Fundação Getúlio Vargas – FGV Management
MBA Gerenciamento de Projetos com Ênfase em TI
Cadeira de Gestão da Segurança da Informação
Questionamentos Úteis

Caros alunos,

Vários assuntos essenciais para a Gestão da Segurança das Informações foram discutidos em nossa cadeira. Dentre eles, posso citar:

1. O conceito de Risco:
    a. É possível mensurar o risco ?
    b. O risco é uma componente absoluta ou derivada ?
    c. Quais são as componentes do risco e suas principais características ?
    d. O risco pode ser controlado ? Como ?
    e. É possível se alcançar um panorama de "risco zero " ?
    f. Qual é a forma economicamente viável de se lidar com o risco ?
2. Uma proposta foi apresentada pelo professor, visando ocupar lacunas que são visíveis na principal referência para a Gestão da SegInfo, a ISO 27001:2005.
    a. Qual é a principal deficiência observada nesta norma (assim como em todas as normas, para possibilitar adequação a qualquer ambiente) ?
    b. Porque precisamos conhecer profundamente o negócio, antes de iniciar o trabalho ?
    c. Porque precisamos nos inteirar do cenário de requisitos legais, de segurança e do negócio ?
    d. Por que é necessária uma clara regra de priorização para os componentes do negócio ?
    e. Qual é a principal orientação a adotar durante o mapeamento dos processos de negócio ?
    f. Qual é o significado de "modelo de maturidade" ? Por que ele é necessário ?
    g. Como pode ser realizada a "GAP analysis" ?
    h. Por que é conveniente a elaboração preliminar de uma Análise de Risco, ainda não baseada em auditorias e/ou testes de robustez, mas apenas em observações óbvias ?
    i. Qual é a razão da elaboração deste planejamento de ações de curto, médio e longo prazos ?
    j. O que seriam as ações e controles "baseline" ?
    k. Porque e como podemos definir "abordagens para gestão de risco" ?
    l. Por que é importante se fazer controle de performance ?
    m. O que seria a "Política de Segurança de Alto Nível" ?
3. Visão Holística da Segurança da Informação:
    a. Por que é importante que o fluxo de informação sensível seja mapeado desde sua criação até o seu descarte ?
    b. Por que devemos identificar os atores deste processo, ou seja, quais ativos estão envolvidos com cada uma das fases do ciclo de vida de cada informação sensível em um Processo de Negócio ?

4. Política de Segurança Baseline:
    a. Quais são os principais influenciadores daquela primeira Política de Segurança da empresa, quando o entendimento de todos os envolvidos ainda não está maduro o suficiente para maiores investimentos financeiros em Segurança da Informação ?
5. Análise CIDAL
    a. Quais são os atributos da informação, quanto à sua sensibilidade ?
    b. Qual é o significado de cada um deles ?
    c. Por que é importante realizar a Análise CIDAL ?
    d. Por que é importante buscar a priorização dos Processos de Negócio, no que diz respeito à sensibilidade de cada um ?
6. Ferramenta GUT
    a. Por que é importante levar em conta, nesta priorização de Processos de Negócio, a possível evolução da sensibilidade ao longo do tempo (TENDÊNCIA) e a necessidade temporal de recuperação das funcionalidades do Processo de Negócio (URGÊNCIA) ?
7. Segurança é um Processo, e não um Projeto:
    a. Por que devemos usar o ciclo PDCA na administração da Segurança da Informação na nossa empresa ?
    b. Este ciclo deve ser cronologicamente regulado ou, em caso de observação de discrepâncias, ações proativas devem ser tomadas ?
8. Plano de Continuidade dos Negócios:
    a. Foi sugerido que o Plano de Continuidade da empresa fosse dividido em Planos de Contingência para cada Processo de Negócios, onde cada possível incidente de Segurança fosse tratado exclusivamente dentro daquele escopo. Qual é a utilidade desta medida ?
    b. Cada Plano de Contingências deve ser subdividido em
        i. PAC – Plano de Administração da Crise
        ii. PCO – Plano de Continuidade Operacional
        iii. PRD – Plano de Recuperação de Desastres

        Que tipo de ação deve ser enquadrada em cada um deles ? Qual é a vantagem de subdividir a ação de contingência em “subplanos” ?

9. Política de Segurança – O dia-a-dia do controle do nível de risco
    a. Que tipo de ações devem estar contidas na Política de Segurança ?
    b. Por que as ações devem ser iniciadas pelas “Diretrizes” ?
    c. Como se deve buscar que todos conheçam e pratiquem a Política de Segurança da empresa ?

Após questionar sobre estes aspectos, avalie os questionamentos sobre os cases a seguir:

CASE 1

Polaroid pede concordata nos Estados Unidos

A Polaroid, empresa pioneira na fabricação de câmeras para fotos instantâneas, pediu concordata nos Estados Unidos, nesta sexta-feira. A empresa alega que não tem condições de pagar suas dívidas e que a medida, restrita à divisão norte-americana da Polaroid, teria o objetivo de proteger a companhia de seus credores, enquanto ela reorganiza as finanças. Os problemas financeiros da empresa, fundada na década de 30, foram agravados com a popularização de câmeras digitais e com a queda de preço das revelações expressas. A Polaroid, que emprega 7 mil funcionários em todo o mundo, garantiu que as demais operações da empresa fora dos Estados Unidos não serão afetadas.

BBC News Brasil, 12 de outubro, 2001

Avalie o risco e ações decorrentes:

1. Durante o período pré-concordata, seria possível mensurar o risco disto acontecer ? Caso afirmativo, identifique:
    a. Ameaças
    b. Vulnerabilidades
    c. Possíveis impactos
    d. Eventuais mecanismos de segurança
2. O cenário de risco, facilmente observável após a ocorrência da concordata, aparentemente não era visível pelos executivos da Polaroid. Que elementos poderiam ter sido utilizados para que este risco fosse percebido e ações preventivas fossem tomadas ?
3. Pelo cenário descrito, pode-se depreender que a empresa não possuía um Plano de Continuidade dos negócios para perda de clientes. Imagine ações para um PAC, PCO e PRD deste Incidente de Segurança: perda irreversível de clientes pela mudança de foco de consumo no mercado fotográfico instantâneo.
4. Se você fosse Presidente da Polaroid, que diretriz você definiria para garantir a imagem de uma empresa sólida, inovadora e voltada para os interesses de seus consumidores ?

CASE 2

CNJ detecta falhas e determina inspeção no sistema de informática do TJ de MT

Cuiabá / Várzea Grande, 28/04/2010 - 12:46.

Da Redação

O corregedor geral do CNJ (Conselho Nacional de Justiça), ministro Gilson Dipp ordenou uma inspeção no sistema de informática do Tribunal de Justiça de Mato Grosso. Segundo o site RDNews, o ministro se baseou em relatório de cinco desembargadores do Estado, detectando falhas graves no sistema.

Pela determinação do ministro, a partir do dia 20 de maio, o sistema será inspecionado pelo juiz-auxiliar da Corregedoria Nacional de Justiça, Friedmann Wendpap. Ele terá total autonomia para fiscalizar o sistema de informática e de distribuição de processos do Judiciário de Mato Grosso. Denúncias apontam que no sistema é onde ocorre o esquema de "venda de sentenças".

Os trabalhos do CNJ irão durar 30 dias e um novo escândalo pode ser instalado no Judiciário do Estado.

Suponha que você foi consultado para a busca da solução definitiva para este problema. Quais seriam suas posições sobre os seguintes aspectos:

1. Quais seriam os passos preliminares a cumprir, antes de colocar a "mão-na-massa" ? Dê exemplos objetivos.
2. Durante a fase de mapeamento dos processos de negócio críticos, dê exemplos objetivos de informações que seriam passadas de um processo para o outro.
3. Suponha gaps existentes no sistema atual, que podem ter provocado a discrepância observada pelos membros da CNJ
4. Sugira uma estratégia para o controle do nível de risco e um mecanismo que poderia ser adotado para um dos gaps que você identificou no item anterior
5. Que mecanismos poderiam ser adotados para aferir se estes controles estariam efetivamente funcionando ?

6. Imagine um Processo de Negócio específico, por exemplo a decretação de sentenças. Qual é a sua avaliação sobre os aspectos da análise CIDAL ? Quais aspectos seriam comparativamente mais críticos que os demais ?
7. Com esta mesma análise, extrapole e elabore um GUT. Há elementos catalisadores da criticidade neste processo específico que possam priorizá-lo em relação a outros Processos eventualmente analisados ?
8. Suponha que uma fraude, ainda não ocorrida, esteja em curso, ou seja, esteja sendo planejada por ameaças dentro deste ambiente. Que elemento da Segurança da Informação é responsável por conter mecanismos para evitar que a fraude ocorra: a Política de segurança ou o Plano de Continuidade dos Negócios ?
9. Supondo que a fraude já ocorreu, é de vital importância que seus impactos não se estendam, prejudicando a imagem da instituição. Qual componente da Segurança da Informação teria essa função ?
10. Dentro deste elemento, temos subdivisões com funções específicas;
    a. Qual deles é responsável pela organização das ações, definindo responsáveis pelas mesmas, cientificando e esclarecendo a opinião pública e os stakeholders, evitando perda de tempo na recuperação da funcionalidade do negócio ?
    b. Qual deles é focado exclusivamente na recuperação do Processo de Negócios, não necessariamente dentro dos patamares máximos, mas sim dentro de limites aceitáveis para o nível impactante resultante e a tolerância temporal definida ?
    c. Qual deles é responsável não apenas por trazer o Processo de Negócios para sua operacionalidade normal, mas principalmente por reunir as informações pertinentes às falhas de segurança ocorridas no Processo que permitiram que o incidente ocorresse, propondo ações objetivas para que o mesmo não mais ocorra ?