

Estudo de Caso para a Utilização da Planilha de Gerencia de Riscos em SegInfo

Para a empresa de XPTO de Treinamento de Pessoal, foram obtidas as seguintes informações através de Entrevistas, Análise do Plano de Negócios, Reuniões com o Gestor, Testes de Invasão, técnicas de Engenharia Social, testes no Plano de Continuidade e nos controles da Política de Segurança e outros instrumentos, focando na coleta de elementos para a Análise de Riscos do PN Marketing e Contatos:

O seu Gestor, Sr. Xavier Moura, declarou trabalhar com um orçamento anual de R\$ 120.000,00 para o seu centro de custo, de onde são debitados todos os insumos, inclusive a remuneração de pessoal, para o funcionamento do PN em busca do atendimento das metas estabelecidas no Plano de Negócios pelo setor executivo. Seu PN encontra-se subordinado à Assessoria de Relações Públicas, que recebe as solicitações de alterações no orçamento e as encaminha (caso concorde) à vice-presidência Financeira da XPTO. Na análise técnica realizada pelos especialistas em auditoria de SegInfo, foram observadas as seguintes variáveis, já organizadas no formato adequado para a utilização da planilha de Gerência de Riscos v.5.1a, adaptada de um instrumento para Análise de Riscos em Projetos:

Amostra da Análise de Vulnerabilidades Realizada pela Equipe de Auditoria

Nº	Ativo	Tipo	Vulnerabilidade	Ameaça	Prob.	Custos do Impacto	Possível Controle/Contingência	Custo estimado da Reação
1	BD	Tecnológico	Controle de acesso lógico (disponibilidade/confidencialidade / integridade)	Próprio colaborador, concorrente	30%	R\$ 25.000,00	Hardening lógico, segregação física	R\$ 5.500,00
2	HD's	Físico	Ausência de redundâncias (disponibilidade)	Dano elétrico	15%	R\$ 15.000,00	Implementação de um RAID juntamente com estabilização	R\$ 3.000,00
3	HD's	Físico	Ausência de controle de MTBF e desempenho (disponibilidade)	Dano físico por desgaste temporal	5%	R\$ 15.000,00	Implementação de um controle via SNMP	R\$ 500,00
4	Servidores	Físico-Tecnológico	Inadequação da Segregação no acesso (confidencialidade/ integridade/ disponibilidade)	Próprio colaborador, concorrente	10%	R\$ 15.000,00	Implementação de um controle físico de segregação	R\$ 1.800,00
5	Servidores	Físico-Tecnológico	SO desatualizado (disponibilidade)	Vírus, worms e hackers	50%	R\$ 5.000,00	Compra de licenças e WSUS	R\$ 2.300,00
6	Gestor	Humano	Cultura de Segurança insuficiente (confidencialidade)	Gestor, concorrente (involuntário)	2%	R\$ 3.000,00	Treinamento e Políticas de Segurança	R\$ 500,00
7	Funcionários	Humano	Cultura de Segurança insuficiente (confidencialidade)	Próprio Colaborador, concorrente (involuntário)	15%	R\$ 3.000,00	Treinamento e Políticas de Segurança	R\$ 1.500,00
8	Funcionários	Humanos	Baixa remuneração (confidencialidade)	Próprio Colaborador, concorrente (voluntário)	5%	R\$ 3.000,00	Plano de Cargos e salários e Treinamento	R\$ 8.000,00
9	Ambiente de Trabalho	Físico	Controle do Acesso inadequado (confidencialidade)	Concorrente	5%	R\$ 3.000,00	Segregação física e controle de acesso	R\$ 1.800,00
10	Infra Telefônica	Físico	Alta dependência com inexistência de contingências (disponibilidade)	Surtos elétricos	15%	R\$ 1.500,00	No-break/estabilizador para a central telefônica	R\$ 1.200,00
11	Estações de Trabalho	Físico-Tecnológicos	Indisponibilidade de antivírus (disponibilidade)	Vírus, worms, malware	50%	R\$ 1.000,00	Compra, instalação e treinamento	R\$ 800,00
12	Estações de Trabalho	Tecnológicos	Senhas fracas (confidencialidade, integridade. e disponibilidade)	Concorrente	5%	R\$ 3.000,00	Treinamento e Policy	R\$ 500,00

Aba Abertura

Primeira Decisão: Foco em Resultado (custos + receita) ou em custos. Para o caso de SegInfo, o ideal é a Análise focada em custos, já que pretendemos verificar o quanto devemos investir na proteção dos ativos. Os demais campos são óbvios.

Aba Ameaças-Pré-reação

Esta planilha descreve os resultados da Auditoria de Riscos realizada, quando foram observadas as vulnerabilidades existentes no Processo de Negócios antes que qualquer contingência ou controle adicional aos já existentes seja implementado. São identificadas as potenciais ameaças em relação a estas vulnerabilidades e o efeito resultante (o incidente de segurança). Este evento deve ser complementado através de uma probabilidade, que deve ser obtida da forma mais técnica possível, de preferência através de dados reais de ocorrência na própria empresa ou em empresas similares. Apenas para exemplificar, no ramo de seguros de automóveis, a probabilidade é a estatística de ocorrências para o perfil do segurado (sexo, idade, bairro onde mora e locais que frequenta, possuir garagem ou não, etc.). O Impacto é uma estimativa dos custos para executar a contingência, ou seja, para as fases PAC, PCO e PRD, bem como eventuais impactos subjetivos tais como prejuízos para a imagem e a consequente perda de clientes.

Aba Oportunidades-Pré-reação

Uma “oportunidade” nada mais é do que um risco positivo, ou seja, um investimento que, uma vez realizado, terá um custo, mas pode trazer lucros ou redução de prazos no cumprimento de metas, aumento de produtividade e etc.

Análise de Oportunidades Pré-Reação

Não foram observados Riscos Positivos na Análise Pré-reação neste Estudo de Caso

Aba Valor Esperado-Pré-reação

É uma síntese do que foi obtido até então, agregando ao orçamento do PN os eventuais prejuízos com os impactos causados pelas ameaças e os resultados da ação bem-sucedida das oportunidades. Com isso, evidenciamos um “pior caso” – Todas as ameaças atuando, e o “melhor caso”, com as oportunidades ocorrendo com sucesso. A medida mais expressiva e interessante, no entanto, é a do Valor Esperado do PN com riscos, haja vista que é uma medida estatística que indica a situação mais provável de operação do PN durante o exercício financeiro, uma vez que é pouco provável que todas as ameaças se concretizem, porém é bem provável que algumas aconteçam.

Aba “Prioridade”

Esta é uma das principais funcionalidades da ferramenta GerenciaDeRiscos.xls para a Análise de Riscos em SegInfo. Como discutido durante o curso, sabe-se que não é viável a implementação de todos os controles e contingências por conta dos seus custos, e, mesmo que os recursos estejam disponíveis, é necessária uma ordem de

implementação passo-a-passo. Nesta aba, faremos a comparação item a item de prioridade, considerando-se probabilidades, custos impactantes e a sensibilidade do analista. Automaticamente, a Abas “Ameaças-Pré-reação” é atualizada com a prioridade aferida, e a aba “Reação-Ameaças” já insere os eventos em ordem de prioridade.

Aba “Reação-Ameaças”

Nesta aba temos um cálculo de extrema importância: o valor esperado para cada reação, que é o valor sensato, à luz das probabilidades indicadas e do impacto, para o investimento nas proteções. Qualquer coisa acima disso indica desperdício ou, na pior das hipóteses, a escolha de uma estratégia inadequada para o valor do ativo e a probabilidade do mesmo ser comprometido. Outro aspecto relevante é a escolha desta estratégia, que poderá ser:

- Aceitar (passiva ou ativamente)
 - Ativamente – estabelece-se um Plano de Contingências, sem adoção de controles para mitigar, transferir ou eliminar; ou
 - Passivamente – não se faz nada. Apenas “torce” para não ocorrer a falha.
- Mitigar – Minimizar eventuais prejuízos
- Transferir – Um eventual prejuízo é absorvido por terceiros – caso típico do seguro.
- Eliminar – bloquear as ameaças através de controles agressivos

De acordo com a estratégia adotada, deve-se então recalcular as probabilidades de ocorrência dos incidentes de segurança correspondentes, já que este é o objetivo vislumbrado com os investimentos em SegInfo.

Após a inserção dos controles e o recálculo das probabilidades, são inseridos os últimos esteios de garantia da funcionalidade dos PN: as contingências e seus respectivos custos.

Aba Reação-Oportunidades

Nesta aba são inseridos elementos de oportunidade planejados para inserção prévia no PN, bem como outros que possam servir para intensificar o efeito do risco positivo. No caso em estudo, não foram evidenciados elementos deste tipo, apesar de ser função do analista buscar tais elementos.

Aba Valor Esperado

Nesta aba sintetizamos todos os elementos da análise, possibilitando a tomada de decisão. Por exemplo:

- Necessidades para a execução de contingências;
- Reserva gerencial para eventualidades, inferior aos típicos 10% em função dos controles adotados, que reduzem a probabilidade da ocorrência de impactos e consequentemente a necessidade de reservas; e
- Agregação do custo dos impactos aos custos das contingências propostas.

A conclusão mais expressiva, no entanto é a do “Novo Valor Base do PN”, onde estão agregados ao orçamento do PN os custos dos novos controles planejados.

Abas “Ameaças, Oportunidades e Controle de Riscos”

Capturam o resultado final deste trabalho de Análise de Riscos, servindo como instrumento de tomada de decisão (onde investir ou não), como indicador da prioridade entre as ações e, finalmente, como fomentador do PDCA, já que periodicamente novas Análises de Risco podem ser feitas de forma mais simples e objetiva à partir do trabalho de análise anterior.

Prof. Dr. Frederico Sauer
fsauer@gmail.com