Questão 1

Segundo a ABNT (2018), a avaliação de riscos de TI e segurança da informação é baseada na elaboração da uma matriz de risco estruturada com aderência à norma ISO/IEC 27005. Tal norma identifica os principais itens que compõem o ambiente avaliado, especificando com clareza suas vulnerabilidades e ameaças.

Além disso, a matriz apresenta o impacto da exploração dessas vulnerabilidades pelas ameaças e a probabilidade de tal ocorrência. O risco, portanto, é um resultado da função impacto versus probabilidade, sendo estimado quantitativa (estimativa numérica) e qualitativamente (conceitual).

Analise as afirmativas a seguir:

I - Uma vez que uma ameaça explora vulnerabilidade(s) de um ativo e causa um incidente de segurança da informação, este, por sua vez, poderá causar um impacto não desejável à organização, ou seja, uma mudança não desejável nos objetivos de negócios.
II - Se uma organização adotar o conjunto mais econômico de medidas para controlar os riscos, pode-se afirmar com toda a certeza que ela pode dispensar a utilização das etapas da gerência de riscos, pois toda a organização irá obter o nível de risco no patamar "inexistente".
III - Uma típica matriz de risco consegue apresentar graus para a medição qualitativa ou quantitativa da probabilidade, mas fica inviável apresentar graus para a medição do impacto.

Marque a alternativa que possui somente as afirmativas verdadeiras:

A Somente II.

B Somente I. check_circle

C I e III.

D I, II e III.

E I e II.

check_circle

**Parabéns! A alternativa B está correta.**

A Gerência de Riscos (GR) deve ser permanente, pois sempre podem existir vulnerabilidades e ameaças que podem afetar os pilares de segurança da informação. A adoção permanente de uma cultura de Gestão de Riscos pode manter o nível dos riscos em patamares aceitáveis. Em uma GR, as Matrizes de Riscos serão elaboradas, utilizadas e melhoradas continuamente. Uma típica matriz de riscos apresenta os possíveis graus de riscos, decorrentes das escalas de medição qualitativa e/ou quantitativa da probabilidade e do impacto.

Questão 2

A tabela a seguir oferece um resumo dos tipos de ameaças à segurança enfrentadas no uso da web:

| | AMEAÇAS | CONSEQUÊNCIAS |
|---|---|---|
| Integridade | • Modificação de dados do usuário;<br>• Navegador cavalo de troia;<br>• Modificação de memória<br>• Modificação de tráfego de mensagem em trânsito. | • Perda de informações;<br>• Comprometimento da máquina;<br>• Vulnerabilidade a todas as outras ameaças. |
| Confidencialidade | • Espionagem na rede;<br>• Roubo de informações do servidor;<br>• Roubo de dados do cliente;<br>• Informações sobre configuração de rede;<br>• Informações sobre qual cliente fala com o servidor. | • Perda de informações;<br>• Perda de privacidade. |
| Negação de serviço | • Encerramento de processos do usuário;<br>• Inundação da máquina com solicitações falsas;<br>• Preenchimento do disco ou da memória;<br>• Isolamento da máquina por ataques de domain name system (DNS). | • Interrupção;<br>• Incômodo;<br>• Impede que o usuário realize o trabalho. |
| Autenticação | • Personificação de usuários legítimos;<br>• Falsificação de dados. | • Má representação do usuário;<br>• Crença de que informações falsas são válidas. |

Tabela: STALLINGS, 2015, p. 412.

Mostramos acima um levantamento das consequências de algumas ameaças para um grupo de aspectos de segurança. Na gestão de riscos, este tipo de tabela, sem levar em consideração a tomada de decisão feita após sua elaboração, pode ser um dos frutos da atividade da seguinte etapa:

A Estabelecimento do contexto.

B Análise dos riscos. check_circle

C Tratamento do risco.

D Aceitação do risco residual.

E Matriz de probabilidade *versus* impacto.

check_circle

**Parabéns! A alternativa B está correta.**

A análise ou estimativa de riscos faz parte da etapa de processo de avaliação deles. Os objetivos desta etapa são identificar os riscos e definir o que deve ser feito para diminui-los até um nível aceitável. Esta tabela mostra o levantamento realizado na etapa de identificação deles. Após isso, é possível realizar sua estimativa e avaliação.