Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

CONCURSO PÚBLICO

GOVERNO DO DISTRITO FEDERAL
PROCURADORIA-GERAL DO DISTRITO FEDERAL

CARGO 3: ANALISTA JURÍDICO
ESPECIALIDADE: ANALISTA DE SISTEMA (SUPORTE E INFRAESTRUTURA)

PROVA DISCURSIVA

Aplicação: 29/8/2021

PADRÃO DE RESPOSTA DEFINITIVO

1. A segurança da Informação ~~pode ser definida como a~~ é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos do negócio e maximizar o retorno sobre investimentos e as oportunidades de negócio, através da preservação da confidencialidade, integridade e disponibilidade da informação. Ela também inclui outras propriedades como a autenticidade, o não-repúdio e a confiabilidade.
2. Risco é o efeito da incerteza sobre os objetivos; uma combinação da probabilidade de um evento e sua consequência (probabilidade *versus* impacto). O risco residual, por sua vez, é aquele que permanece após o tratamento do risco e que pode conter riscos não identificados.
3. A política de segurança da informação tem como objetivo prover orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. Essa política deve contemplar os requisitos oriundos da estratégia do negócio, de regulamentações, da legislação e contratos e do ambiente de ameaça da segurança da informação, atual e futuro.
4. No nível mais baixo, convém que a política de segurança da informação seja apoiada por políticas de tópicos específicos. A seguir, são listados exemplos desses tópicos.

- controle de acesso
- classificação e tratamento da informação
- segurança física e do ambiente
- tópicos orientados a usuários finais (por exemplo, uso aceitável dos ativos, mesa limpa e tela limpa, transferência de informações, dispositivos móveis e trabalho remoto, restrições sobre o uso e instalação de *software*)
- *backup*
- transferência de informação
- proteção contra códigos maliciosos
- gerenciamento de vulnerabilidades técnicas
- controles criptográficos
- segurança nas comunicações
- proteção e privacidade da informação de identificação pessoal
- relacionamento na cadeia de suprimento

QUESITOS AVALIADOS

2.1

0 – Não definiu segurança da informação pela perspectiva da preservação dos seus conceitos básicos.

~~1 – Definiu segurança da informação citando apenas a preservação de um dos conceitos básicos.~~

~~2 – Definiu segurança da informação citando apenas citando apenas a preservação de dois dos conceitos básicos.~~

~~3 – Definiu segurança da informação citando apenas citando apenas a preservação de três dos conceitos básicos.~~

~~4 – Definiu segurança da informação citando apenas citando apenas a preservação de quatro dos conceitos básicos.~~

~~5 – Definiu segurança da informação citando apenas citando apenas a preservação de cinco dos conceitos básicos.~~

~~6 – Definiu segurança da informação citando apenas citando a preservação de todos os seis conceitos básicos.~~
1 – Definiu segurança da informação citando a garantia da continuidade dos negócios e minimizando os riscos.
2 – Definiu segurança da informação, englobando o item 1 e adicionalmente destacou a maximização do retorno sobre investimentos e as oportunidades de negócios.
3 – Definiu segurança da informação, englobando o item 2 e citou o conceito de confidencialidade, apenas.
4 – Definiu segurança da informação, englobando o item 3 e acrescentou o conceito de integridade.
5 – Definiu segurança da informação, englobando o item 4 e acrescentou o conceito de disponibilidade.
6 – Definiu segurança da informação, englobando o item 5 e acrescentou pelo menos uma das propriedades adicionais como a autenticidade, ou o não-repúdio ou a confiabilidade.

2.2
0 – Não definiu risco nem risco residual.
1 – Limitou-se a apresentar uma definição genérica de risco, sem tratar de risco residual.
2 – Definiu adequadamente risco, mas não risco residual, ou vice-versa.
3 – Definiu adequadamente risco e risco residual, mas não ressaltou que o risco residual pode conter riscos não identificados.
4 – Definiu adequadamente risco e risco residual, ressaltando que o risco residual pode conter riscos não identificados.

2.3
0 – Não tratou do objetivo da política de segurança da informação previsto na ISO/IEC 27002.
1 – Apresentou o objetivo da política de segurança da informação previsto na ISO/IEC 27002, mas não indicou seus requisitos, ou vice-versa.
2 – Apresentou o objetivo da política de segurança da informação previsto na ISO/IEC 27002, mas indicou apenas um de seus requisitos.
3 – Apresentou o objetivo da política de segurança da informação previsto na ISO/IEC 27002, indicando ao menos dois de seus requisitos.

2.4
0 – Não citou exemplos de políticas de tópicos específicos.
1 – Citou apenas uma política de tópicos específicos.
2 – Citou apenas duas políticas de tópicos específicos.
3 – Citou apenas três políticas de tópicos específicos.
4 – Citou apenas quatro políticas de tópicos específicos.
5 – Citou cinco políticas de tópicos específicos.