FAETERJ-Rio – 4SEG – 2022/1 – Revisão AV2
Profa. Maria Claudia Roenick Guimarães

(Prova: TCE/AM 2012 - FCC - Analista Técnico de Controle Externo - TI) Sobre a gestão estratégica de TI e o alinhamento estratégico entre TI e negócios, é correto afirmar:
(a) A atuação da TI tornou-se mais que um processo de suporte, gerando valor à estrutura de negócio das organizações, entretanto, seus recursos ainda não são utilizados para auxiliar a tomada de decisões alinhada ao planejamento estratégico, por não fornecerem dados confiáveis.
(b) A Governança de TI em todas as organizações provê controles, indicadores e aponta tendências que auxiliam as corporações a ter uma visão global do universo que envolve a TI, incluindo suas capacidades, limitações, interdependências e, principalmente, como gera valor para as corporações.
(c) A gestão efetiva e eficaz de TI deve envolver o seu alinhamento ao negócio, o processo de tomada de decisão acerca de prioridades e da alocação de recursos, os mecanismos para a gestão estratégica de TI e as operações de serviços de TI.
(d) A Governança de TI se restringe à implantação de melhores práticas como COBIT e ITIL e de ferramentas que se propõem a resolver os problemas da organização. O uso dessas práticas e ferramentas resolvem as questões sobre como alinhar a TI ao negócio e envolvem os executivos de negócio nas decisões relativas à TI.
(e) A Governança de TI deve garantir o alinhamento da TI ao negócio, tanto no que diz respeito às aplicações como à infraestrutura de serviços, e garantir o alinhamento da TI a marcos de regulação externos. Não é responsabilidade da Governança de TI, porém, garantir a continuidade do negócio contra interrupções e falhas.

Considerando as normas que regulam a segurança da informação e o sistema de gestão de segurança da informação (SGSI), julgue os próximos itens.

51 ( ) Ao estabelecer o SGSI, a organização deve selecionar e implementar objetivos de controle para atender aos requisitos identificados durante as etapas de análise e avaliação de riscos e de processo de tratamento de riscos.

52 ( ) De acordo com a ISO/IEC 27005, os responsáveis pela estimativa de riscos devem entregar uma lista de riscos na qual constem níveis de valores designados com base nos cenários de incidentes e nas consequências deles para os ativos e o negócio.

Acerca do gerenciamento de serviços, com base na ITIL v3, julgue os itens subsecutivos.

55 ( ) Há um processo específico para gerenciar a continuidade de serviço da TI, o qual possui como objetivo o planejamento da recuperação dos serviços de TI.

58 ( ) Na ITIL v3, os processos são separados em cinco publicações voltadas à execução e ao monitoramento dos serviços de TI: uma para os processos de governança e quatro para os processos de gestão.

Considerando o COBIT 5, julgue os itens a seguir.

60 ( ) Alinhamento estratégico, escopo da governança, indicadores de desempenho e estrutura organizacional são os componentes formadores de um sistema de governança.

61 ( ) Portfólio de produtos e serviços competitivos é um dos objetivos corporativos do framework e está enquadrado na perspectiva financeira do balanced scorecard, ao passo que prestação de serviços de TI, em consonância com os requisitos de negócio, é um dos objetivos de TI.

Julgue os próximos itens, relativos às políticas de segurança da informação:

91 (X) Em uma organização, o planejamento para a implementação de mecanismos de segurança deverá ter início com a definição dos requisitos de disponibilidade e integridade e concluir-se com a elaboração das políticas de segurança.

92 ( ) Ao desenvolver as políticas de segurança de uma organização, o gerente deverá considerar, além do valor dos ativos a ser protegidos, a relação entre os custos de segurança e os custos de falha e recuperação.

Acerca das NBR ISO/IEC 27001, 27002 e 27005 e plano de continuidade de negócios, julgue os itens a seguir.

103 (X) O objetivo da classificação da informação é assegurar que todas as informações produzidas pela organização recebam os níveis máximos de proteção e sigilo disponíveis.

104 ( ) A análise crítica de políticas de segurança da informação deve apoiar o gerenciamento da segurança da informação propondo melhorias na política de segurança da informação em resposta às mudanças no ambiente organizacional, nas circunstâncias do negócio, nas condições legais ou no ambiente de tecnologia.

105 ( ) As expectativas e percepções das partes interessadas, a imagem e a reputação da organização devem ser consideradas no desenvolvimento dos critérios de avaliação dos riscos de segurança da informação.

(X) (CESPE 2018) Uma empresa que siga a norma NBR ISO/IEC 27001 é obrigada a implementar um sistema de gestão de segurança da informação que abranja todas as possibilidades da ISO, mesmo que estas sejam superiores às necessidades da organização.