- Uma **auditoria** de **segurança** é um processo de verificação das boias práticas do mercado em relação à segurança de informação, de forma a reforçar os sistemas internos da empresa, mostrando para seus clientes o investimento feito.

E- Uma **auditoria** de **segurança** é um processo de ajuste de todos os pontos de problema identificados pelos colaboradores no dia a dia da execução das suas funções, pois eles conhecem as vulnerabilidades dos sistemas e podem evitar novos ataques.

7- Um dos processos definidos pelo COBIT é o processo de Gestão de Problemas, que é um processo de Gestão relacionado ao domínio de Entregar, Atender e Dar Suporte. Marque a opção que define o objetivo principal do processo de Gestão de Problemas, segundo o COBIT:

A) Gerenciar todos os problemas de maneira controlada e organizada, resolvendo de imediato os incidentes de acordo com a criticidade do mesmo.

B) Identificar e classificar os problemas de acordo com sua causa-raiz e fornecer resoluções para prevenir incidentes recorrentes.

C) Monitorar os incidentes para, através da análise de Pareto, definir ações para evitar que os problemas voltem a ocorrer.

D) Utilizar o COBIT para identificar a causa dos problemas e assim evitar que os inventários tenham que ser constantemente realizados.

E) Gerar uma base de conhecimento com os principais problemas ocorridos em empresas do mesmo porte e área de atuação, como forma de facilitar a resolução dos incidentes.

8- A segurança da informação é um assunto crítico para todas as empresas. A ISO 27000 tem como objetivo direcionar as empresas com um conjunto de passos que definem o que deve ser feito para minimizar os riscos com a segurança da informação. Avalie as afirmações a seguir:

I. O SGSI é uma forma de segurança para todos os tipos de dados e informações, e possui atributos básicos: confidencialidade, integridade e disponibilidade.
II. O ataque passivo observa e coleta informações.
III. O ataque ativo pode alterar os dados ou informações dos dispositivos invadidos.

Assinale a alternativa que corresponde apenas às afirmações CORRETAS:

A- I e II, apenas
B- I e III, apenas
C- III, apenas
D- Todas as afirmações estão erradas
E- Todas as afirmações estão corretas

9- O ITIL é um conjunto de boas práticas, criado por iniciativa do Governo do Reino Unido, com o envolvimento de empresas e institutos, que começaram a construir esta biblioteca no início da década de 80, com o objetivo de organizar as áreas de conhecimento como Governança de TI e Gestão de Serviços de TI. O ITIL possui um ciclo de vida organizado em 5 fases, sendo elas:

1. Estratégia
2. Desenho
3. Melhoria Contínua
4. Transição
5. Operação

Relacione cada fase do ciclo de vida do ITIL com o seu objetivo:

(2) Esta é a fase em que o serviço de TI é projetado para que cumpra seu objetivo durante todo o ciclo de vida, garantindo uma abordagem holística em todos os aspectos do serviço.

(1) O propósito desta fase é criar valor para os clientes através de serviços, transformando o gerenciamento de serviços em um ativo estratégico.

(3) Esta é a fase que visa garantir que grandes volumes de mudanças possam ser tratadas com menor impacto, minimizando os riscos envolvidos com implantação de novos serviços e serviços modificados.

(4) O principal objetivo desta fase é garantir a estabilidade dos serviços de TI para que agreguem valor ao negócio.

(5) O propósito desta fase é melhorar a eficácia e a eficiência dos processos e serviços, bem como sua relação custo-benefício.

Marque a opção que corresponde ao correto relacionamento da fase do ciclo de vida com seu objetivo:

A- 1, 2, 3, 4, 5
B- 2, 1, 4, 5, 3
C- 5, 3, 4, 1, 2
D- 2, 4, 1, 5, 3

E- 1, 3, 5, 4, 2

10- Segundo o ITIL, a gestão de problemas e a gestão de incidentes possuem objetivos diferentes. Avalie as asserções a seguir:

I. O gerenciamento de incidentes deseja restaurar rapidamente o serviço com falha.

ENQUANTO

II. O gerenciamento de problemas tem foco em incidentes de segurança, e deseja eliminar a causa raiz.

Marque a alternativa verdadeira em relação às asserções:

A- As duas asserções são verdadeiras e a II complementa a I
B- As duas asserções são verdadeiras, mas não estão relacionadas
C- As duas asserções são falsas
D- A asserção I é verdadeira e a II é falsa
E- A asserção I é falsa e a II é verdadeira