Exemplos de Respostas para as “Dicas da Prova”

1. O conceito de Risco:

    a. Sim. É sempre possível mensurar o risco. Mensurar significa “reduzir incerteza”. Nossa obsessão por números precisos nos conduz a abrir mão de uma mensuração que, se por um lado pode representar grande imprecisão, por outro lado possibilita uma aferição e discussão que, aos poucos, reduzirão a sua incerteza;
    b. O Risco é uma componente DERIVADA. Isto significa que ele não pode ser avaliado diretamente, e sim de suas componentes.
    c. As componentes do risco são:
        i. AMEAÇAS – são os elementos ativos, que exploram vulnerabilidades existentes causando impacto. Um funcionário desonesto explora os controles ineficazes das empresas para se locupletar. Ele é uma ameaça;
        ii. VULNERABILIDADES – são os elementos passivos, pertencentes ao sistema e que nem sempre são visíveis e óbvios. Um funcionário desatento, que tem a responsabilidade de vigiar a correta execução de procedimentos, mas que não faz isto com atenção é uma vulnerabilidade, uma vez que o funcionário desonesto pode usar esta falta de controle para efetuar sua ação impactante;
        iii. IMPACTO – é o EFEITO, para o negócio, da ação de uma ameaça explorando vulnerabilidades. O funcionário desonesto, explorando os controles ineficientes que o funcionário desatento deveria impor, pode realizar uma fraude desviando recursos financeiros. É importante observar que, neste momento, não apenas impactos tangíveis devem ser avaliados, mas também os intangíveis, como uma possível agressão à imagem da empresa; e
        iv. MECANISMOS DE SEGURANÇA – são os CONTROLES do nível de RISCO que devem ser usados para que o risco permaneça a um nível aceitável. Podem ser FÍSICOS, TECNOLÓGICOS ou HUMANOS, como barreiras físicas de proteção, sistemas de firewall e treinamento dos colaboradores.
    d. O Risco pode ser controlado através da identificação dos processos de negócio críticos, Análise de Risco e adoção de uma estratégia, que poderá ser: MITIGAR, RETER, ELIMINAR ou TRANSFERIR.
    e. O custo para o controle do nível de risco, que envolve ações de prevenção (Política de Segurança) e de reação (Plano de Continuidade dos Negócios) deve ser compatível com o potencial impactante de cada incidente de segurança possível.

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. A Norma apenas diz O QUE FAZER, sem dizer COMO FAZER. Inicia bruscamente sugerindo uma Análise de Risco, o que é impossível sem um profundo

conhecimento do negócio. Sugere um PDCA rigidamente seqüencial, sem possibilitar que o monitoramento contínuo possa implementar uma ação proativa;

b. Partindo da simples observação de que, para investir em segurança é necessário conhecer o potencial impactante dos incidentes de segurança, que para serem identificados é necessário um grande e profundo conhecimento do negócio, a sugestão é que isso seja feito de forma metodológica, documentada, envolvendo todos os Gestores de processos de negócio e estimulando a participação de todos os conhecedores do negócio;
c. Mecanismos de Segurança envolvem regras. Ocorre que já existem regras, muitas delas, se descumpridas, causam impactos graves para o negócio. Todo um levantamento da questão legal deve ser feito preliminarmente, como ponto de partida para a criação de eventuais novas regras que, obviamente, não poderão contrariar as básicas;
d. Disse várias vezes na aula que as empresas nunca terão recursos financeiros, tempo e pessoas disponíveis para fazer tudo o que precisa para operar sob risco controlado. Naturalmente, é importante que os Processos de Negócio sejam priorizados de forma que os mais críticos, por serem altamente impactantes em um cenário da muitas vulnerabilidades e ameaças e poucos controles existentes, sejam tratados prioritariamente;
e. O mapeamento deve ser feito com o foco na INFORMAÇÃO. O mais físico dos incidentes sempre envolve informação, ou na maioria das vezes, falta dela;
f. O "Modelo de Maturidade" é a decisão absolutamente particular de cada empresa sobre a temporalidade de seus processos de segurança. Por exemplo, de quanto em quanto tempo um determinado processo de negócios da empresa deve ser auditado ? Estas decisões devem ser tomadas com antecedência e serem alteradas sempre que demonstrar incoerência com a real necessidade da empresa;
g. *Gap Analisys* é um procedimento de avaliação de situações de risco existentes em um determinado sistema empresarial. Pode ser realizado com base nas ISO 27001 e 27002, por exemplo, mas outros instrumentos também podem (e devem) ser utilizados. Basicamente, duas preocupações devem nortear este trabalho: *gaps* metodológicos e *gaps* em mecanismos de controle. Um *check-list* básico pode ser seguido com orientação nos tópicos a seguir:
    i. *Conformidade com Requisitos Regulatórios (ISO, CoBIT, HIPAA, SOX, PCI, etc.)*
    ii. *Gerenciamento da Política de Segurança*
    iii. *Gerenciamento de Ativos*
    iv. *Gerenciamento dos Recursos Humanos*
    v. *Gerenciamento da Segurança Física*
    vi. *Gerenciamento das Operações e das Comunicações*
    vii. *Gerenciamento do Controle do Acesso à Informação*
    viii. *Gerenciamento da Segurança em Sistemas de Informação*
    ix. *Gerenciamento de Incidentes de segurança da Informação*
    x. *Gerenciamento da Continuidade dos Negócios*

Uma boa prática é elaborar questionários com base nestes controles que sejam aplicáveis ao ambiente onde se vai trabalhar.

h. A filosofia de trabalho da cadeira é que o principal ganho em cada ação de segurança é a cultura que se estabelece, e não é perdida se for permanentemente valorizada, praticada e atualizada. Uma análise de risco óbvia, com elementos conhecidos de todos, explora a característica natural do ser humano de se sentir mais seguro com coisas que ele já conhece. Por isso, incidentes de segurança já ocorridos na empresa são excelentes insumos para a elaboração de uma Política de Segurança baseline;
i. Adequação ao *Budget* da empresa;
j. Controles de uma Política de Segurança e ações de um Plano de Continuidade baseados na Análise de Riscos *baseline*, com o principal objetivo de iniciar a criação da cultura de segurança;
k. Gestão de Risco é uma atividade complexa e que envolve a necessidade de um profundo conhecimento do negócio e de seus processos, uma vez que envolve investimentos. Na ISO 27005 são definidas as estratégias MITIGAR, RETER, ELIMINAR e TRANSFERIR. Uma delas deverá ser adotada pelo corpo executivo da empresa, uma vez executada a Análise de Riscos;
l. Questionamento típico e justo dos executivos as empresas. O excesso desmesurado de controles pode "engessar" processos produtivos, o que é inadmissível para qualquer empresa. É essencial que a adoção de controles tenha um acompanhamento de desempenho dos processos de negócios, visando evitar que isso aconteça. É importante, para o sucesso desta empreitada, que a segurança agregue valor;
m. A Política decorrente do Planejamento e Implementação de controles decorrentes da Análise de Riscos baseline.

3. Visão Holística da Segurança da Informação
    a. O incidente ocorre onde a segurança falha, ou seja, onde não há controles ou os mesmos não são eficazes. É importante que o foco seja NA INFORMAÇÃO, ou seja, se a informação é sensível, é vital que a mesma tenha o mesmo nível de proteções na sua manipulação, armazenamento, transporte e descarte;
    b. Os atores (ou seja, os ativos) da informação são efetivamente os elementos que executam as fases do ciclo de vida. São eles, então, que recebem a atenção das ações de controle;

4. Política de Segurança Baseline
    a. Incidentes de Segurança JÁ OCORRIDOS na MESMA EMPRESA, Incidentes de Segurança OCORRIDOS em EMPRESAS SEMELHANTES, e EXPERIÊNCIA ESPECIALISTA, deixando aqui bem claro que está se referindo a elementos pertencentes à própria estrutura corporativa, profundos conhecedores da natureza do negócio;

5. Análise CIDAL
    a. CONFIDENCIALIDADE, INTEGRIDADE, DISPONIBILIDADE, AUTENTICIDADE E LEGALIDADE;

b. Significados:
    i. CONFIDENCIALIDADE – restrição de acesso à informação com base no princípio da "necessidade de conhecer a informação" para o negócio;
    ii. INTEGRIDADE – garantia de que a informação não foi alterada ou deteriorada por alguém não-autorizado;
    iii. DISPONIBILIDADE – garantia de que a informação estará disponível para o seu uso dentro das tolerâncias temporais para o negócio;
    iv. AUTENTICIDADE – garantia de que uma determinada informação é autentica, ou seja, foi adequadamente manipulada por quem está sendo identificado; e
    v. LEGALIDADE – observância dos diplomas legais para sua manipulação, armazenamento, transporte ou descarte.

    É importante ressaltar que a identificação de um incidente de um determinado tipo pressupõe que os demais estão sendo garantidos. Por exemplo: o acesso a uma informação sigilosa, protegida por controle de acesso, demanda recursos de proteção da confidencialidade. No entanto, é mister que a autenticidade neste acesso seja garantida, senão o mecanismo de confidencialidade não funcionará.
c. A análise CIDAL permite que se evidencie necessidades específicas, que demandam mecanismos de controle especializados. Confidencialidade, por exemplo, demanda ferramentas de criptografia. Disponibilidade, por sua vez, demanda redundâncias, etc.
d. A priorização é essencial porque aponta a criticidade, em termos de nível de risco aferido, para os Processos de Negócio (PN) de forma comparativa. Isso permite que os PN mais críticos sejam atendidos antes dos menos críticos.

6. Ferramenta GUT
    a. Processos de Negócio são avaliados de forma estática, à luz de uma realidade momentânea que pode mudar ao longo do tempo. Além disso, cada incidente de segurança ocorrido demandará uma recuperação em tempo variável, o que influenciará a sua criticidade. A ferramenta GUT permite que os aspectos temporais relacionados com a Urgência para seu contingenciamento e a Tendência de evolução da criticidade do Processo de Negócios ao longo do tempo sejam aferidos e levados em consideração na priorização entre os PN;

7. Segurança é um Processo, e não um Projeto
    a. Um erro típico das empresas é considerar a Segurança da Informação como um projeto a ser implementado. Imagina-se que, com alocação de recursos, aquisição de ferramentas e alguns testes a empresa estará segura e livre de incidentes. As empresas são entidades vivas, dinâmicas, com mudanças diárias que influenciam no cenário de riscos. A forma mais correta de se abordar este problema é de forma contínua, onde o planejamento feito em um determinado momento gera uma solução, que deve ser continuamente monitorada, avaliada e dar origem a correções no planejamento, de forma a acompanhar a dinâmica da empresa. O Ciclo de Deming (PDCA) é bastante conhecido e espelha esta dinâmica cíclica processual;

b. Ambos. É importante que hajam momentos periódicos de avaliação, como auditorias, mas também é vital que a observação de não-conformidades com o nível de risco desejado provoquem mudanças nos controles.

8. Plano de Continuidade dos Negócios
    a. Há várias vantagens na modularização dos processos, mas neste caso, a mais visível é a de proporcionar capacitação apenas àqueles diretamente envolvidos com o PN a ser contingenciado, evitando-se os caros e inócuos treinamentos hoje feitos nas empresas que não se traduzem necessariamente em sucesso em uma situação real;
    b. A divisão em subplanos possibilita a especialização no treinamento e a simultaneidade de ações com objetivos diferentes, porém todos associados ao contingenciamento do Processo de Negócios. Ações típicas de cada subplano:
        i. PAC – comunicação com os *stakeholders*, identificação dos responsáveis pelas ações de contingenciamento, identificação e localização dos insumos necessários para o contingenciamento, questões temporais (gatilhos) para as ações de contingenciamento, registro do histórico do incidente;
        ii. PCO – é o contingenciamento em si. É o passo-a-passo das ações que visem a garantia de um nível aceitável de alcance dos objetivos do Processo de Negócios afetado na presença de elementos da crise;
        iii. PRD – é a recuperação do *status quo*. Restauração de ativos e operacionalidade aos níveis anteriores à crise. Análise das razões que permitiram que o incidente acontecesse e proposição de ações para que ele não volte a ocorrer. Ações indenizatórias em benefício da empresa e, eventualmente, de terceiros prejudicados com o incidente, quando cabível.

9. Política de Segurança – O dia-a-dia do controle do nível de risco
    a. A Política de Segurança deve conter exclusivamente controles para evitar a ocorrência de incidentes de segurança. Não fazem parte dela ações de contingenciamento. É importante ressaltar, no entanto, que testes periódicos dos Planos de Contingência reduzem o risco de comprometer o negócio de forma impactante, logo, estes testes devem ser previstos na Política de Segurança;
    b. As Diretrizes são instruções diretas, objetivas e abrangentes, emitidas pelo setor estratégico da empresa. Devem ser poucas e muito claras para todos. Deve-se iniciar pelas diretrizes porque as Normas, que são setoriais, focadas em um ou mais Processos de Negócio específicos, decorrem das diretrizes, e os procedimentos nada mais são do que os "*how-to*" que possibilita que todos os responsáveis sejam capazes de cumprir adequadamente as diretrizes e as normas;
    c. Há várias técnicas que podem ser usadas. Naturalmente, um bom plano de capacitação é fundamental, mas para haver uma motivação permanente é importante que sejam estabelecidos e implementados prêmios e punições para o nível de conformidade dos colaboradores com a Política de Segurança da empresa;

Case 1 – Polaroid pede Concordata

1. Durante o período pré-concordata, seria possível mensurar o risco disto acontecer ? Caso afirmativo, identifique:
    a. Ameaças – Cenário altamente competitivo: aumento do número de empresas bem estruturadas no segmento fotográfico; aumento da exigência do

consumidor; evolução tecnológica no mercado fotográfico com o advento da fotografia digital, queda de preço das revelações de fotografias digitais.

   b. Vulnerabilidades – inexistência de um segmento (na época) tecnologicamente capaz de oferecer um produto competitivo na modalidade digital;
   c. Possíveis impactos – redução significativa nos lucros, perda de fidelização, crise financeira, falência.
   d. Eventuais mecanismos de segurança - O artigo não cita nenhum mecanismo de segurança disponível para este cenário.

2. Monitoramento no nível de satisfação do consumidor final; acompanhamento das tendências; análises de perda de faturamento.
3. PAC – anúncio de novidades para o consumidor fidelizado até então, estimulando a curiosidade do ainda não fidelizado e do já usuário de câmeras digitais
   PCO – parceria ou aquisição de/com algum detentor da tecnologia digital, porém com fatia inexpressiva no mercado. Uso da marca Polaroid nos produtos desta empresa
   PRD – investimentos com meta de retorno aceitável; reassociação da marca Polaroid com a tecnologia "imagem instantânea". Análise da crise.
4. Diretriz exemplo: "A imagem da Polaroid é o seu principal patrimônio. Deve ser valorizada permanentemente por todos da empresa"

Case 2 - CNJ detecta falhas e determina inspeção no sistema de informática do TJ de MT

1. Estudo de toda a legislação pertinente ao nicho do problema. Leis, regulamentos, políticas. Tudo que possa influenciar os caminhos do trabalho. A sistemática legal vigente para distribuição de processos, por exemplo, deve ser profunda e detalhadamente conhecida;
2. Despachos, recursos, requerimentos, inevitavelmente sentenças. É importante observar que são informações ALTAMENTE sensíveis;
3. Um *gap* óbvio é a falta de um eficaz controle de acesso
4. Estratégia → reduzir a possibilidade da venda de sentenças através do robustecimento do sistema de controle de acesso. Mecanismos → adoção de mecanismos de identificação digital para todos os envolvidos no trâmite processual, através de tokens criptográficos; adoção de auditoria permanente pela corregedoria da justiça;
5. Monitoramento. É vital que os responsáveis pelas varas sejam imbuídos da sua função de garantir a lisura dos processos e passem a monitorar e reagir prontamente em caso de discrepâncias;
6. Este PN é altamente sensível. Inevitavelmente, pode-se observar que a INTEGRIDADE e a AUTENTICIDADE são notadamente mais críticos que os demais;
7. Não, a princípio;
8. Política de Segurança;
9. No Plano de Continuidade dos Negócios;
10. Dentro deste elemento, temos subdivisões com funções específicas
    a. PAC – Plano de administração de Crise
    b. PCO – Plano de Continuidade Operacional
    c. PRD – Plano de Recuperação de Desastres