Fundação Getúlio Vargas - FGV - Management
MBA em Gestão de TI e Gerencia de Projetos
Cadeira de Gestão da Segurança da Informação

Gabarito do Simulado

Assertiva 1 – A falta de investimentos em proteção da informação estratégica decorre do fato do risco não ser mensurável. Incidentes ocorrem porque situações fortuitas e imprevisíveis acontecem. São os chamados "cisnes negros";

Resposta sugerida – O risco é sempre mensurável, desde que se admita que mensuração seja redução de incertezas. A grande maioria dos incidentes é previsível, é mapeável, e sua ocorrência não é espontânea, havendo um processo perceptível de mudança de condições no ambiente da empresa que, se monitorada, permite uma reação proativa, evitando incidentes;

Assertiva 2 – No texto podem ser identificados componentes do risco. As vulnerabilidades, por exemplo, são elementos ativos que causam incidentes quando combinados com ameaças presentes no sistema. Os executivos acusados, por exemplo, são ameaças presentes no sistema;

Resposta sugerida – Vulnerabilidades são elementos PASSIVOS, ou seja, não causam incidentes sozinhos. Dependem da ação de Ameaças, que são elementos ATIVOS que exploram as vulnerabilidades pertencentes ao sistema. Os executivos não são ameaças, e sim VULNERABILIDADES, já que sucumbiram a uma oferta em dinheiro pelos projetos. A ameaça é a montadora chinesa;

Assertiva 3 – A Renault deveria ter implementado um setor de Gestão de Segurança da Informação, que deverá assumir a responsabilidade pela definição e implementação de regras para a Gestão da Segurança. Convém que tenha perfil técnico da área de TI, por possuir formação adequada para os desafios que irá enfrentar;

Resposta sugerida – Há dois erros nessa assertiva. A definição e implementação de regras de segurança não deve ser atribuída a um único grupo, e sim compartilhada por toda a empresa, quer seja através de um Fórum ou um CGSI, mas deve haver sim uma estrutura para administrar o processo de Gestão da Segurança da Informação na empresa. Este grupo deve ser chefiado por um profissional com visão de negócio e formação executiva;

Assertiva 4 – Ações cotidianas de controle do nível de risco são essenciais para qualquer empresa. No caso da Renault, teria sido importante, para evitar o incidente de segurança, que houvesse um Plano de Contingência que monitorasse e mitigasse o risco do incidente de disponibilidade, caracterizado pela disponibilização das informações estratégicas do projeto do carro elétrico;

Resposta sugerida – Dois erros: Para evitar Incidentes de Segurança são criadas POLÍTICAS. Planos de Contingência se destinam a incidentes já ocorridos; e a disponibilização de informações estratégicas é um incidente de CONFIDENCIALIDADE;

Assertiva 5 – O Plano de Continuidade dos Negócios envolve ações de Administração de Crise (PAC), Continuidade Operacional (PCO) e de Recuperação de Desastres (PRD). Apesar de desastrada e inoportuna, por não agregar valor à imagem da empresa, a ação de comunicação através de seu Diretor Jurídico, declarando a gravidade dos acontecimentos, é uma ação planejada e incluída no PCO.

Resposta Sugerida – Não pertence ao PCO, e sim ao PAC – Plano de Administração da Crise, e são muito importantes para manutenção da imagem da empresa, acima dos incidentes perante a opinião pública e de todos os *stakeholders*.