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

AUDITOR FEDERAL DE CONTROLE EXTERNO

ORIENTAÇÃO: AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva P_4 – Questão

Aplicação: 16/8/2015

PADRÃO DE RESPOSTA DEFINITIVO

2.1. Atividades do processo “Identificação de Riscos” da NBR ISO/IEC 27005:2011
São atividades do processo: identificação dos ativos, identificação das ameaças, identificação dos controles existentes, identificação das vulnerabilidades e identificação das consequências.

2.2. Itens identificados de cada um das atividades do processo “Identificação de Riscos” para a HTYZ:

1. Identificação dos ativos: a) Centro de dados, ativo primário, responsável: diretor de TI; b) Aplicativo HTYZ, ativo primário, responsável: diretor de negócios; c) Projetos de aplicativos, ativo primário, responsável: diretor de negócios.
2. Identificação das ameaças: a) Incêndio criminoso originado nos vizinhos (contra o centro de dados); b) Ataques *hacker* contra a infraestrutura de TI (contra os projetos e o aplicativo HTYZ); c) Regulamentação oficial ou decisões judiciais favorecendo interesses contrários (contra o aplicativo HTYZ e os novos projetos); d) Avanço expressivo de produtos concorrentes sobre o mercado (contra o aplicativo HTYZ).
3. Identificação dos controles existentes: a) Seguro de toda a infraestrutura (centro de dados); b) Plano de continuidade de negócios (aplicativo HTYZ e novos projetos); c) Investimentos em segurança da informação e atualização dos equipamentos e do *software* (centro de dados, aplicativo e novos projetos); d) Política de comunicação e transparência de negócios para controle social (regulações oficiais); e) Departamento jurídico robusto e capacitado (demandas judiciais); f) Desenvolvimento do aplicativo HTYZ e novos projetos (concorrência).
4. Identificação das vulnerabilidades: a) Falta de domínio sobre a segurança física dos vizinhos (incêndio); b) Seguro repõe o prejuízo material, mas não garante a continuidade da HTYZ; c) Plano de continuidade só é eficiente contra sinistros sem perda do edifício do centro de dados; d) vulnerabilidades de *software* não conhecidas ou não corrigidas; e) Atuação mais forte dos contrários na política das regulações oficiais e derrotas judiciais.
5. Identificação das consequências: a) Perda do centro de dados e desaparecimento da HTYZ; b) Invasões, danos e vazamentos de projetos; c) Regulamentação oficial contrária à organização que inviabilizem ou dificultem os negócios; d) Condenações judiciais que acarretem prejuízos financeiros e de imagem e reputação.