Respostas do Estudo de Caso

Componentes do Grupo \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Turma:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Critérios de Aceitação do Risco:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Um critério de aceitação de risco é uma fronteira entre o aceitável e o inaceitável para o negócio. Limites financeiros, perda de *market-shar*e e comprometimento de metas são critérios típicos. Neste trabalho, vamos usar a abordagem QUALITATIVA, estabelecendo condições perceptíveis porém baseadas em condições limite não numéricas. Por exemplo, podemos definir que não são aceitos incidentes de segurança de forma a causar perda irreversível de clientes, a ponto de provocar comprometimento da imagem. Observe que este critério é abrangente, servindo para todos os setores da empresa, inclusive para o foco do trabalho que é a loja virtual. Leia o ANEXO do case antes (página 82).

1. Mapeamento dos Ativos mais Relevantes:

|  |  |  |  |
| --- | --- | --- | --- |
| Ativo | Tipo | Fase | Informação Sensível |
| BD | F/T | A | Cadastros de clientes, estoque, preços |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_O mapeamento de ativos é importante porque direciona as ações de treinamento, no caso de ativos humanos, favorece a utilização de auditorias produtivas, para processos ou sistemas, a permite o desenvolvimento de ações físicas onde o risco é maior. A coluna “Tipo” deve definir se o ativo é (F)ísico, (T)ecnológico ou (H)umano, ou uma combinação deles. A coluna “Fase” define se o ativo participa da (M)anipulação, (A)rmazenamento, (T)ransporte ou (D)escarte da informação, ou ainda uma combinação deles. Na coluna “Informação Sensível” vamos identificar qual ou quais informações efetivamente importantes para o negócio participam do alcance do ativo ora mapeado.

1. Mapeamento de Vulnerabilidades:

|  |  |  |
| --- | --- | --- |
| Vulnerabilidade | Ameaça | Possíveis Impactos |
| Código Vulnerável | Hacker | Roubo de Dados do BD |
|  |  |  |
|  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Mapear Riscos é a próxima fase, a partir da identificação das vulnerabilidades existentes no escopo em estudo. Vulnerabilidades são elementos passivos, como por exemplo funcionários destreinados ou com excesso de direitos de acesso aos sistemas e dados, equipamentos expostos ao acesso físico de estranhos ou bugs em sistemas que possam ser explorados interna ou externamente. Já a ameaça é um elemento ativo, que pode explorar a vulnerabilidade mapeada. Um concorrente pode convencer um funcionário desmotivado a roubar dados; um hacker pode explorar os bugs dos sistemas, e um elemento estranho, não necessariamente de forma intencional, pode danificar equipamentos que estejam expostos. O impacto é o resultado da ação da ameaça na vulnerabilidade.

1. Análise CIDAL:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **C** | **I** | **D** | **A** | **L** |
| Ataque cibernético | **3** | **3** | **5** | **3** | **3** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Média: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Justificativas:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Na análise CIDAL, vamos agora avaliar um processo de negócio específico, em relação aos riscos evidenciados na fase anterior. Na segunda linha você identificará o incidente da segunda linha da tabela do item 3 deste trabalho e na terceira linha trará o terceiro incidente escolhido. Para cada um deles você avaliará qual a intensidade do dado para o negócio, à luz do significado da tabela da página 53 e do significado de cada atributo, que você encontra nos comentários das páginas 49 e 50. Atribua valores de acordo com a sua visão da extensão dos danos ao negócio para cada atributo. Ao final, calcule a média dos valores de CADA LINHA. Por exemplo, para a primeira linha do quadro, já preenchida como exemplo, a média é M1 = $\frac{3+3+5+3+3}{5}$ = 3,4. Calcule a média da segunda e da terceira linhas. Suponha que dê M2 = 2 e M3 = 4. Após isso, calcule a média das médias M = $\frac{M1+M2+M3}{3}$ = $\frac{3,4+2+4}{3}$ = 3,13. Este valor será usado no próximo passo.

1. Análise GUT:

|  |  |  |  |
| --- | --- | --- | --- |
| **Processo** | **Gravidade** | **Urgência** | **Tendência** |
| Loja Virtual |  |  |  |

Resultado: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Na análise GUT nós agregamos a urgência relativa em se restaurar cada processo afetado, quando submetido a um incidente. Um incêndio, por exemplo, demanda muito mais urgência na reação do que a perda de uma máquina, então deve ser priorizado. A Tendência agrega a antecipação de prioridade de um processo que talvez hoje não esteja com nível de sensibilidade alto, mas em função de planos e projetos estratégicos venha a se tornar mais sensível futuramente. Imagine uma empresa que está passando por um processo de fusão. Vários processos após a fusão ficarão mais sensíveis e outros talvez nem tanto. Para este trabalho considere que não há dados para análise de tendência, então vamos multiplicar por “1”, mas a urgência deve ser avaliada de acordo com a sua visão de agravamento do negócio com o passar do tempo em situação de impacto, multiplicando por “1” se você achar que há alta tolerância temporal, podendo a reação ser planejada sem pressa, “3” se a demanda por urgência é muito grande e “2” para uma situação intermediária. Na coluna GRAVIDADE você deve usar a tabela de conversão da página 57. Por exemplo, no CIDAL do exemplo tivemos um resultado final de “3,13” pontos, que na tabela de conversão está na faixa 2,4 ≤ C ≤ 3,7, que converte para “2”. Os números da tabela GUT estão sempre entre 1 e 3 e o valor de cada célula deve ser multiplicado.

1. Avaliação do Risco e Tipo de Ação a tomar:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Agora é a hora de usarmos o critério de aceitação de risco que definimos no item 1 deste trabalho. Se você achar que o risco é aceitável, bastarão apenas ações de controle do nível do risco. Escolha entre MODIFICAR, MANTER, ELIMINAR ou COMPARTILHAR. Se você considerar que o risco é INACEITÁVEL, além de indicar uma estratégia das 4 citadas acima, serão necessárias ações de Continuidade dos Negócios (um plano de contingências)

1. Esboço de DIRETRIZ de uma Política:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_DIRETRIZES são regras basais, cabíveis para qualquer colaborador, porém diretamente elaboradas para situações de risco evidenciadas durante o trabalho que fizemos. Identifique pontualmente um risco e descreva uma diretriz que servirá como uma regra para evitar que o incidente ocorra.

1. Ações de Continuidade dos Negócios:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Aqui você pode escolher entre ações de Administração de Crise, de Continuidade Operacional ou de Recuperação de Desastre, indicando qual foi a que você escolheu e dando um exemplo. Não esqueça que ações de Administração de Crise envolvem comunicação com os *stakeholders*, de continuidade operacional são focadas no processo e não nos ativos, e de recuperação de desastres são focadas nos ativos, mas também nas lições aprendidas

Envie este trabalho ao professor até a data combinada. Ele valerá de 0 a 10, comparado aos outros trabalhos de sua turma. Há uma cópia deste template em http://www.fredsauer.com.br.