

Lista 07 - Gerenciamento de Riscos e Plano de Continuidade de Negócios

Professor: Fábio Engel de Camargo
Disciplina: Segurança em Tecnologia da Informação
Meio para entrega: Moodle

1. De acordo com o PMI, qual termo descreve a lista de riscos identificados?
 - a) Lista de verificação de riscos
 - b) Registrador de riscos**
 - c) Metodologia de riscos
 - d) Lista de atenuação
2. Que tipo de análise de risco usa fórmulas e valores numéricos para indicar seriedade de risco?
 - a) Análise objetiva de risco
 - b) Análise qualitativa de risco
 - c) Análise subjetiva de risco
 - d) Análise quantitativa de risco**
3. Qual tipo de análise de risco usa classificação relativa?
 - a) Análise objetiva de risco
 - b) Análise qualitativa de risco**
 - c) Análise subjetiva de risco
 - d) Análise quantitativa de risco
4. Qual valor de análise de risco representa a probabilidade anual de uma perda?
 - a) EF
 - b) SLE
 - c) ALE**
 - d) ARO

5. Qual opção de resposta a risco descreveria melhor a realização de um seguro contra incêndio?
- a) Aceitar
 - b) Atenuar
 - c) Transferir**
 - d) Evitar
6. Qual resposta a risco seria mais apropriada se a possibilidade do impacto de um risco se tornar realidade for desprezível?
- a) Aceitar**
 - b) Atenuar
 - c) Transferir
 - d) Evitar
7. Qual das seguintes afirmações descreve melhor a relação entre um BCP e um DRP?
- a) Um BCP é obrigatório, mas um DRP não.
 - b) Um DRP é um componente de um BCP.**
 - c) Um DRP é obrigatório, mas um BCP não.
 - d) Um BCP é um componente de um DRP.
8. Qual termo é usado para indicar a quantidade de perda de dados aceitável?
- a) RAI
 - b) ROI
 - c) RTO
 - d) RPO**
9. Qual metodologia de avaliação de risco é comercializada como abordagem autodirecionada e tem duas edições diferentes para organizações de tamanhos diferentes?
- a) CRAMM
 - b) OCTAVE**
 - c) NIST
 - d) EBIOS
10. Um Analista de Segurança de Informações do Tribunal de Justiça está redigindo um documento que estabelece ações de monitoração de riscos e prevenção de problemas, de forma a evitar interrupções em operações do negócio. Esse documento será parte integrante
- a) do Plano de Recuperação de Desastres.
 - b) do Plano de Continuidade dos Negócios.**
 - c) do Plano de Segurança da Informação.
 - d) da Estratégia de Serviços de TI.

11. No que se refere ao plano de continuidade de negócios, assinale a opção correta.

- a)** Os objetivos do plano em tela incluem evitar a interrupção das atividades do negócio, proteger os processos críticos contra o acesso de pessoas estranhas ao ambiente e assegurar a retomada dos processos em tempo hábil, caso necessário.
- b) A existência de um gestor específico para cada plano de continuidade é desvantajoso, visto que causa aumentos significativos dos custos dos planos como um todo.
- c) Os planos de continuidade do negócio devem ser testados e atualizados infreqüentemente, já que a realização regular dessas ações acarreta o aumento significativo dos custos dos planos.
- d) A estrutura de planejamento para continuidade de negócios deve abranger os ativos e os recursos críticos para uma eventual utilização dos procedimentos de emergência, recuperação e ativação.

12. O plano de continuidade do negócio deve

- a)** ter a mesma definição e desenvolvimento para todas as organizações e utilizar uma abordagem genérica, já que dessa forma poderá abranger todos os aspectos críticos que causam impactos negativos ao negócio.
- b) ser eficiente e eficaz, ser mantido atualizado e ser testado periodicamente contando com a participação de todos os envolvidos.
- c) ser do conhecimento apenas da alta administração que deve conhecer e aprovar as ameaças e riscos que estão fora do escopo do plano.
- d) ser elaborado de forma que possibilite seu funcionamento em condições perfeitas, em nível otimizado, garantindo que não haja a possibilidade de incidentes que gerem impactos financeiros ou operacionais.

13. O Plano de Continuidade do Negócio:

- a) não precisa ser testado antes que se torne realmente necessário, pois testes por si só implicam em riscos aos ativos de informação.
- b) prioriza e estabelece as ações de implantação como resultado de uma ampla análise de risco.
- c)** define uma ação de continuidade imediata e temporária.
- d) precisa ser contínuo, evoluir com a organização, mas não precisa ser gerido sob a responsabilidade de alguém como os processos organizacionais.

14. Considerando a TI, as empresas devem ter constante preocupação com os riscos, que se concretizados, podem vir a prejudicar suas atividades. Dessa forma, a gestão de riscos é uma atividade de grande importância na condução dos negócios de uma empresa. Na maioria dos casos, a primeira etapa a ser realizada na gestão de riscos é a identificação dos riscos, que consiste em
- a) elaborar os planos de contingência, cujo objetivo é obter um controle preciso dos riscos presentes.
 - b) minimizar os problemas que possam surgir, eventualmente, em função dos riscos existentes.
 - c) detectar os perigos potenciais que possam vir a prejudicar as operações da empresa, como, a execução de um projeto de TI.
 - d) registrar todas as ações tomadas no decorrer da concretização de um risco de forma a evitar problemas semelhantes no futuro.