

Planejamento Estratégico da Segurança da Informação

SÃO PAULO - 2010



Apoio:

Microsoft®

Associações representadas no **Infosec Council**:



Instituto Brasileiro de Peritos



O InfoSec Council

O InfoSec Council foi criado em 2005, idealizado como uma reunião de profissionais de alto nível (“C-level”), cujas áreas de atuação implicam no estímulo, criação, manutenção e evolução de técnicas e estratégias voltadas à segurança da informação, aqui considerada em um espectro bem amplo.

Neste aspecto, estão compreendidas as disciplinas de:

- Tecnologia da Informação;
- Segurança da Informação;
- Segurança Corporativa;
- Auditoria de Sistemas;
- Governança de Tecnologia da Informação;
- *Compliance*;
- Recursos Humanos (voltado à segurança e auditoria).

Ainda que estes profissionais exerçam atividades em suas respectivas organizações – públicas, privadas e associativas –, sua participação se dá em caráter pessoal em função de sua comprovada e reconhecida experiência neste exercício.

O objetivo do InfoSec Council é atender às três comunidades-alvo (usuária, provedora e acadêmica) e contribuir e influenciar na evolução dos aspectos regulatórios da tecnologia e da segurança da informação.

Divulgação

Os direitos autorais deste documento são do InfoSec Council e devem ser respeitados nos termos da Lei 9.610, de 19/02/1998, em especial quanto ao artigo 46.

É autorizada a reprodução do todo ou de suas partes para uso acadêmico, devendo ser citada expressamente sua fonte. É vedada a reprodução ou armazenamento deste documento para fins comerciais, exceto em caso de autorização anterior, por escrito, do InfoSec Council. Nenhuma outra permissão ou direito são concedidos em relação a este documento.

InfoSec Council

security.advisor@live.com

www.infosecouncil.org.br

Profissionais membros do InfoSec Council

- **Astor Calasso** – Gerente Consultor – Governança, Auditoria e Segurança de TI
CONSIST Business Information Technology
- **Christiane Mecca** – Gerente de Segurança da Informação / Rhodia
- **Dioniso Campos** – Gerente de Segurança Corporativa / Nextel e VP / ABSEG
- **Djalma Andrade** – Gerente de Estratégias da Microsoft
- **Edison Fontes** – Consultor e Professor de Segurança da Informação
- **Fabiana Santos** – Analista de Marketing da Microsoft
- **Giuliano Giova** – Economista, Perito de TI e Diretor do IBP Brasil
- **Igor Pipolo** – *Chairman* da ABSEG
- **João Rufino de Sales** – Chefe da Assessoria de TI do DEC-Exército
- **Juliana Abrusio** – Advogada, especialista em Direito Eletrônico / Opice Blum Advogados Associados
- **Marines Gomes** – Gerente de Segurança da Microsoft
- **Mônica Orsolini** – Gerente de Infraestrutura da Promon Engenharia
- **Renato Opice Blum** – Advogado, especialista em Direito Eletrônico / Opice Blum Advogados Associados
- **Ricardo Castro** – Coordenador de Auditoria e Presidente da ISACA-SP
- **Ricardo Franco Coelho** – Coordenador Segurança-DF / Banco Central e VP / ABSEG
- **Valmir Schreiber** – CSO / Banco BNP Paribas e *Past President* da ISACA Capítulo SP

Autores

Mônica Orsolini

Formada em análise de sistemas, com mestrado em gerenciamento de sistemas de informação, é gerente de infraestrutura da unidade de sistemas da Promon Engenharia, empresa onde atua desde 1987, tendo trabalhado em várias áreas de TI. Sua principal missão é prover uma infraestrutura de TI segura e confiável para suportar os negócios da Promon.

Astor Calasso

Economista, gerente consultor da Consist Business Information Technology. Atua na área de tecnologia da informação (TI) há mais de 35 anos, gerenciando e implantando soluções de TI e de governança em empresas de grande porte, além de atuar como consultor em áreas corporativas estratégicas. Foi *chief information officer* (CIO) e *chief security officer* (CSO) da área corporativa da Accor Brasil (Ticket Serviços), acumulando as áreas de telecomunicação, consultoria interna e *shared services*. É membro da Comissão Organizadora do Congresso Nacional de Auditoria de Sistemas, Segurança e Governança de TI (CNASI) e membro fundador e vice-presidente do *InfoSec Council* (SP). Foi diretor da *Information Systems Audit and Control Association* (ISACA) em São Paulo nas gestões 2004 a 2006.

João Rufino de Sales

Coronel do Exército Brasileiro. Mestre em aplicações militares, especialista em segurança da informação, armamento e guerra eletrônica, atualmente exerce a função de chefe da assessoria especial de tecnologia da informação do Departamento de Engenharia e Construção do Exército Brasileiro. Foi membro do Comitê Gestor da Segurança da Informação, do Comitê Gestor de Chaves Públicas Brasileira, chefe da Seção de Internet

do Centro de Comunicação Social do Exército Brasileiro, onde foi responsável pela implantação do Provedor de Internet do Exército. Foi chefe do Grupo de Assessoramento Técnico do Gabinete de Segurança Institucional da Presidência da República e chefe do 3º Centro de Telemática de Área – São Paulo. É membro da Sociedade Brasileira de Engenharia de Rádio e TV e membro fundador do InfoSec Council.

Edison Fontes

Consultor, gestor e professor de segurança da informação, assunto ao qual se dedica desde 1989. Bacharel em informática pela Universidade Federal de Pernambuco (UFPE), instituição na qual fez especialização em ciência da computação, pós-graduado em gestão empresarial pela Fundação Instituto de Administração, da Universidade São Paulo (FIA/USP), e mestrando em tecnologia da informação pelo Centro Paula Souza, de São Paulo (SP). É autor dos seguintes livros:

- *Praticando a Segurança da Informação*, Editora Brasport, 2008.
- *Segurança da Informação: O Usuário faz a Diferença*, Editora Saraiva, 2006.
- *Vivendo a Segurança da Informação*, Editora Sicurezza, 2000.

Christiane Mecca

Gerente de segurança da informação da Rhodia. Analista de sistemas com mais de 20 anos de atuação em tecnologia da informação (TI), possui larga experiência em segurança da informação, *e-commerce* e redes. Graduada em análise de sistemas, pós-graduada em marketing e MBA em engenharia da qualidade, atua também como auditora ISO 9001.

Alvaro Teófilo

Administrador de empresas, com 15 anos de experiência no mercado financeiro, com foco na gestão de segurança digital e combate à fraude eletrônica. Foi CSO do Grupo Caixa Seguros e Business Security Officer do Citigroup. Atualmente, é superintendente do Centro de Serviços de Segurança Gerenciados na Produban, empresa de TI do Grupo Santander. Foi professor do curso de Gestão de Segurança da Informação da Universidade Euro-Americana, em Brasília (SF), e professor-convidado do Curso de MBA em TI da Fundace-USP, em Ribeirão Preto (SP). Já escreveu artigos sobre segurança para a Gazeta Mercantil, KPMG Business Magazine, Microsoft Business Magazine, TI Inside, entre outras publicações. É também palestrante, tendo realizado apresentações em 2009 no CERT-Forum, em São Paulo (SP), e no Security Summit 2009, organizado pela Revista The Economist, em Washington, DC (Estados Unidos).

Valmir Schreiber

Profissional com mais de 25 anos nos segmentos de informática e segurança da informação. Atualmente é *Chief Security Officer* (CSO) do Banco BNP Paribas Brasil. Graduado em matemática e pós-graduado em segurança da informação; possui certificado *Certified Information Security Manager* (CISM) pela *Information System Audit and Control Association* (ISACA); certificado em *Information Technology Infrastructure Library* (ITIL Foundation); representante da Associação Brasileira de Bancos Internacionais (ABBI) no Banco Central para o grupo de trabalho de segurança do Sistema de Pagamento Brasileiro (SPB); membro do InfoSec Council do Brasil; premiado em 2004, 2005, 2006 e 2007 entre os 50 mais influentes *Security Officer* pela revista IT Intelligence Magazine. Foi Presidente da ISACA capítulo São Paulo nos anos de 2005, 2006 e 2007. Atua no mercado em palestras sobre gestão de riscos tecnológicos, governança de TI e conscientização da segurança da informação.

André Pitkowski

Consultor sênior em governança corporativa e de TI, avaliação de riscos e projetos de compliance (GRC) há mais de 15 anos. Possui MBA em governança de TI pela Fundação IPT, é certificado CGEIT (Cer-

tified in the *Governance of Enterprise IT*) pela ISACA, onde atua como diretor do capítulo São Paulo desde 2003 e é coordenador da ISACA-EUA para o *Risk IT Framework*. É certificado OCTAVE pela *Software Engineering Institute* (SEI), da Carnegie Mellon University (CMU), de Pittsburg (EUA). É ainda auditor líder em ISO 31.000, *framework* de riscos corporativos. Atualmente, gerencia projetos para avaliação de riscos em ativos críticos, mapa de riscos de TI e projetos para governança de TI e compliance em empresas nacionais e internacionais, realiza palestras em âmbito internacional e é professor universitário de pós-graduação e MBA.

Ricardo Castro, CISA CFE

Coordenador de auditoria interna no grupo Hamburg-Süd de Navegação e Logística e presidente da *Information Systems Audit and Control Association* Capítulo São Paulo (ISACA-SP). Profissional com mais de 11 anos de experiência nas áreas de segurança da informação, gestão de riscos, auditoria e investigação de fraudes corporativas. Graduado em tecnologia e processamento de dados pela Universidade Presbiteriana Mackenzie e pós-graduado em análise e projeto de sistemas. Foi o primeiro brasileiro a receber o Prêmio *ACFE Outstanding Achievement Awards*, concedido pela *Association of Certified Fraud Examiners* norte-americana por suas contribuições no combate às fraudes corporativas. É palestrante e professor em cursos de MBA e pós-graduação nas disciplinas de governança e gestão de riscos, auditoria, investigação e prevenção de fraudes, introdução à forense computacional e gestão por processos.

Renato Opice Blum

Advogado e economista; Coordenador do curso de MBA em Direito Eletrônico da Escola Paulista de Direito; Professor convidado do Curso "Electronic Law" da Florida Christian University, Fundação Getúlio Vargas, PUC, FIAP, Rede de Ensino Luiz Flávio Gomes (LFG), Universidade Federal do Rio de Janeiro, FMU e outras; Professor palestrante/congressista da Universidade Mackenzie, FMU; Professor colaborador da parceria ITA-Stefanini; Árbitro da FGV, da Câmara de Mediação e Arbitragem de São Paulo (FIESP); Presidente do Conselho Superior de Tecnologia da Informação da Federação do Comércio/SP e do Comitê de Direito da Tecnologia da AMCHAM; Membro da Comissão de Direito da Sociedade da Informação – OAB/SP; Vice-Presidente do Comitê sobre Crimes Eletrônicos – OAB/SP; Coordenador e coautor do livro "Manual de Direito Eletrônico e Internet"; Sócio do Opice Blum Advogados; Currículo Plataforma Lattes: <http://lattes.cnpq.br/0816796365650938>.

Juliana Abrusio

Sócia da Opice Blum Advogados Associados, é advogada atuante na área de Direito Eletrônico. Mestre pela Universidade de Roma II, é professora da Faculdade de Direito Mackenzie e da Pós-Graduação em Computação Forense desta mesma instituição. É membro do Conselho de Comércio Eletrônico da Federação de Comércio (SP) e co-coordenadora da obra *Manual de Direito Eletrônico e Internet*, da Editora Lex.

Giuliano Giova

Executivo e profissional de processamento de dados há mais de 30 anos. Economista, perito judicial em questões de tecnologia da informação (TI) e telemática, diretor do Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática (IBP Brasil), instrutor e palestrante a respeito de perícia em TI, som, imagem e crimes perpetrados por meios eletrônicos.

Sumário

Apresentação	10
Capítulo 1	
Sistema de gestão de segurança da informação	11
Mônica Orsolini	
1. Patrocinadores e comitê	11
1.1. Conceito-chave	11
1.2. Mecanismos de controle	11
1.2.1. Métricas	11
1.2.2. Definição	12
1.2.3. Tipos de métricas	12
1.2.4. Coleta de resultados	13
1.2.5. Fatores-chave de sucesso	13
Capítulo 2	
Participação do negócio no PESI	14
Astor Calasso	
1. A responsabilidade dos gestores no PESI	14
2. Quem paga pela segurança?	15
3. Como fazer a segurança?	15
4. Segurança interna ou <i>outsourcing</i> ?	15
5. Quem é o comitê do PESI?	16
6. Quais riscos e vulnerabilidades devem ser tratados?	16
7. O papel da administração e dos investidores	17
Capítulo 3	
Gestão de riscos	18
João Rufino de Sales	
Capítulo 4	
Aspectos tecnológicos, humanos e financeiros	20
Edison Fontes	
1. Introdução	20
2. Definições	20
2.1. Aspectos sociais	20
2.2. Aspectos técnicos	20
3. Planejamento da segurança da informação	20
4. Aspectos sociais	22
4.1. Regulamentos	22
4.2. Cultura organizacional	22
4.3. Clima organizacional	22
4.4. Processo contínuo de treinamento	23
4.5. Profissionalismo	23

5. Aspectos técnicos	23
5.1. Atualização da tecnologia	23
5.2. O fornecedor da solução.....	23
5.3. Requisitos de segurança devem ser mantidos.....	24
6. Aspectos financeiros.....	24
7. Conclusão	24

Capítulo 5

Serviços internos.....	25
-------------------------------	-----------

Christiane Mecca

Capítulo 6

Provedores externos.....	26
---------------------------------	-----------

Álvaro Teófilo

1. Introdução.....	26
2. Gestão de parceiros de negócios.....	26
3. Quem, quando e o que avaliar.....	26
4. Avaliando e monitorando o risco.....	27
5. Implantando o processo	27

Capítulo 7

Melhores práticas.....	29
-------------------------------	-----------

Valmir Schreiber e André Pitkowski

1. Introdução.....	29
1.1. As dimensões.....	29
1.2. Os mecanismos.....	29
2. CobiT	30
2.1. Um modelo unificado	30
3. ITIL.....	31
3.1. ITIL – uma visão geral.....	31
4. CobiT e ITIL agregando resultados.....	31
4.1. Combinando CobiT e ITIL para atingir os desafios dos negócios.....	31
4.2. Combinação de modelos.....	32
5. COSO.....	32
6. CBK.....	33
7. Associações.....	34
7.1. ISACA.....	34
7.2. ISSA.....	34

Capítulo 8**Gerenciamento de mudanças** 35**Ricardo Castro**

1. Mudanças como causas de incidentes 35
2. Desafios na gestão de mudança 35
3. Gestão de mudanças segundo o CobiT® 36
4. Mantendo os riscos sob controle 37
5. Medindo a eficiência dos controles 37
6. Pergunta para pensar 38

Capítulo 9**Aspectos jurídicos do PESI** 39**Renato Opice Blum e Juliana Abrusio**

1. Introdução 39
2. A estratégia da organização frente às normas de segurança 39
3. Conformidade com requisitos legais 39
4. Regulamento Interno de Segurança da Informação 40
5. Termo de Uso da Segurança da Informação 40
6. Monitoramento de *e-mails* 40
7. Responsabilidades 41
8. Implementação 42

Capítulo 10**Computação forense** 44**Giuliano Giova**

1. O poder do faraó 44
2. Milhares de anos depois 44
3. E hoje? 45
4. Revisitando o velho conflito de interesses 46
5. Computação forense 47
6. Princípio de Locard 48
7. Heisenberg e a física quântica 48
8. Cadeia de custódia 48
9. Quesitos 49
10. Exames técnicos 49
11. Laudo pericial 50
12. Finalmente 50

Apresentação

À medida que a tecnologia representa cada vez mais um componente importante e preponderante dos negócios – em muitos casos, é parte integrante dos próprios produtos e serviços oferecidos –, não é permitido que as organizações descuidem do controle adequado e metucioso de seus processos. Caso contrário, elas terão perda expressiva de capacidade de operação nos seus mercados e da credibilidade de sua administração.

Durante diversos eventos, em que participamos como membros do InfoSec Council ou em decorrência das nossas atividades profissionais, de forma recorrente somos confrontados com questionamentos referentes à forma de criação, elaboração e estabelecimento de um Planejamento Estratégico de Segurança da Informação (PESI).

As questões levantadas são multidisciplinares e frequentemente referem-se a:

- Metodologias empregadas;
- Cuidados considerados;
- Envolvimento da alta administração;
- Formas de *funding* e custeio;
- Gestão de riscos e vulnerabilidade dos processos;
- Determinações legais e regulatórias;
- Gerenciamento da execução.

Em face desta demanda, o InfoSec Council resolveu, em suas reuniões periódicas, que deveria propiciar à nossa comunidade um material para servir como guia e consulta para esta tarefa. Assim, seus membros foram alocados para compilar suas experiências, lições aprendidas e, por que não, dificuldades enfrentadas e até os erros cometidos.

Este material foi consolidado neste documento, cuja finalidade é fornecer informações, sugestões e alertas sobre uma forma de atingir o objetivo maior: mobilizar todas as áreas das organizações em torno de um tema fundamental. Portanto, não é nossa ambição estabelecer aqui um formato final e definitivo sobre a matéria. Neste sentido, trata-se da soma das experiências vividas, ajustadas a uma pesquisa de melhores práticas, buscando traçar recomendações e direções a serem observadas na elaboração do PESI.

A quem se destina este documento

Este trabalho é endereçado à gerência executiva e aos profissionais responsáveis pelos controles e pela informação, incluindo gestores de SI e de TI e aos profissionais de auditoria, apoiando-os na avaliação dos ambientes da informação.

Particularmente, recomendamos também sua leitura ao *board* das organizações.

Agradecimento

O InfoSec Council deseja agradecer às Organizações e Empresas em que os seus Membros atuam, pelo estímulo e motivação que proporcionam aos seus Executivos. O InfoSec Council também agradece à Consist pelo apoio editorial na impressão deste *paper*.

Agradecemos, também, ao inestimável apoio de:

Fabiana Santos – Analista de Marketing da Microsoft

Marcelo Melro – LAM Solutions Consulting Manager / Siemens Enterprise Communications

Capítulo 1

Sistema de gestão de segurança da informação

Mônica Orsolini

1. Patrocinadores e comitê

A escolha dos “patrocinadores” é fundamental para o sucesso da implantação de um Sistema de Gestão de Segurança de Informação (SGSI) em uma organização. É por meio deles que se obtêm o respaldo para a implantação do SGSI, tornando viável a tomada de ações decorrentes da aplicação do sistema. Geralmente, são escolhidos como patrocinadores profissionais da alta direção da organização, além de outras pessoas-chave da área do negócio.

Estas pessoas devem formar um comitê, comumente chamado de Grupo Gestor de Segurança da Informação (GGSI), que tem como meta a manutenção do SGSI na organização. Entre as atribuições deste grupo, está a criação da “Política de Segurança da Informação”, bem como os procedimentos que decorrem dela e a aplicação de eventuais sanções, que devem ser aplicadas de forma imparcial a qualquer colaborador que infrinja a política estabelecida, não importando seu grau hierárquico. Para que esta premissa possa ser cumprida, entretanto, é necessário que o GGSI tenha influência suficiente para sensibilizar os colaboradores dos riscos envolvidos no não-cumprimento da política.

Porém, vale destacar que a segurança da informação é uma questão cultural, de aprendizado e de processos. Por isso, as sanções devem ser aplicadas à medida que o sistema torna-se consistente, de conhecimento de todos, e a partir do momento em que a curva de aprendizado se mostrar favorável. Este é um processo lento e que exige muita dedicação do GGSI.

1.1. Conceito-chave

Sanções: regras têm de ser cumpridas e, a cada não-cumprimento, uma sanção pode ser aplicada. Todas as regras devem ter os riscos associados ao seu não-cumprimento muito bem documentados, bem como têm necessidade de deixar claras as sanções possíveis de aplicação.

Perguntas para pensar:

- Você escolheu um “patrocinador” que poderá dar respaldo adequado ao projeto?
- Seu “patrocinador” apoiará as sanções contra qualquer membro, caso ele mesmo cometa alguma irregularidade?
- O “patrocinador” é um dos maiores interessados no sucesso do projeto?

1.2. Mecanismos de controle

“Não se gerencia o que não se mede, não se mede o que não se define, não se define o que não se entende, não há sucesso no que não se gerencia” (William Edwards Deming).

1.2.1. Métricas

Em vista da diversidade de atividades executadas, quando se desenvolve e implanta um SGSI, naturalmente este processo implica ao gestor responsável pela missão a necessidade de gerenciar diversos mecanismos de controles implementados em diversas plataformas e em vários ambientes organizacionais. Dependendo do número de pessoas, processos e tecnologias envolvidas, esta atividade pode se tornar árdua, devido à quantidade e à diversidade de elementos a serem monitorados.

Surge, então, a necessidade iminente de responder algumas questões:

- Como podemos saber se o nível atual de segurança está no patamar requerido para o nosso negócio?
- Como medir o nível de eficácia dos controles atuais frente aos riscos identificados?

Uma boa estrutura de métricas permite avaliar a efetividade de um SGSI. Mas, para se chegar a este nível, a organização precisa desenvolver um plano de métricas, que deve incluir a forma de coleta, o repositório, os

procedimentos para retenção e a forma de avaliação, entre outras. O primeiro passo é compreender quais são os objetivos a serem atingidos e, a partir disto, desenvolver métricas que satisfaçam estes objetivos.

Medir a eficácia de um SGSI está longe de ser uma tarefa fácil. Para tanto, estratégias devem ser elaboradas para monitorá-la, resultando em informações que façam sentido e auxiliem os tomadores de decisão. Em muitos casos, a falta de tempo, conhecimento e a adoção de uma estratégia inadequada para a criação de métricas podem prejudicar o SGSI.

Por outro lado, como o SGSI é muito dinâmico. Métricas bem definidas ajudam a visualizar a situação atual, bem como auxiliam a realização de simulações e o desenvolvimento das melhorias necessárias. É preciso manter o SGSI vivo e em constante evolução.

1.2.2. Definição

Métricas em um SGSI são medidas estipuladas com base em metas a serem atingidas, as quais são comparadas aos resultados obtidos durante a sua operação de um SGSI. Contudo, isto não invalida a importância de comparar os resultados alcançados anteriormente, pois, desta forma, é possível vislumbrar tendências e avaliar o amadurecimento de seu SGSI. Esta análise de tendência ajudará a organização a se precaver e tomar medidas preventivas para a correção de determinados desvios.

Um método bastante importante no SGSI é o *Benchmarking*. Ele é usado para se comparar o desempenho de algum processo a outro similar, de outra organização, que esteja sendo executado de maneira mais eficaz e eficiente.

1.2.3. Tipos de métricas

Mediante uma diversidade de métricas, devemos escolher as mais adequadas a cada caso. Algumas podem ser utilizadas (mas não se limita a estas) para medir eficácia, eficiência, tempo, produtividade, qualidade, performance e confiabilidade do SGSI.

Como exemplo de acompanhamento das métricas, podemos citar:

- *Benchmarking* de pesquisas de sobre segurança da informação;
- Resultados de pesquisas internas de avaliação do SGSI;
- Gestão de incidentes de segurança.

Independente da diversidade dos tipos de métricas existentes, a organização deve selecionar aquelas que lhe forneçam informações relevantes de seu SGSI, conforme citado anteriormente. A seguir, apresentamos uma tabela com as informações mínimas, porém, necessárias, para se criar um plano de métricas.

Tabela 1 – Passo a passo para o estabelecimento de métricas.

Métrica	Este campo deve conter o nome da métrica e a descrição da escala que será usada.
Escopo da métrica	Este campo descreve o que deve ser medido. Por exemplo: o processo ou controles do ISMS e quais partes do processo ou controles.
Propósito e objetivo	Este campo deve definir o propósito da métrica, quais as metas e objetivos devem ser atingidos
Método de medição	Este campo deve descrever como a medição será realizada, por exemplo, usando cálculo, fórmula ou porcentagens.
Frequência da medição	Este campo deve descrever a periodicidade da medição. Por exemplo: mensal, semanal, diário etc.
Origem dos dados e procedimento de coleta	Este campo deve definir de onde os dados serão coletados e quais métodos são usados para a coleta.
Indicadores	Este campo deve conter os indicadores usados para otimizar a métrica e definir o seu propósito e como eles são entendidos e podem ser aplicados.
Data da medição e responsável	Este campo deve descrever a data da medição e a pessoa responsável por esta ação.
Nível da efetividade alcançada	Este campo deve conter o resultado e a data da medição
Causas do não-cumprimento	Este campo deve conter as causas do não-cumprimento dos objetivos, indicadores etc.

Fonte: "Measuring the effectiveness of your ISMS".

1.2.4. Coleta de resultados

A atividade de medir demanda recursos e, obviamente, tempo para a coleta e análise dos resultados. Por esta razão, as métricas devem fazer sentido e ser coerentes, além de alinhadas aos objetivos a serem alcançados. Como nem todos os resultados podem ser coletados automaticamente, é importante determinar a melhor forma de fazê-lo, principalmente quando o envolvimento de outras áreas se faz necessário e a coleta tem de ser realizada manualmente.

Alguns processos eventualmente são executados e os registros coletados e armazenados em outra localidade. Independente disto, o resultado deve ser coletado e consolidado em um único repositório.

1.2.5. Fatores-chave de sucesso

Destacamos alguns fatores que devem ser gerenciados adequadamente para que a organização consiga desenvolver métricas adequadas e que ajudem a monitorar de forma mais assertiva o seu SGSI.

- Conhecer o objetivo a ser alcançado;
- Conhecer as metas a serem alcançadas;
- Coletar os resultados em tempo hábil;
- Apresentar resultados válidos e confiáveis;
- Criar métricas que permitam monitorar o SGSI;
- Desenvolver metas desafiadoras.

É de fundamental importância que os fatores-chave de sucesso sejam identificados e documentados para que a organização consiga administrá-los. Por fim, é notória a importância do estabelecimento de métricas, para que seja possível vislumbrar a efetividade de qualquer SGSI. Sem elas, o gerenciamento passa a ser realizado de forma pontual, com muitas ações sem foco e, em alguns casos, sem critérios definidos.

A gestão que utiliza um sistema de métricas permite não apenas uma visualização rápida da situação atual, mas, também, contribui para uma tomada de decisão mais assertiva.

Bibliografia

HUMPHREY, Ted, PLATE, Angelika. *Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001*. London: BSI Standards, 2006.

NIST SPECIAL PUBLICATION. *Security Metrics Guide for Information Technology Systems*. 800-55, July 2003.

PAYNE, Shirley. "A Guide to Security Metrics". *SANS Security Essentials GSEC Practical Assignment*, Version 1.2e, July 2004.

Capítulo 2

Participação do negócio no PESI¹

Astor Calasso

“Quem conhece os outros é inteligente. Quem conhece a si mesmo, é iluminado”.

(Tao Te King – Lao Tzu)

“Predição é algo muito difícil. Especialmente sobre o futuro”.

(Niels Bohr, Nobel de Física-1922)

“Nós somos o que repetidamente fazemos. Excelência não é um ato, mas um hábito”.

(Aristóteles)

“A premissa fundamental da gestão de riscos corporativos é que cada organização existe para proporcionar VALOR aos seus investidores. Todas as organizações enfrentam incertezas, e o desafio para os seus gestores é determinar o quanto de incerteza deve ser aceita, uma vez que dificultam o crescimento de valor aos investidores.

A incerteza apresenta tanto riscos quanto oportunidades, com potencial para destruir ou aumentar o valor. A gestão dos riscos propicia aos gestores lidar efetivamente com a incerteza e os riscos e oportunidades associados, reforçando a capacidade de criar valor.

O valor é maximizado quando os gestores estabelecem a estratégia e os objetivos para atingir o equilíbrio ideal entre as metas de crescimento / retorno e os riscos a elas relacionados, empregando os recursos de forma eficiente e eficaz para a consecução dos objetivos da Organização (COSO – *Committee of Sponsoring Organizations of the Treadway Commission*)”.

A citação acima dá início ao Sumário Executivo do *Enterprise Risk Management – Integrated Framework*, editado e distribuído pelo COSO. Estas afirmações exprimem, em suas essências, o papel fundamental e indelégável da diretoria e dos gestores de todas as organizações. Deve-se notar que nenhuma designação é feita a funções específicas, referindo-se aos “gestores” de forma generalizada.

1. A responsabilidade dos gestores no PESI

De fato, esta responsabilidade repousa por inteira sobre os ombros do board gestor. Ainda que a execução de determinadas ações sejam atividades delegadas a uma área especializada (por exemplo, ao CSO – *Chief Security Officer*), o estabelecimento de seus objetivos e limites é responsabilidade de todos os gestores. À área delegada cabe o papel de implantar tecnicamente, observando a execução e a realização da estratégia (“fazer-fazer”) e, com a autoridade associada à responsabilidade que recebeu, atuar para seu correto direcionamento e efetividade. E isto é fundamental: a área delegada tem a responsabilidade e, na mesma medida, autoridade recebida do board sobre os eixos estratégicos a ela atribuídos.

Entretanto, como reza a boa prática na delegação de poderes, “todas as tarefas podem ser delegadas, mas nenhuma tarefa pode ser delegada por inteiro; a porção que fica com quem delega constitui o ponto de controle”.

É o negócio quem tem as medidas exatas dos riscos a que estão expostos e, da mesma forma, quais incertezas, na sua justa medida, devem ser prevenidas (ou aproveitadas) para a geração de melhores negócios e o atendimento diferenciado de seus mercados. Nem mais, nem menos. Outra vantagem expressiva deste envolvimento é que, ao entender a exata aplicação das medidas, os gestores do negócio poderão também apresentar ao seu mercado esta segurança como um benefício adicional agregado aos seus produtos e serviços.

¹Plano Estratégico de Segurança da Informação.

2. Quem paga pela segurança?

Atualmente, é inaceitável a situação muitas vezes encontrada, em que, de um lado, a gestão de riscos deve cobrir vulnerabilidades de tecnologia da informação (TI) ou de processos e, ao mesmo tempo, não consegue recursos para implantar seus projetos. Ora, se é fundamental que o negócio estabeleça a organização e o comportamento frente aos riscos, é ele quem deve prover seus recursos e, a partir daí, cobrar pelo seu correto emprego. E isso, sem qualquer dúvida, é parte integrante do custo do negócio. A ideia de que “custos de TI e da segurança são destas áreas e não do negócio” é uma forma inconsistente de administrar. São custos que o negócio deve arcar, considerando a evolução no curto, médio e longo prazos. Mas é importante não perder de vista que a aplicação, a existência e a extensão da segurança deve ser uma imposição estratégica da organização.

Em resumo, é saudável considerar que o setor de segurança da informação é uma área de “custo zero”, em que suas despesas e investimentos são repassados às demais áreas, produtos ou filiais da organização. Desta forma, melhora a percepção de todos de que é obrigatória a gestão do risco e a segurança da informação e que isto é responsabilidade de todos. Aliás, esta cultura é saudável também quando aplicada a toda a área de TI.

3. Como fazer a segurança?

Não raro, nos deparamos com situações em que os projetos são estabelecidos em função apenas de alertas do mercado, principalmente de consultores e fornecedores. Não que eles sejam errados ou perniciosos, mas é comum que, apenas vindos de fora para dentro da organização, não enderecem adequadamente as reais características demandadas ou suportadas pelo negócio. Exploram, em muitos casos, as técnicas de *fear, uncertainty and doubt* (FUD, sigla em inglês para designar “medo, incerteza e dúvida”). Projetos assim, no mais das vezes, resultam em custos e esforços desproporcionais às necessidades reais – ou muito grandes, implicando ociosidade, ou muito pequenos, implicando em grande vulnerabilidade residual.

Estes projetos acabam ficando no campo da capacidade política e de convencimento dos gestores de risco, simplesmente aceitos pelos demais gestores de forma passiva, acreditando somente na argumentação apresentada (fenômeno conhecido no campo comportamental como “O paradoxo de Abilene”, um fenômeno no qual um grupo de pessoas se vê forçado a agir de forma oposta às suas convicções).

Na melhor das hipóteses, esta prática representa apenas pura perda de esforços, tempo, credibilidade e, finalmente, dinheiro. Nestes casos, quando os problemas acontecem, invariavelmente toda a responsabilidade recai sobre o CSO. Cada organização deve estabelecer, à luz de suas características próprias, da evolução prevista, de novos negócios planejados e dos *benchmarks* que lhe fazem sentido, as melhores práticas a serem seguidas e qual será a medida da aversão ao risco a ser observada. O contrário implica em corte arbitrário dos recursos a cada vez que o negócio enfrente percalços, não havendo certeza do emprego adequado dos recursos.

4. Segurança interna ou *outsourcing*?

O cenário que tratamos até aqui diz respeito à política a ser empregada na segurança e deve ser considerado sem importar qual modelo operacional a ser praticado. Mesmo quando falamos em *outsourcing*, estas questões devem ser adequadamente endereçadas, para que o baseline a ser contratado seja o mais realista possível. Afinal, *outsourcing* não significa transferência de responsabilidade, apenas uma delegação da atividade operacional.

Da mesma forma, a decisão por *outsourcing* apenas pela ótica da redução de custos pode mostrar-se perigosa em todas as situações, mas, particularmente, no que tange à segurança da informação. É preciso ter em mente dois aspectos:

- Terceirizar aquilo que não se domina ou apenas por ser mal feito internamente pode significar insucesso e maiores custos;
- O período imediatamente anterior à contratação do *outsourcing* é um momento privilegiado para a reorganização do processo a ser terceirizado.

A redução de custos, neste cenário, poderá, então, ser mais facilmente atingida, de uma forma mais consistente, resultando em que o que for contratado seja realmente o *baseline* necessário: nem tão pequeno que gere não-qualidade, nem tão grande que signifique custos indevidos (ociosidade).

Dentro disso, outro aspecto desta mesma situação é o caso frequente que acontece quando é definido o fornecedor antes da escolha do processo ou da solução adequada, também conhecida como “Síndrome da Grife” ou “Efeito Manada”. Esta inversão da ordem de escolha é uma prática recorrente, citada pelo Gartner como sendo uma das fontes de problemas na gestão da segurança (e da TI como um todo). Nestes casos, é comum que a organização seja adaptada à solução, quando o correto é o contrário. Depois de escolhido o fornecedor, é muito difícil mudar alternativas e até mesmo definir os SLA (*Service Level Agreement*, ou acordo de nível de serviço) convenientes, pois as atividades serão desenvolvidas apenas segundo as práticas deste fornecedor, ou “amarradas” ao *baseline* contratado.

Como qualquer investimento, os projetos propostos no PESI devem prover sempre a análise de ROI (*return on investment*, ou retorno sobre o investimento), seja financeiro ou intangível. Para que esse retorno seja efetivo, é imprescindível que os benefícios sejam mensurados e determinados pelo negócio, segundo sua visão da taxa interna de retorno aceitável. E vale repetir o alerta: os gestores de riscos não devem procurar sozinhos os índices de retorno adequados; de novo, é o negócio quem pode formular as melhores condições.

5. Quem é o comitê do PESI?

Embora já mencionado em outro capítulo deste documento, vale aqui seu reforço. Um aspecto importante quando falamos da participação do negócio no PESI é deixar bem claro que os gestores envolvidos são aqueles da “linha de frente” da organização, aqueles que atendem diretamente aos processos. Mas eles devem ser secundados e fundamentados pelas equipes de auditoria, departamento jurídico, *compliance*, TI e segurança (de TI e corporativa). Em todos os casos, também a área de recursos humanos (RH) deve participar, uma vez que o comportamento do quadro de colaboradores é um importante elemento de mitigação de riscos. E como um plano só é bom quando é conhecido, compreendido e abraçado por toda a organização, deve-se considerar a mobilização do marketing e da comunicação social para sua divulgação e conhecimento, desenvolvendo ações de endomarketing adequadas a cada organização.

Quanto ao patrocinador, a sugestão é que seja, na medida do possível, o responsável maior da organização (CEO – *Chief Executive Officer* ou presidente etc.). Uma alternativa é ter sua nomeação feita pelo órgão a que a organização esteja subordinada, como conselho de acionistas, conselho curador etc.

Ainda segundo o COSO, no Sumário Executivo acima citado, esta participação visa estabelecer ações conjuntas e harmônicas no sentido de:

- Alinhar a aversão ao risco e a estratégia necessária;
- Melhorar as decisões de resposta aos riscos;
- Reduzir os imprevistos operacionais e as perdas;
- Identificar e gerenciar riscos múltiplos e cruzados na organização;
- Aproveitar as oportunidades em um ambiente proativo;
- Otimizar o emprego de capital / investimentos.

6. Quais riscos e vulnerabilidades devem ser tratados?

A análise das origens dos riscos é um aspecto importante e fundamental a ser considerado. Correntemente, a segurança da informação é tratada como uma das atividades ligadas, de uma forma ou de outra, à própria TI. Neste caso, o que se vê é o tratamento técnico destas ameaças, provendo-se o ambiente de poderosas ferramentas para evitarmos os “ataques externos”, tais como Firewalls, IDS, antivírus etc. Claro, este tipo de ferramenta é fundamental e, infelizmente, continuará a ser. Entretanto, atenção especial deve ser dada às ameaças internas, em que usuários, utilizando operações legítimas e que fazem parte de seu trabalho normal, causam danos às vezes maiores (e quase sempre recorrentes) do que os ataques externos. Estes casos, que incluem vazamento de informações, perda de capital intelectual, fraudes etc., causam prejuízos irreparáveis à organização, tanto em termos de expressivas perdas financeiras como (pior) de imagem. O importante é que

estes riscos e vulnerabilidades quase nunca são objeto de consideração pela área técnica, mas são fontes de enorme preocupação por parte dos gestores do negócio e, em última análise, pelos gestores maiores – CFO (*chief financial officer*), COO (*chief operating officer*), CTO (*chief technical officer*), CCO (*chief compliance officer*) etc., inclusive do CEO.

Além das questões organizacionais relativas aos riscos derivados do negócio, há que se preparar também para as questões regulatórias. Mais e mais surgem (e surgirão) regras impostas para a condução das organizações, em função da crescente interdependência dos mercados globais e da proteção necessária aos investidores e *stakeholders*. Neste aspecto, a organização deverá estar preparada para outro tipo de risco, não menos importante: as questões de *compliance*. E aí surgem novas condições: as organizações devem, sistematicamente, adequar-se a diversas regras de natureza e origens diferentes. Como exemplo, temos as regras internacionais, as dos países de origem, as do país de operação (estas duas conhecidas como questões *home-host*), as estabelecidas pelos segmentos em que operam, além das próprias regras internas. Todas estas regulações são dirigidas diferentemente (às vezes de forma quase conflitante) a todas as áreas da organização: administrativa, financeira, operacional, comercial, logística, produção etc. A inobservância de apenas uma delas pode ser fatal a todo o empreendimento, sendo, portanto, uma enorme questão de RISCO.

7. O papel da administração e dos investidores

Neste processo, os responsáveis diretos pela segurança deverão desempenhar um papel que vai além da simples coleta de informações para a tomada de decisão, pois deve apresentar um modelo com escopo definido e sugerir critérios para que o processo decisório seja estruturado e não apenas baseado em um evento. Como os riscos, invariavelmente, são maiores do que os recursos disponíveis, o colegiado de gestores deverá, então, definir o que será feito e suas prioridades frente às realidades atuais e das tendências do negócio. Apenas assim é possível defender, junto à direção da organização e aos investidores, a alocação de recursos para sua realização e a obtenção da força e autoridade indispensáveis na sua condução.

Um processo decisório estruturado e conjunto permitirá:

- Alinhar a visão dos gestores quanto aos aspectos estratégicos e sua importância;
- Elencar critérios qualitativos e quantitativos das diversas áreas;
- Decisões consistentes, baseadas em regras claras e de consenso;
- Otimização dos recursos em função da própria evolução do negócio (análise estratégica dos cenários);
- Priorizar os projetos de forma consistente e estruturada;
- Comunicar a decisão e seus critérios de forma adequada a todo o corpo da organização;
- Assegurar *compliance* da organização adequado aos seus ambientes;
- Resultados justificáveis.

Procurar usar uma linguagem comum é uma tarefa importante, sempre considerando que os diversos atores têm modelos mentais diferentes, segundo suas atribuições funcionais. O ideal é criar um modelo comum, que permita compartilhamento entre eles: o CEO com o CFO, com o COO etc. E eles devem entender que serão responsáveis também pelo sucesso e pelas metas que declararem.

É importante ter em mente que os investidores estão interessados em dois aspectos e que nenhum deles deve ou pode ser minimizado. Por um lado, eles querem os melhores resultados imediatos possíveis, rentabilizando os investimentos feitos e, de outro, preocupam-se com a capacidade de a organização proporcionar lucros e benefícios futuros – em última análise, a perenidade da operação, que determina o valor real do negócio (*goodwill*).

Capítulo 3

Gestão de riscos

João Rufino de Sales

Rir é correr o risco de parecer um tolo.

Chorar é correr o risco de parecer sentimental.

Abriu-se para alguém é arriscar envolvimento.

Expor os sentimentos é arriscar a expor-se a si mesmo.

Expor suas idéias e sonhos é arriscar-se a perdê-los.

Amar é correr o risco de não ser amado.

Viver é correr o risco de morrer.

Ter esperanças é correr o risco de se decepcionar.

Tentar é correr o risco de falhar.

(Autor desconhecido)

A nossa vida é assim: uma seqüência infindável de escolhas entre uma situação ou outra. O risco é inerente às sociedades humanas. A nossa condição de seres inteligentes faz de nossas opções uma constante escolha se devemos ou não aceitar o próximo passo. Dentro deste aspecto é que a gerência de riscos em segurança assume decisivo papel na elaboração do Planejamento Estratégico de Segurança da Informação (PESI).

Mais do que arriscar para ter sucesso em um bom planejamento, é necessário ter apetite pelo risco, quantificar corretamente e escolher os tipos de riscos que uma organização está preparada para correr ou perseguir. É o risco aceitável que nos faz diferentes e competitivos na sociedade moderna. O risco deve ser retido de forma consciente e alinhado aos nossos objetivos. Devemos sempre, a cada passo, estar preparados para escolher qual o risco que desejamos aceitar para atingir nossos objetivos.

A gestão de riscos, portanto, é um processo sistemático para identificar, analisar, avaliar e tratar os riscos e permite melhorar o desempenho da organização por meio da identificação de oportunidades de ganhos e de redução de probabilidades ou impactos de perdas, indo além de demandas regulatórias. O processo de avaliação de riscos (*risk assessment*), na verdade, não é um processo único e, sim, uma composição de três outros processos: identificação de riscos, análise de riscos e avaliação de riscos. O objetivo final do processo é sempre que o risco seja reduzido ao nível aceitável, o que significa que o custo do tratamento não deve ultrapassar o custo proporcionado pelo risco.

Os *hackers* e *crackers* estão mais atuantes a cada dia. As mazelas do mundo real estão cada vez mais presentes no virtual, em um cenário complexo de redes interconectadas. Pesquisa realizada pela AON com 320 executivos de diversos segmentos, em 29 países, revelou que o risco mais temido pelas grandes corporações é o "dano à reputação da organização" seguido de perto pela interrupção dos negócios e pela responsabilidade civil. Podemos verificar, então, que todos os maiores temores estão diretamente ligados à informação, à sua integridade e disponibilização adequada. Confiança e credibilidade constituem a base de nossa sociedade e podem ser amplamente prejudicadas pela informação.

Como fazer para implantar uma adequada gestão dos riscos? Em minha opinião e de muitos autores, a melhor maneira é escolher o *framework* de trabalho mais adequado e obter da alta administração o comprometimento. Normas e diretrizes não faltam. Experimente digitar as palavras "normas", "gestão" e "riscos" no *Bing*: milhares de *links* lhe indicarão bons caminhos. Selecione aqueles que lhe pareçam mais adequados, busque especialistas, implemente soluções automatizadas de análise de riscos para auxiliar a tomada de decisões.

Finalmente, tenha sempre em mente que não existe como eliminar 100% dos riscos. Fazer gestão de riscos é descobrir qual nível de risco é aceitável para o seu negócio ou até mesmo para sua vida. Depender de oráculos é algo do passado, onde tudo parecia ser determinado pelo destino e um ser superior decidiria por nós. Para crescer e para, acima de tudo, sermos mais competitivos, é necessário e urgente ousar. E ousar em italiano é

riscare, ou seja, o poema de autor desconhecido (pelo menos por mim) continua como uma grande verdade “tentar é correr o risco de falhar”; porém, se não tentarmos, nunca saberemos a consequência de nossa decisão, e consequência é mistério e mistério, acima de tudo, é vida.

Capítulo 4

Aspectos tecnológicos, humanos e financeiros

Edison Fontes

Neste capítulo, destacamos um aspecto que deve ser considerado no Planejamento Estratégico da Segurança da Informação (PESI) nas organizações, independente do seu porte ou tipo do negócio. Trata-se do aspecto humano, que é tão importante quanto a questão técnica e a financeira. Acreditamos que o balanceamento adequado destes três elementos possibilita o sucesso do planejamento e da execução do processo de segurança da informação.

1. Introdução

A segurança em sistemas de informação deve contemplar não apenas os aspectos técnicos. As particularidades sociais referentes ao ambiente da organização e às pessoas também têm sua importância e devem ser consideradas. Pelo fato de, historicamente, a segurança da informação ter início a partir da área técnica de processamento de dados, os aspectos sociais da organização e das pessoas têm sido deixados de lado ou têm tido uma menor prioridade ou, em caso extremos, têm sido completamente esquecidos. Este fato pode ser uma boa explicação para muitas empresas, mas, com certeza, não justifica as atitudes de muitas organizações pelo desinteresse ou não consideração dos aspectos relativos às pessoas, seja considerando os indivíduos isoladamente ou o ambiente social da organização.

Precisamos de regras explícitas, rígidas o suficiente para que sejam cumpridas por todos. Porém, mais do que isso, precisamos de pessoas que entendam o porquê das regras de proteção da informação e as sigam não por medo, mas por alinhamento com a organização em termos de proteção do negócio e de que o sucesso do negócio é o sucesso de todos. Isto não quer dizer que todos concordarão com todas as regras, normas e políticas, mas que todos terão uma postura profissional perante a segurança da informação.

Em relação aos aspectos técnicos, chamamos a atenção para o fato de muitas vezes o profissional de segurança da informação focar-se apenas na proteção do recurso, sem se preocupar com os fatores gerenciais e outros que permitam um planejamento adequado e uma execução do processo de segurança da informação com mais chances de sucesso. O profissional de segurança da informação deve ter uma visão ampla de tudo que contribui para o sucesso do processo de Segurança da Informação (bem como o que pode prejudicar), começando pelo planejamento e se cristalizando na sua implantação.

O terceiro aspecto fundamental a ser contemplado no processo de segurança da informação é a questão financeira, que possibilita a viabilização do uso dos bens de informação e dos recursos de proteção.

2. Definições

2.1. Aspectos sociais

São os aspectos relacionados às pessoas e ao ambiente em que as elas vivem e trabalham.

2. 2. Aspectos técnicos

São os aspectos relacionados à tecnologia e aos seus recursos.

3. Planejamento da segurança da informação

A elaboração de um planejamento é primordial para a implantação de um processo de segurança da informação. Abaixo, consideramos os principais itens que devem ser observados em uma ação de planejamento neste sentido.

A segurança da informação é rica em atividades operacionais. Em função de fraquezas existentes, somos levados a começar imediatamente pelas ações técnicas que são importantes. Porém, o perigo reside em ficarmos limitados às atividades operacionais. Por ser um elemento importante para a organização, é fundamental a existência de um elaborado planejamento estratégico, que deve ser validado com a alta administração da

organização e que orienta o direcionamento dos caminhos que os projetos e atividades devem seguir. Em sua montagem, o PESI deve ter orientações básicas que devem proteger a estratégia a ser adotada.

Entre elas, consideramos:

a) Alinhamento com a legislação e políticas da organização – todas as ações voltadas à segurança da informação devem respeitar a legislação vigente do país e não devem ir de encontro às políticas organizacionais.

b) Consideração às iniciativas de negócio – realização dos negócios é a ação mais importante, afinal, dela depende a sobrevivência da organização. A segurança deve garantir que o uso da informação nas diversas iniciativas esteja acontecendo de forma adequada, assim como uma proteção extremada pode acabar inviabilizando a realização de negócios.

c) Definição da estrutura e forma de atuação da área de segurança – esta questão deve definir alguns pontos, como abaixo:

- Se a área de segurança da informação irá utilizar recursos humanos próprios ou de outras áreas para os projetos;

- Qual será a posição organizacional da área de segurança da informação;
- Qual será o escopo de atuação da área de segurança da informação.

d) Definição de onde virão os recursos financeiros – é durante o planejamento do processo de segurança da informação que se deve definir estrategicamente de onde virão os recursos financeiros para viabilizar a execução dos diversos projetos, bem como a utilização pela organização de vários recursos de informação. Neste momento, também se deve esclarecer as responsabilidades (em relação aos recursos financeiros) para as áreas usuárias, técnicas e para a de segurança da informação.

e) Arquitetura de segurança da informação – o processo de segurança da informação deve seguir uma arquitetura e é importante que seja algo possível de ser implantado. Afinal, ela possibilita a visão completa da abordagem da proteção. Em meu livro *Vivendo a segurança da informação*, sugiro uma arquitetura prática.

f) Ser humano – o comprometimento do usuário é um pilar para que a segurança da informação seja efetiva para a organização. É necessário que este usuário receba treinamento específico para:

- Conscientização em segurança;
- Conhecimento das políticas, normas e procedimentos;
- Conhecimento técnico, relativo às questões que lhe afetam.

g) Tecnologia para ações de proteção – o uso da tecnologia é necessário para a proteção no ambiente computacional. A organização, por meio da área de segurança, deve utilizar todos os recursos disponíveis para a proteção da informação; evidentemente, de forma profissional e compatível e com os seus recursos financeiros.

Muitas vezes, o profissional de segurança da informação, pressionado pela situação da organização, foca apenas neste aspecto das soluções tecnológicas para a proteção da informação. Situações deste tipo podem existir, mas de forma temporária, pontual. Para implantar um processo efetivo de segurança da informação é necessário não ficar focado neste aspecto.

Figura 1. Estrutura do PESI.



4. Aspectos sociais

4.1. Regulamentos

Os regulamentos (políticas, normas e procedimentos) proporcionam a construção e explicitação dos pontos considerados como “padrão de conduta”. As pessoas devem seguir estes regulamentos; caso contrário, estarão quebrando regras de convivência com a organização.

Para melhor compreensão, é importante que estes documentos sejam objetivos, claros e transmitam o essencial. Isto é, quando falamos em política, significa a cultura da organização em relação ao tema segurança da informação. Ela deve ter poucas páginas e dizer explicitamente o que se quer. Não precisa entrar em detalhes do como fazer, já que nas normas e procedimentos teremos este detalhamento.

É importante para o aspecto social que a política principal da organização para a segurança da informação seja assinada pelo presidente. As pessoas, ao lerem a política e identificarem que a mesma foi assinada pelo presidente da organização, entenderão mais facilmente a importância da segurança da informação para o negócio.

Os regulamentos sobre a segurança da informação devem ser sempre lembrados aos usuários nos treinamentos periódicos. Eles devem ser de fácil acesso, tipo intranet da organização. Evidentemente, junto com a existência destes documentos, é fundamental que as regras descritas sejam seguidas por todos, inclusive pelo presidente. As pessoas precisam entender que as regras são para cumprimento profissional por todos da organização.

4.2. Cultura organizacional

Esse aspecto social é construído ao longo do tempo. Quando implantamos um processo de segurança da informação devemos considerar a cultura da organização. Na medida do possível, devemos definir os controles de segurança respeitando esta cultura. Não quer dizer que este processo vá se curvar e deixar de fazer a devida proteção de um recurso por que isto vai contra a cultura. Quer dizer que, ao implantar um controle, devemos considerar seu impacto sobre as pessoas e a cultura organizacional existente. A implantação de um processo de segurança da informação em órgão do governo é bem diferente de uma empresa de publicidade, por exemplo. Contudo, ambas as implantações buscam proteger adequadamente a informação necessária ao sucesso do negócio e/ou alcance dos objetivos da organização.

Mas, cultura organizacional também se cria. Normalmente, para que o processo de segurança da informação aconteça de forma adequada é necessário que os requisitos de segurança sejam considerados no início do desenvolvimento de sistemas. Na vida prática das organizações, muitas vezes esta área é envolvida em novos sistemas na fase de implantação do sistema em produção. Neste caso, tem de haver uma mudança na cultura organizacional no que diz respeito ao processo de desenvolvimento de sistemas para que os requisitos de segurança sejam discutidos e a sua utilização seja validada na especificação técnica do desenvolvimento de sistemas.

Sendo assim, considerar a cultura organização é uma estrada de duas vias. A segurança considera as características da organização, que deve desejar que a segurança proteja adequadamente a informação, mesmo que (na verdade, quase sempre) este fato acarrete um custo de tempo e de esforço nos processos.

4.3. Clima organizacional

O clima organizacional é o ar virtual de todos os pensamentos e sentimentos em relação à organização que as pessoas inspiram e expiram. Quanto melhor o clima organizacional, mais chances de sucesso o processo de segurança da informação terá. Este aspecto é fundamental e será um acelerador ou um impedimento para que a informação tenha a proteção adequada. Isto não quer dizer que organizações que possuam um clima organizacional em baixa não possam implantar um processo de segurança da informação. Podem e devem. Porém, o profissional da área deve estar atento, pois será uma tarefa mais difícil.

Mais importante do que o nível do clima organizacional, entretanto, é a sua causa. Seu nível é apenas uma foto. Precisamos estar cientes e acompanhando a causa. Se uma organização será adquirida por outra ou se está deixando de atuar no país, evidentemente, o clima será tenso e a alegria não será o forte.

Esta situação é bem diferente de uma organização que possui historicamente um programa de “busca o culpado”, “caça às bruxas”, altíssima rigidez (não compatível com o negócio) em relação a atitudes do funcionário ou terceiros e outras situações equivalentes.

Uma organização que possui funcionários e prestadores de serviço satisfeitos com o trabalho, orgulhosos das conquistas de todos e desejosos de continuarem neste ambiente nos próximos cinco anos, tem facilitada a implantação do processo de segurança da informação. Isto não quer dizer que todos acharão uma maravilha estas ações. Significa que todos terão uma atitude profissional perante às políticas, normas e procedimentos de proteção da informação.

Concluindo, ambiente de não-confiança entre as pessoas, clima de inimizades, revolta contra a organização e outros problemas não impedem a implantação de um processo de segurança, mas dificultam em muito.

4.4. Processo contínuo de treinamento

Quando uma organização possui um processo de treinamento contínuo, é mais fácil desenvolver um processo de conscientização em segurança da informação, que, por sua vez, contribui para que o ambiente de trabalho das pessoas esteja constantemente possibilitando o crescimento profissional e como ser humano do funcionário ou prestador de serviço. À medida que a pessoa se sente considerada para treinamentos e outras ações, o ambiente social torna-se mais positivo. É necessário que todos, ao entrarem na organização, recebam um treinamento inicial em segurança da informação e, ao longo da sua permanência na empresa, recebam treinamento periódico sobre o assunto, tanto com foco de conscientização quanto com uma abordagem mais técnica.

A realização de campanhas de segurança é recomendável, mas elas devem fazer parte de um conjunto de medidas praticadas por toda a vida da organização. Hoje, já há elementos que ajudam neste processo: palestras, livros, teatro corporativo, entre outros.

4.5. Profissionalismo

Muitas organizações ainda possuem um clima amador nas relações com seus funcionários e entre eles. Um processo de segurança da informação será mais bem-sucedido quando o ambiente é pautado pelo profissionalismo. O amadorismo / informalismo profissional em questões empresariais aparece mais nas empresas médias e nas familiares (independente do tamanho) e este elemento está intimamente ligado com a questão das políticas, normas e procedimentos. Organizações pautadas pelo profissionalismo desenvolvem e implantam mais facilmente regulamentos deste tipo.

5. Aspectos técnicos

5.1. Atualização da tecnologia

Estamos em um mundo que tem uma fantástica rapidez na mudança e aprimoramento da tecnologia, fazendo com que o negócio utilize cada vez mais estes novos recursos. Desta forma, a segurança da informação tem de alcançar esta nova tecnologia e definir quais serão os novos controles. Esse fato, muitas vezes, faz com que a questão esteja (considerando o cronograma) atrás das iniciativas do negócio. O que devemos garantir é que esta diferença seja aceitável e não ponha em risco o negócio.

Precisamos considerar como a área de segurança da informação se manterá atualizada em termos de tecnologia. Para isso, as formas variam desde uma solução interna até a utilização de um parceiro competente. O que é importante é que o responsável pela área de segurança da informação tenha isso esclarecido.

5.2. O fornecedor da solução

Quando uma organização adota uma solução ou um fornecedor de tecnologia, de uma maneira mais ou menos forte, ele fica refém desta solução ou do provedor de recurso. Sendo assim, é muito importante que sempre seja considerada a continuidade da solução (ou do fornecedor). Nos últimos anos, mesmo empresas sólidas foram adquiridas por outras organizações que simplesmente congelavam uma solução da primeira, obrigando os clientes mudar para a solução da organização compradora.

Porém, estes acontecimentos não devem impedir a utilização de parceiros. “Homem algum é uma ilha”, já dizia um pensador. Organização alguma sobrevive sozinha, é a nossa realidade. Precisamos de parceiros e teremos parceiros sempre. É necessário termos uma visão profissional que nos permita analisar e gerenciar o risco que estes relacionamentos e dependências trazem para a organização.

5.3. Requisitos de segurança devem ser mantidos

Não é pelo fato de estarmos utilizando uma nova tecnologia ou solução que os requisitos de segurança devem ser deixados de lado. Identificação individual, registro dos acessos realizados, controle de acesso, cópias de segurança, continuidade de negócio etc. são aspectos da segurança da informação que sempre devem ser considerados, independente da solução ou tecnologia. Todo profissional da área deve ter claro os seus principais requisitos, que são válidos há séculos e continuarão assim por muitos outros.

Em alguns momentos, a tecnologia disponível não facilita; em outras vezes, ela torna possível e facilita a implantação de requisitos específicos. Não devemos confundir os requisitos de segurança com as facilidades que a tecnologia nos disponibiliza para implantar estes requisitos.

6. Aspectos financeiros

O planejamento e implantação do processo de segurança da informação necessitam de recursos financeiros para a sua execução. Pessoalmente, sou da opinião de que todas as organizações têm condições de planejar, implantar e manter um processo de segurança da informação. Todas têm recursos financeiros suficientes para ter uma proteção da informação compatível com o porte e seu negócio/objetivo.

O que se precisa é identificar como o recurso financeiro realizará o processo de segurança. Isto é, de quem será a verba financeira para o processo de segurança. Por exemplo: a compra de equipamentos tipo *firewall* e os respectivos produtos serão pagos pela área de tecnologia ou pela área de segurança da informação?

É necessário que este aspecto esteja explícito para que o planejamento do recurso financeiro esteja sincronizado com o cronograma do planejamento, desenvolvimento e manutenção do processo de segurança da informação.

7. Conclusão

A segurança para sistemas de informação não é uma atividade trivial, pois deve considerar tanto os aspectos técnicos quanto os do ambiente da pessoa e do ambiente da organização. Cada um dos aspectos apresentados pode (e deve) ser subdividido. O importante é que você entenda este conceito e aplique quando da implantação e manutenção do processo de segurança da informação em uma organização.

Capítulo 5

Serviços internos

Christiane Mecca

O grande desafio enfrentado pelos CIO's (*Chief Information Officers*) no cenário atual é o alinhamento do trabalho da área de tecnologia da informação (TI) à estratégia de negócios da organização. Os serviços oferecidos no passado tinham como principais características o atendimento ao usuário, foco na tecnologia, uso de recursos internos e comportamento reativo. À medida que a TI passou a trabalhar com o objetivo de atender seus clientes e processos internos, gerando valor para a organização e maximizando o retorno para os negócios dos investimentos realizados na área, novos conceitos, como melhores práticas e qualidade do serviço, foram introduzidos no cenário atual.

Atualmente, o atendimento ao cliente, foco no processo e comportamento proativo são extremamente valorizados. Até mesmo atender à demanda interna dos processos de negócios e suas certificações da qualidade, como ISO 9001, ISO/TS:16494 e tantas outras, levaram a área de TI a reavaliar seus serviços, no sentido de estar estruturada para atender aos requisitos destas normas. Como processo de suporte para os principais processos da organização, faz-se necessário o conhecimento dos requisitos das normas que impactam diretamente a performance dos processos principais, e que são passíveis de auditorias internas e externas. A TI deve se preparar, não com o objetivo principal de obter a certificação do próprio processo, mas para atender os requisitos mínimos que impactam os processos clientes.

Quando falamos em serviços de TI, é fundamental falarmos em ITIL (*Information Technology Infrastructure Library*) – um conjunto das melhores práticas para atender às exigências dos cenários atuais. Nela, a definição de serviço pode ser encontrada como “um ou mais sistemas de TI que habilitam um processo de negócio”. Um sistema está baseado em *hardware*, *software*, pessoas e processos. ITIL pode ser considerado um referencial para se estabelecer serviços de qualidade integrando pessoas, processos e tecnologia, e gerenciando a TI como um negócio da organização.

O valor do serviço de TI é percebido por meio do alinhamento com a estratégia da organização, custo, tempo de resposta às demandas internas e qualidade. O gerenciamento dos serviços de TI com qualidade exigem equilíbrio das demandas internas e recursos disponíveis, com custos aprovados pelo negócio.

O nível de serviço oferecido e acordado com o negócio, SLA (*Service Level Agreement*), é um indicador da performance e qualidade do processo TI. Por meio dele se pode medir a satisfação do cliente, isto é, como ele percebe o serviço prestado. Os SLA's dos serviços que afetam o desempenho dos negócios, como disponibilidade dos sistemas críticos, infraestrutura de rede, *help desk*, fornecimento de equipamentos de TI etc., quando não atingem os níveis acordados devem ser utilizados como parâmetros para o processo de melhoria contínua do processo TI. Um plano de ação deve ser desenvolvido e apresentado para as áreas de negócio da organização.

O desenvolvimento e implantação de controles internos são fundamentais para avaliação da maturidade do gerenciamento de serviços de TI e garantia de alinhamento à estratégia e processos do negócio.

Bibliografia

- FOINA, Paulo Rogério. *Tecnologia da informação – planejamento e gestão*. 2ª Ed. São Paulo: Atlas, 2006.
- MAGALHÃES, Ivan Luizio, PINHEIRO, Walfrido Brito. *Gerenciamento de serviços de TI na prática: uma abordagem com base na ITIL*. São Paulo: Novatec, 2007.

Capítulo 6

Provedores externos

Álvaro Teófilo

Neste capítulo, trataremos dos desafios de uma organização ao contratar serviços externos. Veremos também os desafios que estes terceiros representam no cotidiano da gestão de segurança, tanto no cumprimento de seus prazos SLA's (*Service Level Agreement*) quanto na conformidade dos mesmos com a política vigente em sua organização.

1. Introdução

É cada vez maior o número de organizações que tomam a decisão de terceirizar parte de suas operações. Muitos iniciaram este campo contratando parceiros para execução de serviços de tecnologia e de operações muito específicas (como os *call centers*) a outras empresas de grande e médio porte, para que estas fizessem pela organização o que até então era responsabilidade de seus próprios funcionários.

A principal razão da terceirização é, sem dúvida, a redução de custos diretos e indiretos que um determinado serviço gera para uma organização. Agregado a isso, a especialização de algumas empresas em executar determinadas funções com maior conhecimento atrai muitos gestores, que precisam de um serviço de qualidade, mais livre para se alinhar ao negócio da organização e oferecer novos serviços a ela.

No entanto, se torna mais usual que operações de *backoffice* e até mesmo serviços que são considerados *core business*, ou seja, a "alma do negócio" das organizações, sejam transferidas para um parceiro de negócios. Apesar de forma ainda tímida, já existem várias iniciativas que indicam que as organizações, procurando ganhar eficiência e que irão claramente para um caminho sem volta de terceirizar parte de suas operações mais críticas, trazendo à discussão a necessidade de entendermos e endereçarmos os impactos destas decisões sob o ponto de vista de riscos.

Terceirizar serviços necessários, mas que não sejam o *core business* da organização e que possuem um alto custo administrativo, como um *call center*, pode ter um excelente retorno. Ao terceirizar uma operação importante para o negócio, o parceiro selecionado precisa ter reputação e porte para assumir os problemas operacionais desta função.

2. Gestão de parceiros de negócios

Independente do grau de profundidade que a terceirização de operações já atingiu em uma organização, alguém deve assumir, dentro de cada corporação, o papel de orientar homens de negócios e de tecnologia a respeito de quais preocupações devem ser endereçadas no momento em que uma externalização de operações é feita. Obviamente, é necessário que a organização compreenda a importância desta decisão e as conseqüências que a falta de uma avaliação e gestão de riscos operacionais pode trazer para ela. Com esta questão reconhecida, cada organização deve definir quem fará o papel de gestão de riscos em operações terceirizadas. Normalmente, temos visto a própria área de segurança da informação como a líder da gestão de parceiros em grandes organizações.

Neste sentido, é importante se observar algumas questões:

- a) A terceirização deve ter um gestor, responsável por acompanhar as métricas e fazer com que os SLA's sejam cumpridos.
- b) O apoio jurídico é importantíssimo na hora de se estabelecer os SLA's e as penalidades pelo seu não-cumprimento.
- c) Não subestime o impacto que uma má contratação pode ocasionar em sua operação. A responsabilidade continua sendo do gestor; e, para os clientes, os problemas são sempre da sua organização.

3. Quem, quando e o que avaliar

Uma das perguntas mais comuns no mercado a respeito da questão da terceirização é: por onde começar a gestão? Antes de tudo, tenha em mente que existem dois mundos que precisam ser trabalhados paralelamente: a)

a gestão de serviços e operações que já estão terceirizadas; e b) a gestão de novas terceirizações.

A gestão de riscos de serviços já contratados deve ser iniciada a partir de um levantamento completo de todos os serviços prestados fora de sua organização. Algumas outras áreas internas poderão ajudar na sua pesquisa, especialmente as áreas de gestão de contratos, jurídico, compras e até mesmo tecnologia. Você terá de definir uma pessoa ou equipe que terá a responsabilidade, dentro de sua área, de executar esta tarefa em tempo integral.

Separar estas operações por nível de criticidade para os negócios envolve um esforço razoável e, neste sentido, encontramos duas variáveis que conseguem dar peso a elas e nos ajudam a determinar a priorização das avaliações:

a) Quanto maior o nível de dependência da operação externalizada para a sua organização, maior deve ser a prioridade dada à sua gestão de riscos. É importante deixar claro que a "dependência" aqui está relacionada à importância que a operação traz para a organização e, obviamente, de que forma a falha da entrega de seus serviços pode impactar seus negócios.

b) O armazenamento de informações de clientes deve ser visto como um fator crítico na avaliação de parceiros. A possibilidade de vazamento de uma base de dados ou um incidente envolvendo a divulgação de informações de clientes pode levar a organização contratante a uma séria exposição de imagem, cujas consequências são sempre difíceis de serem medidas.

Avalie o grau de dependência da operação terceirizada e a sensibilidade das informações confiadas a terceiros.

4. Avaliando e monitorando o risco

O primeiro passo deste trabalho deve ser feito junto ao jurídico da organização. A existência de cláusulas de responsabilidade, privacidade e segurança devem ser avaliadas contrato por contrato, o que gera um esforço razoável para advogados e gestores. Deve-se também incluir no aditamento uma cláusula de acordo onde a empresa se compromete a adotar todas as políticas e medidas de segurança que a contratante exigir, bem como aceitar a existência de auditorias periódicas que avaliarão seu nível de adaptação a estas políticas. Estas cláusulas também devem ser utilizadas nos novos contratos que a organização assinar no futuro.

A existência das cláusulas não deve ser considerada como uma premissa para o início do trabalho de avaliação, mas as experiências das organizações encaram esta questão de uma forma bastante conservadora. Se há, por exemplo, uma boa relação entre contratante e contratado, é muito provável que a avaliação de riscos possa ser feita antes do aditamento.

Com a lista de operações críticas em mãos e com a questão contratual endereçada, é hora de definir qual será o nível e a profundidade das avaliações de risco. Neste momento, a organização deverá construir questionários que incluam todas as disciplinas de segurança que desejam ser avaliadas, como a existência de políticas de segurança, a gestão de segurança de redes, atendimento às legislações e *compliance*, entre outros.

Uma boa ferramenta encontra-se livre na Internet e pode ser utilizada por qualquer indivíduo que tenha interesse em utilizá-la. Construída pelo BitsInfo, o processo chamado *Financial Institution Shared Assessment Program* produziu uma planilha que cobre com bastante extensão as principais ações e processos de gestão e controle de riscos de segurança em ambientes físicos e lógicos. A planilha encontra-se no próprio site da instituição, em www.bitsinfo.org.

5. Implantando o processo

Com os questionários desenvolvidos e definidos, deve-se construir um processo com diversas fases que indiquem o começo, meio e fim do processo, incluindo, pelo menos, dez pontos:

1) O envio de uma carta ao provedor de serviços, informando a existência do processo de avaliação de riscos e solicitando o seu acordo, bem como a determinação de um nome de gerente ou diretor responsável pelo atendimento da demanda;

2) A definição do escopo de trabalho baseado na realidade de cada operação;

3) A definição de cronograma de trabalho entre as partes;

4) O envio e devolução dos questionários aos responsáveis na empresa parceira;

5) A visita ao *site* para testes dos controles declarados pelo provedor;

6) A geração de relatório *draft* que indique os primeiros resultados do trabalho, que deve ser usado como base para uma discussão com o parceiro;

7) A emissão de relatório final, informando o nível de aderência do parceiro às práticas exigidas pela organização;

8) A determinação de plano de ação de melhorias, se for necessário, bem como a obtenção do comprometimento da empresa parceira declarada

9) O acompanhamento da aplicação dos pontos pendentes de acordo com os prazos estabelecidos entre as partes;

10) A reavaliação periódica (a cada ano, por exemplo) do processo, passando por todas as fases anteriores.

Observe que este processo pode também ser aplicado para a segunda "dimensão" de trabalho que destacamos neste documento. A contratação de novas operações terceirizadas pode utilizar os mesmos passos para ajudar às áreas de negócios a avaliar empresas que estão concorrendo em um novo contrato. Temos vivido experiências bastante positivas em relação a este tema, percebendo que, uma vez apoiados desde o primeiro momento em que tomam a decisão de externalizar uma operação, homens de negócios utilizam nossas avaliações como um dos principais fatores de decisão sobre qual empresa contratar.

Neste momento, também tivemos a ideia clara de que a gestão de riscos em operações terceirizadas é muitas vezes ignorada pela simples falta de conhecimento e experiência dos gestores de negócios. É uma questão cultural que nós, gestores de segurança da informação, podemos trabalhar na empresa e que geramos resultados excelentes na relação entre segurança e negócios. Neste caso, estreitamos relacionamentos, geramos valor agregado para os negócios e temos muito mais claramente uma foto de onde estão os riscos associados a este tipo de operação.

Finalmente, com a tendência clara demonstrada pelo mercado de que a terceirização continuará sendo utilizada como um fator de ganho e eficiência, qualidade e redutor de custos, é imperativo que um processo muito bem definido garanta que a gestão de riscos operacionais e de segurança faça parte das avaliações de novas parcerias.

Capítulo 7

Melhores práticas

Valmir Schreiber

André Pitkowski

1. Introdução

Um dos maiores desafios da área de TI nos dias de hoje é estruturar os esforços para obter a conformidade com os critérios da SOX (*Sarbanes-Oxley*), circulares governamentais ou até mesmo as contratuais, PCI (*Payment Card Industry*). De modo geral, a maioria das empresas entende que precisam manter estruturas de proteção e segurança para seus sistemas e dados, mas tem dificuldade em entender quanto detalhadamente ou amplamente estes requerimentos devem ser interpretados. Neste ponto, as estruturas de controles internos como o CobiT (*Control Objectives for Information and Related Technology*), ITIL (*Information Technology Infrastructure Library*) ou a ISO 27001 (padrão relacionado à segurança da informação) podem ajudar o profissional.

Estruturas de controle e governança como o CobiT, ITIL ou catálogos de práticas como a ISO 27001 podem ajudar as empresa de três formas distintas:

- Explicitando as dimensões dos requerimentos de segurança e governança;
- Demonstrando as várias opções para se atingir estes requerimentos; e
- Estruturando um programa de conformidade.

1.1. As dimensões

Fácil pensar nos aspectos de conformidade como sendo o mesmo que um dos mecanismos que podem ajudar o profissional de TI a atingir suas metas de segurança. Por exemplo, seria o mesmo que os profissionais de segurança pensarem em seus *firewalls*, autenticação e mecanismos de autorização quando considerarem como sua informação deve ser protegida.

Uma forma mais produtiva é ver a segurança sob a perspectiva do que e como a organização costuma se proteger. Estruturas de controle exigem uma avaliação de riscos e a classificação de informações e ativos a serem protegidos antes de decidir como protegê-los. Ao considerar os riscos associados a uma atividade de conformidade, a avaliação de riscos irá forçar a organização a perceber quais das suas informações e processos irão impactar a precisão, transparência e responsabilidade final sobre os seus relatórios financeiros. A identificação e o processo de avaliação de riscos permitem à organização definir o escopo das atividades de conformidade e os riscos que deverão ser mitigados.

As estruturas de controle como o CobiT e ITIL expõem o fato de que segurança é mais do que simplesmente controles sobre sistemas e aplicativos. O escopo total da segurança inclui como uma organização está estruturada corporativamente – os checklists elaborados para desenvolver, manter e auditar os processos de negócio que estão contidos no escopo do *Compliance*. Inclua neste escopo mais do que as atividades internas, mas as externas, como os provedores de serviços e contratos com terceiros, por exemplo.

1.2. Os mecanismos

As estruturas de controle ajudam na identificação das ofertas de mecanismos, serviços e metodologias que as organizações podem fazer uso para mitigar riscos. Enquanto os tecnólogos tendem a estabelecer soluções técnicas, os padrões do CobiT, ITIL e da ISO enfatizam a necessidade de políticas e procedimentos baseados em processos de negócios corretamente estruturados para gerenciar riscos.

Por exemplo, existem momentos em que os mecanismos mais efetivos para garantir que somente os usuários apropriados obtenham acesso às informações financeiras da organização são envolver as pessoas corretas na aprovação e certificação destes controles de acesso. Algumas organizações podem passar ao largo da necessidade de mecanismos de segurança simplesmente configurando políticas que declarem qual informação

sensível para o negócio deve estar contida em determinados ambientes de processamento de dados apropriadamente protegidos e devem ser transmitidas de forma particular. Esta medida compensatória simplifica tremendamente a tarefa de conformidade.

2. CobiT

Uma parte importante a ser considerada no texto de um documento de *compliance* deve ser a dedicada ao processo de continuidade de melhoria do próprio *compliance*, que, com qualquer regulamentação, contrato ou padrão, requer uma abordagem cíclica e estruturada para que se atinjam as metas. O CobiT apresenta e descreve os seguintes processos, que podem ser encontrados também em outras estruturas de controle:

- Definir as metas específicas para o contexto do negócio e da organização da empresa;
- Seleção dos controles para atender estas metas;
- Organizar e implementar estes controles;
- Avaliar a efetividade dos controles;
- Repetir o processo.

Na medida em que o negócio evolui e se adequa ao mercado, o ambiente de trabalho acompanha estas mudanças. Cresce, encolhe, oferece novos produtos, instala novos processos ou se torna exposto a novas ameaças. Se os riscos mudam, os controles acompanham estas mudanças.

Há de se considerar, também, que uma prática considerada boa hoje poderá não mais atender às demandas de mercado amanhã. Em outras palavras, faz-se necessário um processo que se adapte e reconheça mudanças do negócio para as atividades de *compliance*, isto é: de uma estrutura de controle.

O público-alvo do CobiT é a alta administração das organizações, como também diretores e gerentes de IT e auditores em geral. O CobiT consiste em quatro seções:

- Avaliação executiva;
- Estrutura;
- Conteúdo principal (objetivos de controle, guia de gerenciamento e modelos de maturidade);
- Apêndices (mapas, referências e glossário).

A seção conteúdo principal é dividida em 34 processos, nos quais em cada um deles está descrito em quatro subseções de cerca de uma página cada. Cada subseção contempla:

- Visão geral dos objetivos de controle, que inclui um resumo das metas do processo, métricas e práticas;
- Uma descrição dos objetivos e um mapeamento do processo e seus domínios, critérios de informação e recursos de TI;
- Objetivos detalhados dos controles dos processos, que provê um total de 214 indicadores divididos entre os 34 processos;
- Guias de gerenciamento, que incluem as entradas e saídas do processo, a tabela RACI (*responsible, accountable, consulted, and informed*), metas e métricas;
- Modelo de maturidade para o processo, que orientada à ação.

Este material tem como objetivo ajudar às organizações a responder perguntas gerenciais, tais como:

- Quanto a empresa pretende investir? Os custos são justificados pelos benefícios?
- Quais são os indicadores que medem boas performances?
- Quais são os fatores críticos de sucesso?
- Quais são os riscos se os objetivos da organização não forem alcançados?
- O que outras organizações iguais à minha estão fazendo? E como elas fazem para medir e comparar?

2.1. Um modelo unificado

O CobiT contempla os modelos estabelecidos, como o CMM (*Capability Maturity Model*, ou Modelo de Maturidade de Capacidade) do Instituto de Engenharia de *Software*, ISO 9000, ITIL e ISO 27001 (modelo de segurança padrão, agora ISO 27001). Na realidade, 13 dos 34 objetivos de controle de alto nível são derivados diretamente do ITIL *Service Support* e *Service Delivery*.

Em função da sua larga abrangência e também porque está baseado em muitas práticas existentes, o CobiT pode agir como um integrador que traz práticas dispersas debaixo de um modelo único, ajudando a alinhar atividades com os objetivos do negócio.

Orientado para governança de TI, provê um modelo amplo e genérico, o que o torna aplicável na maioria das organizações. Podem ser usados outros padrões que cubram áreas específicas com mais detalhe, como ITIL e ISO 27001, e que, em conjunto com o CobiT, permitem criar uma melhor orientação a resultados.

3. ITIL

O ITIL provê diretrizes para melhores práticas de processos de ITSM (ou gerenciamento de serviços de TI) para melhor alinhar a TI aos negócios. O CobiT ajuda a organização a moldar os processos de ITIL às suas necessidades e metas, além de ajudar a estabelecer um ponto de início e um para o fim; ou seja, avalia onde a organização está agora e onde ela quer chegar. Sabendo-se estas metas, então, criar ou desenvolver as atividades para atingir esse objetivo.

3.1. ITIL – visão geral

O ITIL pode ser definido como um guia para as melhores práticas dos processos de TI. Desenvolvido na década de 1980 pela OGC (*Office of Government Commerce*), uma agência do governo britânico, o ITIL define processos em alto nível, deixando para as organizações a tarefa de implantar os processos da maneira mais satisfatória às suas necessidades.

O ITIL tem se tornado um padrão mundial de fato, desde que milhares de organizações adotaram este guia como modelo de gestão de TI. A principal contribuição do ITIL é promover o alinhamento de TI ao negócio. O ITIL define qualidade de serviço como objetivo e promove o alinhamento entre os serviços a serem entregues e as necessidades atuais do negócio. Organizações que queiram certificar suas áreas de TI em gestão de processo poderão fazê-lo por meio do ISO 20000, baseado no ITIL.

Embora o ITIL tenha uma cobertura abrangente, seu foco principal é o ITSM. O ITIL provê um modelo compreensivo, consistente e coerente de melhores práticas para o ITSM e seus processos relacionados, promovendo foco na qualidade, visando alcançar efetividade empresarial e eficiência no uso de sistemas de informação.

4. CobiT e ITIL agregando resultados

4.1. Combinando ITIL e CobiT para atingir os desafios dos negócios

As áreas de TI estão cada vez mais sob crescente pressão para alinhar-se às metas empresariais de suas organizações. Desafio que pode estar sob a pressão de atender a regulamentações como a lei SOX e Basiléia II. Obter esta conformidade requer forte capacidade de governança, com evidências claras para auditores externos. Em virtude de representar um papel tão importante para os negócios, a área de TI se vê cada vez mais comprometida a prover os meios de demonstrar essa capacidade de responder a estes desafios. Para tal, confiam em diretrizes como o ITIL e o CobiT para ajudar a entender e endereçar estes desafios.

Este tópico discute como ITIL e CobiT podem ser usados em conjunto com uma breve avaliação sobre ambos e uma análise de sua complementaridade. Tanto ITIL quanto CobiT permitem que as organizações alcancem três objetivos:

- Por meio do uso de melhores práticas, prover gerenciamento por processos além de gerenciar TI por meio de uma perspectiva empresarial focada em resultado e conformidade;
- Foco em processos com metas claras, baseado nos objetivos de negócios da organização e provendo recursos que permitam a medição deste progresso;
- Assegurar governança efetiva de TI ao nível de controle de processos e permitindo à TI demonstrar que atende ou excede os requisitos estipulados pela área de negócios ou por regras externas à TI.

Porém, há certa confusão nas áreas de TI sobre estes modelos. Alguns pensam que eles são duas alternativas para uma mesma meta, enquanto outros pensam que eles são mutuamente exclusivos. Na realidade, eles

são altamente complementares e juntos provêm muito mais valor do que se usados separadamente. O CobiT esboça o que você precisa fazer para enfrentar estes desafios, enquanto o ITIL mostra como chegar lá.

4.2. Combinação de modelos

Organizações que querem adotar o ITIL precisam estruturar um modelo para a governança efetiva de TI. O CobiT provê um modelo amplo de governança, que inclui diretrizes para ajudar a estruturar a área de TI para as exigências organizacionais. O CobiT também provê um mecanismo para medir a capacidade da atividade (pessoas, processos e tecnologia) para alcançar um resultado que satisfaça as exigências organizacionais, por medir seu desempenho.

Embora o CobiT seja orientado a processos de TI, não inclui as atividades ou etapas de processos. Focaliza sobre o que a organização precisa fazer em lugar de como fazer isto. É focado nas exigências empresariais e provê orientação do que é necessário para satisfazer estas exigências. Por outro lado, o ITIL define as melhores práticas dos processos para o ITSM e como chegar lá. Focaliza em métodos e define um jogo mais inclusivo de processos que o CobiT, provendo um guia para a construção destes processos.

CobiT e ITIL provêm uma excelente combinação para ajudar às organizações a gerenciar TI a partir de uma perspectiva de negócios, em um modelo conhecido como Gerenciamento de Serviços de Negócios (*Business Service Management*, ou BSM).

Repetindo: o ITIL provê diretrizes para melhores práticas de processos de ITSM para melhor alinhar TI com os negócios. O CobiT ajuda a organização a moldar os processos de ITIL às suas necessidades e metas. Ajuda a organização a estabelecer um ponto de início e um para o fim; ou seja, avaliando onde a organização se encontra e onde quer chegar. Sabendo-se estas metas, criar ou desenvolver as atividades para atingir esse objetivo.

O CobiT também provê um mecanismo efetivo para gerenciar e medir o progresso da implantação dos processos do ITIL, ajudando a organização a entender seus objetivos, além de medir o progresso para atingi-los, em melhoria contínua – uma das maiores contribuições de projetos baseados no ITIL. Para maior proveito, é sugerido, inclusive, o uso do documento “Alinhando CobiT, ITIL, ISO 2000 e ISO 27001 para Gerenciamento dos Negócios” (*Aligning CobiT, ITIL, ISO 20000, and ISO 27001 for Business Benefit Management Summary*), criado pelas entidades ITGI (*IT Governance Institute*), OGC (*Office of Government Commerce*), itSMF (*IT Service Management Forum*) e BSI (*British Standards Institution*), que apresenta um guia sobre como implementar melhor a combinação do CobiT, ITIL e série ISO 27000.

5. COSO

Há mais de uma década, o COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) publicou a obra *Internal Control – Integrated Framework* para ajudar às organizações a avaliar e aperfeiçoar seus sistemas de controles internos. Desde então, a referida estrutura foi incorporada em políticas, normas e regulamentos adotados por milhares de organizações para controlar melhor suas atividades, visando o cumprimento dos objetivos de negócio estabelecidos.

Nos últimos anos, intensificou-se o foco e a preocupação com a gestão de riscos e tornou-se cada vez mais clara a necessidade de uma estratégia sólida, capaz de identificar, avaliar e administrar riscos. Em 2001, o COSO iniciou um projeto com esta finalidade e solicitou à PricewaterhouseCoopers que desenvolvesse uma estratégia de fácil aceitação e utilização pelas organizações para avaliar e melhorar o próprio gerenciamento de riscos. O período de desenvolvimento desta estrutura foi marcado por uma série de escândalos e quebras de negócios, de grande repercussão, que gerou prejuízos significativos a investidores, empregados e outras partes interessadas. Na esteira destes eventos, vieram solicitações de melhoria dos processos de governança corporativa e gestão de riscos, por meio de novas leis, regulamentos e de padrões a serem seguidos. Tornou-se ainda mais necessária uma estrutura de gerenciamento de riscos corporativos capaz de fornecer os princípios e conceitos fundamentais, com uma linguagem comum, direcionamento e orientação claros. O COSO é de opinião que o documento “Gerenciamento de Riscos Corporativos – Estrutura Integrada” vem para preencher esta lacuna e espera que ela seja amplamente adotada pelas empresas e por outras organizações, bem como por todas as partes interessadas. Nos Estados Unidos, entre as consequências, destacam-se a Lei SOX, de 2002, e a

legislação semelhante que está sendo promulgada ou analisada em outros países. Esta lei amplia a exigência de que as companhias que negociam ações em bolsas de valores norte-americanas mantenham sistemas de controles internos, demandem a certificação da administração e contratem os serviços de auditores independentes para atestar a eficácia dos referidos sistemas. A obra *Internal Control – Integrated Framework*, que vem sendo submetida ao teste do tempo, serve como norma de ampla aceitação para o atendimento dos requisitos de comunicação.

A obra “Gerenciamento de Riscos Corporativos – Estrutura Integrada” amplia seu alcance em controles internos, oferecendo um enfoque mais vigoroso e extensivo no tema, mais abrangente, de gestão de riscos corporativos, cuja estrutura proposta, embora não tenha por meta substituir a estrutura de controles internos das organizações, incorpora a estrutura de controles internos em seu conteúdo. Além disso, poderá ser por elas utilizada, tanto para atender às suas necessidades de controles internos quanto para adotar um processo completo de gestão de riscos.

A premissa inerente ao gerenciamento de riscos corporativos é que toda organização existe para gerar valor às partes interessadas (donos, acionistas, investidores e controladores). Todas as organizações enfrentam as incertezas do mercado onde atuam e o desafio de seus administradores é determinar até que ponto pode aceitar esta incerteza e definir como ela pode interferir no esforço para gerar valor às partes interessadas. As incertezas representam os riscos e as oportunidades de negócio, com potencial para destruir ou agregar valor. A gestão de riscos corporativos possibilita aos administradores tratar com eficácia as incertezas, isto é, os riscos e as oportunidades a elas associadas, a fim de melhorar a capacidade de gerar valor.

O valor é maximizado quando a organização estabelece estratégias e objetivos para alcançar o equilíbrio ideal entre as metas de crescimento e de retorno de investimentos, considerando os riscos a elas associados, e para explorar os seus recursos com eficácia e eficiência na busca dos objetivos da organização.

O gerenciamento de riscos corporativos tem por finalidade:

- Alinhar o “apetite” a risco com a estratégia adotada: os administradores avaliam o apetite a risco da organização ao analisar as estratégias, definindo os objetivos a elas relacionados e desenvolvendo mecanismos para gerenciar estes riscos;
- Fortalecer as decisões em resposta aos riscos: o gerenciamento de riscos corporativos possibilita o rigor na identificação e na seleção de alternativas de respostas aos riscos – como evitar, reduzir, compartilhar e aceitar os riscos;
- Reduzir as surpresas e prejuízos operacionais: as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas a estes, reduzindo surpresas e custos ou prejuízos associados;
- Identificar e administrar riscos múltiplos e entre empreendimentos: todo empreendimento enfrenta uma variedade de riscos que podem afetar diferentes áreas da organização. A gestão de riscos corporativos possibilita uma resposta eficaz a impactos interrelacionados e, também, respostas integradas aos diversos riscos;
- Aproveitar oportunidades: pelo fato de considerar todos os eventos em potencial, a organização posiciona-se para identificar e aproveitar as oportunidades de forma proativa;
- Otimizar o capital: a obtenção de informações adequadas a respeito de riscos possibilita à administração conduzir uma avaliação eficaz das necessidades de capital como um todo e aprimorar a alocação deste capital.

Estas qualidades, inerentes à gestão de riscos corporativos, ajudam os administradores a atingir as metas de desempenho e de lucratividade da organização, evitando a perda de recursos. A gestão de riscos corporativos contribui para assegurar comunicação eficaz e o cumprimento de leis e regulamentos, bem como evitar danos à reputação da organização e suas consequências.

6. CBK

O CBK (*Common Body Of Knowledge*) é uma compilação feita pela ISC2 (*International Information Systems Security Certification Consortium*) do conhecimento relativo à área de segurança da informação em dez domínios distintos, que compreendem desde a segurança física até a análise de risco. A ISC criou também um

programa de treinamento e certificação do profissional de segurança, chamado CISSP (*Certified Information Systems Security Professional*).

7. Associações

7.1. ISACA

A ISACA® (*Information Systems Audit and Control Association*) é uma associação internacional formada por profissionais que atuam nas áreas de auditoria de sistemas, segurança da informação e, principalmente, governança de TI. Iniciou suas atividades em 1967, com um pequeno grupo de auditores que atuavam em organizações nas quais os sistemas informatizados começavam a cada vez mais desempenhar operações críticas.

Os associados da ISACA (mais de 86 mil em todo o mundo) são caracterizados por sua diversidade. Estes membros vivem e atuam em mais de 160 países e em diferentes posições relativas à tecnologia da informação (auditores de sistemas, consultores, profissionais de segurança da informação, CIO's, professores e pesquisadores, dentre outros).

É importante notar que a maioria dos associados desempenha suas funções em organizações de todos os segmentos econômicos – indústria, comércio, finanças e governo. Esta é, positivamente, a origem da força e expressividade da ISACA (www.isaca.org). As experiências adquiridas e trocadas entre os associados é o fator mais importante da associação, que possui uma base de conhecimento muito rica e diversificada disponível aos associados.

Esta representatividade da ISACA também reside na sua abrangência global com mais de 175 capítulos estabelecidos em mais de 70 países. Estes capítulos provêm às suas comunidades oportunidades de treinamentos, compartilhamento de recursos, suporte, network profissional e facilidade de interagir pelos cinco continentes e uma série de benefícios em nível local e internacional.

Mundialmente, a ISACA organiza, patrocina e controla a certificação para profissionais que atuam nas áreas de auditoria de sistemas (CISA® – *Certified Information Systems Auditor*), de segurança da informação (CISM® – *Certified Information Security Manager*) e de Governança de TI (CGEIT® – *Certified in the Governance of Enterprise IT*). Estas certificações são internacionais, reconhecidas e altamente valorizadas no mundo inteiro, constituindo hoje uma comunidade de mais de 38 mil profissionais certificados.

No Brasil, a ISACA (www.isaca.org.br) possui capítulos em São Paulo, Rio de Janeiro, Brasília e em formação em outras regiões, com uma rede de mais de 450 associados e em ascensão.

7.2. ISSA®

A ISSA (*Information Systems Security Association*) é uma associação de profissionais de segurança da informação presente hoje em 24 países, com mais de 13 mil associados. Seu objetivo é estimular o relacionamento entre os associados e trazer benefícios a estes por meio de parcerias, eventos, treinamentos e conteúdo. Uma de suas características é ser focada especificamente em segurança da informação, embora a associação possua programas diversificados que beneficiam desde o técnico iniciante até o executivo tomador de decisões das organizações.

Da ISSA nasceu a ISC2, responsável pela certificação de Profissionais SSCP (*Systems Security Certified Practitioner*), voltada à certificação técnica de profissionais de segurança e CISSP® (*Certified Information Systems Security Professional*), uma das mais respeitadas certificações de segurança no mundo, baseada nos dez domínios do CBK, que cobrem praticamente todos os tópicos referentes à segurança da informação.

Para obter a certificação CISSP, é necessário comprovar experiência em pelo menos um dos domínios e realizar uma prova com 250 questões sobre os dez domínios em um prazo máximo de seis horas.

No Brasil, a ISSA possui um capítulo regional que pode ser acessado pelo endereço www.issabrasil.org e a ISC2 pode ser acessada pelo endereço www.isc2.org.

Capítulo 8

Gerenciamento de mudanças

Ricardo Castro, CISA CFE

Neste capítulo, trataremos das questões que envolvem a gestão de mudanças, os desafios relacionados a este processo crítico da tecnologia da informação (TI), como dois dos mais conhecidos modelos de melhores práticas tratam o tema e como é possível avaliar se um processo de gestão de mudanças alinhado ao planejamento estratégico de segurança da informação (PESI) entrega, de fato, valor ao negócio.

1. Mudanças como causas de incidentes

Um percentual significativo dos problemas que ameaçam a disponibilidade, a integridade e a aderência regulatória nos serviços críticos da TI tem sua origem na execução inadequada e pouco planejada de mudanças. Desta forma, ao invés de voltar sua atenção na gestão de incidentes, que trata do problema depois de seu aparecimento, a TI deve olhar, de forma preventiva, para a gestão de mudanças para evitar a ocorrência de incidentes. Na verdade se os processos de gestão de mudanças não são estruturados e constantemente aprimorados (no melhor entendimento do modelo PDCA – Plan, Do, Check and Action, ou planejamento, execução, verificação e ação), provavelmente o departamento de TI entrará em um ciclo vicioso, onde parte dos incidentes de segurança será causada por ações oriundas da própria TI; e mesmo as ações corretivas podem ser a origem de novos incidentes.

Segundo o ITIL® (*Information Technology Infrastructure Library*), os principais problemas relacionados a este processo são:

- A falta de informação para análise de riscos – o surgimento de situações não previstas decorre da falta de uma base de configuração atualizada com as informações necessárias para fazer uma adequada análise de impacto;
- A falta de integração entre processos – a utilização de uma ferramenta adequada apóia o controle de mudanças e a sua integração aos demais processos auxilia o planejamento da mudança;
- Priorização de todas as mudanças – as mudanças devem ser planejadas e agendadas no tempo correto e de acordo com as necessidades de negócio. Devem ser tratadas apenas como mudanças urgentes àquelas que implicam na indisponibilidade atual ou imediata de um serviço.

A cultura da empresa influenciará na adesão e implantação deste processo e seus controles. O fator humano é essencial na mudança de paradigma. É importante fazer com que a equipe em TI esteja consciente dos efeitos positivos do processo como um todo. A falta de comprometimento da equipe é um dos pontos críticos em se tratando da gestão de mudanças. Da mesma forma, os usuários e a alta administração precisam estar conscientes de que o planejamento e os controles não são inimigos da flexibilidade, mas contribuem para um ambiente operacional equilibrado, estável e disponível.

Para colocar um pouco mais de ordem neste cenário extremamente desafiador, podemos lançar mão dos modelos de melhores práticas do CobiT® 4.1, mais especificamente no processo A16 – Gerenciar mudanças.

2. Desafios na gestão de mudança

As exigências pela excelência nos níveis de serviços para alcançar os objetivos do negócio são crescentes. Derivado desta necessidade, é possível perceber a área de TI em constante mudança para atender a demanda da evolução do cenário de negócios, implantando novas soluções, aumentando a capacidade e criando novos controles. Como fazem os tubarões, é preciso estar sempre em movimento, atento e, principalmente, sem se deixar levar pelo pânico. Planejar, ponderar e agir com lucidez são requisitos para que decisões emotivas não nos levem ao fracasso.

A princípio todas as mudanças, previstas ou não, seriam contempladas em um processo de gestão de mudanças. Contudo, na maioria das vezes é impraticável tratar todas as mudanças desta forma. Sinteticamente, podemos dizer que as principais atividades que envolvem a gestão de mudanças são:



- Monitoração e direcionamento do processo de mudança;
- Registro, avaliação e aceite ou rejeição das requisições de mudança (*request for change* ou, simplesmente, RFCs) recebidas;
- Classificação e priorização das mudanças junto aos comitês de negócio competentes para aprovação das RFCs;
- Coordenação do desenvolvimento e implantação da mudança;
- Avaliação dos resultados da mudança e encerramento do processo de mudança em caso de sucesso.

Todas as mudanças, incluindo aplicação de *patches* e manutenções emergenciais, sejam relacionadas à infraestrutura ou aplicações em ambiente de produção, devem ser formalmente geridas de maneira controlada. As mudanças (incluindo de procedimentos, processos, sistemas e parâmetros de serviço) são registradas, avaliadas e autorizadas antes de sua implantação e revisadas frente aos benefícios planejados. Estas etapas garantem certo conforto de que impactos negativos não afetem dois dos principais pilares da segurança da informação: a disponibilidade e a integridade do ambiente de produção.

A gestão de mudanças não pode ser uma cruzada individual da TI. O envolvimento e o apoio da área de negócio são vitais para o sucesso desta empreitada. Desde o primeiro momento, comitês de negócio devem ser formados visando não só a participação das principais áreas da empresa, mas a formação de uma cultura de gestão recursos e governança da TI. Outro suporte altamente recomendável é a aplicação de um modelo de maturidade na indicação dos níveis de formalização e automatização das atividades.

3. Gestão de mudanças segundo o CobiT®

Segundo o modelo de boas práticas e controles da ISACA®, os controles sobre o processo da TI de gerir mudanças visam, de forma direta, a geração de soluções que reduzam defeitos e retrabalho, requisitos alinhados às estratégias de negócio de qualquer companhia. Para isso, é preciso focar nos controles relacionados a avaliações de impacto, na autorização e implantação de todas as mudanças à infraestrutura da TI e na implantação de soluções técnicas. Estas ações minimizam erros originados de requisições de mudança incompletas ou podem chegar a suspender uma implantação de mudanças não autorizadas.

Estes objetivos, contudo, são alcançados pela definição e comunicação de procedimentos de mudança, incluindo-se aí as mudanças emergenciais. Soma-se a este procedimento o desenvolvimento e aplicação de método para avaliação, priorização e autorização de mudanças e, por fim, o rastreamento de status e reporte das mudanças.

O processo em si de gestão de mudanças é subdividido em cinco atividades, a saber:

1) Padrões e procedimentos de mudança: estabelecimento de procedimentos formais de mudança para gerir de forma padronizada todas as solicitações (incluindo manutenção e *patches*) para mudanças em aplicações, procedimentos, processos, sistemas e parâmetros de serviço, em suas respectivas plataformas.

2) Avaliação de impacto, priorização e autorização: avaliação de todas as requisições de mudança (RFCs) de forma estruturada para determinar o impacto nos sistemas em operação e suas funcionalidades. Além disso, garantir que todas as mudanças sejam categorizadas, priorizadas e, principalmente, autorizadas.

3) Mudanças Emergenciais: estabelecimento de um processo para definição, identificação, teste, documentação, avaliação e autorização de mudanças emergenciais que, eventualmente, não seguirão o processo pré-estabelecido de mudanças.

4) Rastreamento de *status* das mudanças e reporte: estabelece um sistema, automatizado ou não, para rastreamento e reportado as mudanças rejeitadas, comunicação do *status* das alterações aprovadas, em ava-

liação, em andamento e das mudanças finalizadas. Ter segurança de que toda as alterações aprovadas foram implementadas conforme planejado.

5) Encerramento e documentação: independente da mudança implementada, deve-se atualizar os sistemas relacionados, bem como a documentação do usuário e procedimentos.

Espera-se que, fruto da implantação destas atividades, tenha-se os seguintes resultados:

- Uma abordagem padronizada e consensual para avaliação de impactos de forma eficiente e eficaz;
- Expectativas formalmente definidas para impactos de mudanças, emergenciais ou não, baseadas nos riscos do negócio e em medições de desempenho;
- Procedimentos consistentes de mudança, emergenciais ou não;
- Uma abordagem padronizada e consensual para documentação das mudanças;
- Mudanças revisadas e aprovadas de forma consistente e coordenada;
- Procedimentos consistentes para mudanças e documentação.

Como em qualquer processo, é vital que todas as atividades gerem um resultado formal, rastreável e auditável.

4. Mantendo os riscos sob controle

O processo de gestão de mudanças tem impactos em virtualmente todos os recursos da TI, como os humanos, infra-estrutura, informações ou aplicações. Da mesma forma, aspectos de eficiência, eficácia, integridade, disponibilidade e confiabilidade das informações (este último, de forma secundária) podem ser afetados negativamente caso um processo formal e bem controlado não esteja implantado. Algumas das principais ameaças à TI que podem ser controladas são:

- Autorização de acesso especial não-revogado adequadamente;
- Efeitos adversos na capacidade e desempenho da infraestrutura;
- Mudanças não registradas ou rastreadas;
- Documentação de configuração que não reflete as configurações atuais do sistema;
- Falta de aderência às normas e políticas internas;
- Falta de habilidade na resposta as necessidades emergenciais de mudança;
- Alocação incorreta de recursos;
- Dependência crescente em pessoas;
- Probabilidade crescente de que mudanças não autorizadas são introduzidas nos sistemas-chave da companhia;
- Alocação insuficiente de recursos;
- Controle insuficiente sobre as mudanças emergenciais;
- Falta de documentação dos processos de negócio;
- Falta de gestão na priorização das mudanças;
- Perda do rastreamento das mudanças;
- Disponibilidade de sistema reduzida;
- Mudanças não autorizadas implantadas, resultando em comprometimento da segurança e acesso não autorizado às informações da companhia;
- Mudanças não detectadas e não autorizadas em ambiente de produção.

5. Medindo a eficiência dos controles

A eficiência e a eficácia deste processo podem ser medidas pela implantação de alguns indicadores de desempenho, a saber:

- Número de falhas graves ou erros de dados causados por uma especificação imprecisa ou uma avaliação de impacto incompleta;
- Volume de retrabalho em aplicações ou infraestrutura causado pela especificação inadequada de mudanças;
- Percentual de mudanças que seguem o processo formal de controle de mudanças.

6. Pergunta para pensar

Um processo é fruto de “entradas” e “saídas”. Ao se implantar um processo para gestão de mudanças, quais seriam as principais fontes dentro da TI e do negócio a serem consideradas? Considerando o CobiT como modelo, consulte os processos PO1, PO4, PO6, PO6 ,PO7, PO8, PO9, PO10, DS3, DS5, DS8, DS9 e DS10.

Leitura recomendada:

CobiT® Mapping Documents. Disponível em: <http://www.isaca.org/cobitmapping>.

Capítulo 9

Aspectos jurídicos do PESI²

Renato Opice Blum

Juliana Abrusio

1. Introdução

No mundo moderno, o bem mais valioso é a informação. As empresas estão preocupadas com o chamado “capital intelectual”. Tudo o que se quer evitar é a ocorrência do dano, aqui entendido como qualquer evento que atinja a propriedade imaterial da empresa, causando-lhe prejuízos.

Muitas vezes tais lesões são irreparáveis, vez que se está diante de um patrimônio que não comporta a simples devolução da coisa móvel. Diante de tal complicação, questiona-se a qual tutela legal as empresas podem recorrer para se protegerem da melhor forma possível. E mais, quais os procedimentos jurídicos devem ser incorporados ao mundo corporativo visando não somente prevenir o evento danoso, mas, também, municiar a empresa de provas contra futuros processos judiciais.

É preciso adotar um Plano Estratégico da Segurança da Informação (PESI) para garantir o binômio “prevenção e reação”. O primeiro é para evitar a ocorrência de fraudes, invasões, descuido de funcionários, condutas de má-fé dos *insiders*, sabotagem, concorrência desleal, fraudes eletrônicas etc. O segundo, como dito, para cercar a parte lesada – no caso, a empresa que já sofreu o ataque – de todas as provas possíveis para o processo judicial. Há, ainda, um terceiro requisito, não menos importante, que, ao lado do binômio “prevenção e reação”, é essencial para a vida de uma empresa bem preparada em sede de segurança da informação, ou seja, a condição em que se encontra toda estrutura de tecnologia da informação da empresa, para, se preciso for, periciá-la. É dizer, a condição da empresa em responder a incidentes e gerar provas diante de tais incidentes, de modo a coletar as provas relacionadas corretamente, para que não sejam desconsideradas no futuro.

2. A estratégia da organização frente às normas de segurança

As questões relacionadas à segurança da informação conquistaram lugar de destaque nas estratégias corporativas em âmbito mundial. Proteger e conservar a informação das inúmeras ameaças tornou-se essencial para garantir a continuidade do negócio, minimizando riscos e maximizando o retorno sobre os investimentos.

Diversas normas regem os procedimentos relativos à segurança da informação. Entre elas, a ABNT ISO/IEC 27001, ABNT ISO/IEC 27002, e outras tais como a Basiléia II e a Sarbanes-Oxley. Porém, não podemos esquecer que o universo corporativo está alocado em um Estado de direito, onde o exercício aos direitos sociais e individuais é assegurado, como valores supremos da sociedade, por meio de vasta legislação.

A adoção e a implantação do “Código de práticas para a gestão da segurança da informação” devem estar obrigatoriamente alinhadas às leis, estatutos, regulamentações e obrigações contratuais inerentes,³ sob pena de sofrer as sanções legalmente previstas. Em que pese referidas práticas estarem restritas ao universo corporativo, em hipótese alguma se deve deixar de considerar os aspectos legais envolvidos.

3. Conformidade com requisitos legais

A primeira grande preocupação no assunto é a conformidade com a legislação pátria vigente, incluindo todas as leis trabalhistas, civis, criminais e administrativas. É preciso repelir a violação de qualquer legislação, bem como de estatutos, regulamentações e obrigações contratuais inerentes aos requisitos de segurança da

²Plano Estratégico da Segurança da Informação.

³Legislação: conjunto de leis decretadas ou promulgadas em um país, disciplinando matéria em caráter geral ou específico. Ex.: Constituição Federal, Código Civil, Código Penal, Consolidação das Leis do Trabalho, Lei do Software, Lei da Propriedade Industrial.

Estatutos: complexo de regras estabelecidas e observadas por uma instituição jurídica a serem adotadas como lei orgânica, que fixam os princípios institucionais de uma corporação pública ou privada. Ex.: Estatuto Social, Estatuto dos Funcionários Públicos.

Regulamentos: conjunto de normas ou regras, em que se fixam o modo de direção ou condução de uma instituição ou associação. Ex.: Regulamento de Segurança da Informação.

Obrigações Contratuais: obrigações oriundas de acordo de duas ou mais pessoas físicas ou jurídicas para entre si, constituir, regular ou extinguir uma relação jurídica. Ex.: Contrato de Compra e Venda, Contrato de Trabalho, Contrato com Empresas Terceirizadas.

informação. Anote-se, ainda, que é extremamente necessária a interligação entre o setor de auditoria e a área jurídica para terem a tranqüilidade de atuar conforme os ditames legais, sem incorrer em qualquer irregularidade.

O tipo de controle sugerido para a identificação da legislação vigente é fundamentado na verificação da documentação. A norma ABNT ISO/IEC 27002 preconiza que todos os requisitos estatutários, regulamentares e contratuais relevantes, bem como o enfoque da organização para atender tais requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação.

4. Regulamento Interno de Segurança da Informação

A organização deve aplicar, internamente, um documento apto a render-lhe a maior segurança possível, considerando os elementos de “prevenção”, “reação” e “condição forense”. Tal documento é conhecido como “Regulamento Interno de Segurança da Informação” (RISI), que constitui um conjunto de normas e regras de segurança da informação, que visam possibilitar o compartilhamento de informações dentro da infraestrutura tecnológica da organização, por meio de seus recursos computacionais.

Por “informação” deve ser entendido todo o patrimônio que se refere à cultura da organização ou ao seu negócio, podendo elas ser de caráter comercial, técnico, financeiro, legal, recursos humanos, ou de qualquer outra natureza que tenham valor para organização e que se encontrem armazenadas em seus recursos computacionais, com tráfego dentro da sua infraestrutura tecnológica.

A eficácia do regulamento depende da vinculação de todas as pessoas que mantêm contato com a organização, como empregados, prestadores de serviços, colaboradores.⁴ Assim, dentro do regulamento serão inseridas cláusulas relativas aos usuários da rede; senhas e amplitude de acesso a arquivos; controle de ameaças (vírus, crackers etc.); uso e instalação de software e hardware; utilização de equipamentos (computadores, impressoras, notebooks, smartphones etc.); procedimentos de acesso à internet e ao correio eletrônico; dentre outras.

5. Termo de Uso da Segurança da Informação

O “Termo de Uso de Segurança da Informação” (TUSI) também deve ser utilizado pela organização em conjunto com o RISI. O TUSI consiste em um compromisso assumido, individualmente, de forma expressa e escrita, pelos empregados, prestadores de serviços ou colaboradores, declarando estarem subordinados ao cumprimento das atribuições e responsabilidades advindas do RISI.

O TUSI é um documento importante à medida que garante a ciência das partes e poderá ser um excelente meio de prova, já que a pessoa se compromete por escrito. Ambos os documentos (RISI e TUSI) devem ser feitos com base nas mais atualizadas e confiáveis diretrizes de segurança mundiais, em especial a NBR ISO IEC 27002 e NBR ISO IEC 27001; na reforma do *Bürgerliches Gesetzbuch* (BGB) envolvendo documentos eletrônicos; no *Data Protection Working Party*, da União Européia, no *Statuto dei Lavoratori Italiani*; *Codice della Privacy* (Itália); Diretiva 2002/58/CE; Decreto Legislativo Italiano n.196 de 30 de junho de 2003 (*Misure di sicurezza*) e outros.

O RISI e o TUSI são os dois principais instrumentos jurídicos que compõem o PESI. Tais instrumentos resguardam não somente a organização, como também os administradores, os empregados e terceiros envolvidos em todas as esferas do direito.

6. Monitoramento de e-mails

O monitoramento de *e-mails* pode ser considerado como válido, desde que se atente a alguns requisitos. O Tribunal Superior do Trabalho, bem como os Tribunais Regionais do Trabalho brasileiros, vêm cristalizando a jurisprudência pátria no sentido de permitir o monitoramento dos meios eletrônicos da corporação para verificação do mau uso dos recursos de processamento da informação, o que possibilita, inclusive, a dispensa

⁴Empregados: considerando os prepostos da empresa que mantêm vínculo empregatício (CLT).

Prestadores de serviços: tendo em vista os prepostos de empresas contratadas, ou autônomos, que, de qualquer forma, estejam alocados na prestação de algum serviço em favor da empresa, por força de contrato de prestação de serviços, sem qualquer vínculo empregatício.

Colaboradores: outras pessoas como estagiários, cooperados e quaisquer terceiros que não se enquadrem no conceito de empregado ou prestador de serviços, mas que, direta ou indiretamente, exerçam alguma atividade dentro ou fora da empresa.

motivada por justa causa, inexistindo expectativa de privacidade por parte dos empregados da organização.

Acertadamente e a fim de evitar maiores discussões, é salutar que todos os usuários estejam conscientes do escopo de suas permissões de acesso e da monitoração realizada, o que pode ser viabilizado por meio de registro de autorizações escritas, devidamente assinadas por funcionários, fornecedores e terceiros envolvidos na organização, o que, mormente, é denominado de “Termo de Uso dos Sistemas de Informação”.

Recomenda-se, ainda, a apresentação de mensagem no momento da conexão inicial, advertindo ao usuário que o recurso de processamento da informação utilizado é de propriedade da organização e que não são permitidos acessos não-autorizados, necessitando de confirmação do usuário para o prosseguimento do processo de conexão.

7. Responsabilidades

O Código Civil Brasileiro, em seu art. 186, prevê a responsabilidade civil para aquele que viola direito ou causa dano a outrem, ainda que exclusivamente moral, por ação ou omissão voluntária, negligência ou imprudência, configurando-se ato ilícito, ficando obrigado a repará-lo independentemente de culpa, quando a atividade normalmente desenvolvida pelo autor do dano implicar por natureza em risco para outrem (art. 927, CC). Ainda na mesma trilha de entendimento, referido diploma legal preconiza, por meio do art. 1.016, a responsabilidade solidária dos administradores perante a sociedade e terceiros prejudicados no desempenho de suas funções.

Tais dispositivos demonstram de forma evidente a necessidade de resguardar juridicamente a corporação na gestão da segurança da informação, considerando-se que o objetivo maior das corporações na adoção da norma é a minimização dos riscos inerentes e não a geração de mais riscos.

Especificamente, em relação aos gestores da segurança da informação, estes estão ligados ao complexo de atividades relacionadas às diversas formas de utilização dos recursos proporcionados pelo computador, e como conseqüência, são responsáveis por proporem soluções capazes de maximizar o uso das ferramentas tecnológicas, bem como por sugerir medidas tendentes a evitar riscos dos mais diversos tipos para a organização, seja com relação à perda de dados, vírus, entre outros. O gestor tem o dever de promover o processo de conscientização e treinamento.

Assim, é recomendável que elabore uma espécie de relatório com a descrição da atual situação da empresa, no que tange à tecnologia empregada. Aliás, a Resolução 3.380 do BACEN, de 2006, inauguradora da primeira fase da adoção da Basileia II no Brasil, acentua a preocupação com a elaboração de relatórios, contendo as questões críticas das instituições financeiras.

É sabido que ninguém pode alegar em sua defesa o desconhecimento das normas vigentes. Portanto, o gestor deverá estar sempre atualizado acerca dos aspectos jurídicos que envolvem sua profissão. É muito importante que exista este tipo de conhecimento, pois o gestor de segurança poderá ser responsabilizado, civil e criminalmente, por seus atos, seja em virtude da conivência com certos comportamentos, ou ainda, por não ter agido com o cuidado e diligência do que se espera normalmente do profissional.

Ademais, o empregado, em razão do cargo ou função que ocupa, poderá tomar conhecimento de informações sigilosas, como componentes de fórmulas criadas por empresas que elaborem produtos; detalhes sobre a vida de clientes que sejam partes em demandas judiciais; dados cadastrais de clientes; planejamento para desenvolver a atividade comercial durante o ano; entre outras.

Por tais motivos, alguns dispositivos do Código Penal poderão ter incidência, conforme listado abaixo:

Divulgação de segredo

Art. 153 – Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:

Pena – detenção, de um a seis meses, ou multa.

§ 1º Somente se procede mediante representação.

§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:

Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

§ 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

Divulgação de segredo

Art. 154 – Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Parágrafo único – Somente se procede mediante representação.

Não obstante a isso, pode acontecer de um funcionário acessar, sem a devida autorização, documentos ou informações confidenciais que não lhe seja permitido o conhecimento. Assim, ocorrerá o descumprimento de ordens de seu empregador ou superior hierárquico, podendo o empregado ser demitido por “justa causa” em virtude de ato de indisciplina ou de insubordinação (artigo 482, alínea “h” da CLT).

Ademais, o gestor pode se deparar com concorrência desleal, que são as práticas antiéticas ou ilegais no exercício da atividade econômica, previstas no art. 195⁵ da Lei 9.279/96.

8. Implementação

Em conclusão às ponderações legais colacionadas, recomenda-se que as principais posturas a serem adotadas pela organização sejam:

- Divulgação de política de conformidades com direitos de propriedade intelectual, que contenha definição expressa sobre o uso legal de software. Será adequado que a política mencione a legislação vigente sobre o tema;
- Aquisição de *software* somente por meio de fontes idôneas para assegurar que o direito autoral não seja violado;
- Conscientizar os empregados por meio de políticas e adotar ações disciplinares em face dos que violarem tais políticas. Seria adequado que as ações disciplinares culminem até em demissão por justa causa;
- Manter o registro de ativos e identificar todos os possivelmente relacionados aos direitos de propriedade intelectual. Assim, deve-se verificar e registrar tudo dentro da organização que esteja submetido à legislação pertinente;
- Manter provas da propriedade de licenças, tais como contrato de licença, recibos, manuais, discos mestres;
- Implantação de controles para que o número de usuários permitidos seja compatível com o número de licenças adquiridas; tal recomendação é extrema importância, haja vista o disposto na Lei n.º 9609/98 (lei do *software*);

⁵Art. 195. Comete crime de concorrência desleal quem:

I – publica, por qualquer meio, falsa afirmação, em detrimento de concorrente, com o fim de obter vantagem;

II – presta ou divulga, acerca de concorrente, falsa informação, com o fim de obter vantagem;

III – emprega meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem;

IV – usa expressão ou sinal de propaganda alheios, ou os imita, de modo a criar confusão entre os produtos ou estabelecimentos;

V – usa, indevidamente, nome comercial, título de estabelecimento ou insígnia alheios ou vende, expõe ou oferece à venda ou tem em estoque produto com essas referências;

VI – substitui, pelo seu próprio nome ou razão social, em produto de outrem, o nome ou razão social deste, sem o seu consentimento;

VII – atribui-se, como meio de propaganda, recompensa ou distinção que não obteve;

VIII – vende ou expõe ou oferece à venda, em recipiente ou invólucro de outrem, produto adulterado ou falsificado, ou dele se utiliza para negociar com produto da mesma espécie, embora não adulterado ou falsificado, se o fato não constitui crime mais grave;

IX – dá ou promete dinheiro ou outra utilidade a empregado de concorrente, para que o empregado, faltando ao dever do emprego, lhe proporcione vantagem;

X – recebe dinheiro ou outra utilidade, ou aceita promessa de paga ou recompensa, para, faltando ao dever de empregado, proporcionar vantagem a concorrente do empregador;

XI – divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

XII – divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; ou

XIII – vende, expõe ou oferece à venda produto, declarando ser objeto de patente depositada, ou concedida, ou de desenho industrial registrado, que não o seja, ou menciona-o, em anúncio ou papel comercial, como depositado ou patenteado, ou registrado, sem o ser;

XIV – divulga, explora ou utiliza-se, sem autorização, de resultados de testes ou outros dados não divulgados, cuja elaboração envolva esforço considerável e que tenham sido apresentados a entidades governamentais como condição para aprovar a comercialização de produtos.

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.

§ 1º Inclui-se nas hipóteses a que se referem os incisos XI e XII o empregador, sócio ou administrador da empresa, que incorrer nas tipificações estabelecidas nos mencionados dispositivos.

§ 2º O disposto no inciso XIV não se aplica quanto à divulgação por órgão governamental competente para autorizar a comercialização de produto, quando necessário para proteger o público.

- Proceder constantes verificações para que somente sejam instalados produtos de *software* autorizados e licenciados na corporação;
- Criar normas para manutenção das condições adequadas de licenças;
- Adotar contratos para transferência de *software* para terceiros;
- Utilizar ferramentas de auditoria adequadas;
- Identificar e respeitar termos e condições para *software* obtido a partir de redes públicas;
- Não duplicar, alterar para outro formato ou ainda extrair registros de filme ou áudio além do que permitido pela lei de direito autoral, qual seja, Lei n.º 9610/98;
- Não copiar livros, artigos ou outros documentos, fora dos padrões admitidos pela Lei de Direitos Autorais n.º 9610/98.

Capítulo 10

Computação Forense

Giuliano Giova

"A informação está substituindo a autoridade".

Peter Druker

1. O poder do faraó

Nada melhor do que começarmos esta rápida viagem no mundo da perícia forense tendo como guia o professor Peter Druker, mente brilhante que nos explica os segredos que entrelaçam poder e informação.

Raramente houve poder maior do que aquele que emanava do faraó. Não era apenas um rei no Egito antigo, podia decidir sozinho o destino da nação e de cada um dos seus habitantes. Dono de autoridade absoluta e cercado por milhares de escravos, o faraó era capaz de construir monumentos que assombraram o mundo, administrar sozinho a justiça, desenvolver as ciências e conduzir os exércitos; não bastasse isso, era considerado o verdadeiro e único representante de Deus na terra.

Exatamente nesse ponto, os ensinamentos de Druker nos ajudam a compreender que, por trás de tanto poder, havia a posse e utilização inteligente de informações tão importantes que seriam consideradas privilegiadas por qualquer bolsa de valores atual.

O observador mais atento percebia que o poder dos faraós vinha, de fato, dos seus sacerdotes, os verdadeiros conhecedores do sistema de construção das pirâmides, da astronomia que trazia alimento e prosperidade ao prever secas e o momento para plantar e colher e, ainda, conhecedores da medicina que aliviava o sofrimento do povo.

Os sacerdotes eram os únicos que sabiam ler escritos antigos sobre matemática, química e posição dos astros. Guardiões dos grandes segredos, eles interpretavam sonhos, dominavam magias que curavam ou amaldiçoavam e conduziam rituais. Assim, a felicidade e a própria sobrevivência do faraó e do seu reino dependiam bem mais do conhecimento detido pelo sacerdote do que do poder absoluto do seu governante, ou seja, mesmo na antiguidade posse e utilização da boa informação era mais importante do que apenas ser ungido como autoridade.

2. Milhares de anos depois

Foram precisos alguns milhares de anos para que a humanidade conseguisse produzir máquinas eficazes para o tratamento de informações. Nas décadas de 1950 e 1960, imensos computadores, os famosos *mainframes*, ofereceram um novo tipo de magia sacerdotal: coletar e processar milhões de dados e fornecer serviços de processamento de dados simultaneamente a legiões de usuários. O Eniac, o *System/360* da IBM e outros da Burroughs e HP forneceram a governos e empresas capacidade de atender cada vez mais clientes e processar mais serviços, levando à redução de custos via ganhos de escala e, paulatinamente, à substituição do trabalho braçal por processos automáticos, tendo o desemprego como efeito colateral.

Nesta época, as diretorias de informática e O&M (organização e métodos) ostentavam o título de mais poderosas, eleitas pontas de lança da alta administração para modificar e desenvolver comportamentos na organização, novas guardiãs da informação e entes responsáveis por sua aplicação nas questões práticas da empresa, mostrando "a cara do dono". Novamente, presenciamos o efeito Druker, pois vimos o poder dos conselhos e da presidência executiva materializa-se pelas áreas que dominam e aplicam as informações relevantes.

Como consequência, as áreas de informática e O&M inicialmente cresceram muito, com quadros que chegavam a centenas ou milhares de funcionários, mas algum tempo depois não mais davam conta do recado. Acumulavam anos de *backlog*, enormes listas de serviços pendentes sem previsão razoável de atendimento, tornando-se mais um problema no desenvolvimento da empresa do que uma solução confiável.

A contrapartida veio naturalmente, ao longo dos anos 1970 e 1980, com o surgimento comercial do microcomputador, equipamento inicialmente desacreditado para aplicações mais sérias na empresa, mas que logo se impôs ao trazer autossuficiência informática aos usuários finais.

A despeito das previsões catastróficas no quesito segurança da informação, pelo alto risco de perda ou cópia indevida dos dados, o novo equipamento pessoal multiplicou-se rapidamente porque os usuários sentiram-se livres para criar suas próprias aplicações sem ter de negociar prioridades e prazos com a área de desenvolvimento de sistemas. Usuários finais dominaram a tecnologia e desenvolveram seus próprios sistemas de pequeno e médio porte, muitas vezes em Lotus 123, Excel, Access ou mesmo algum dialeto *xBase*. Gerentes de áreas administrativas especializavam-se na tarefa de controlar e consolidar informações. Muitas dessas aplicações nasceram timidamente *stand-alone* e depois foram se integrando, entre si e com *mainframes*.

O resultado não poderia ser outro: a partir do momento em que a integração dos sistemas mostrou-se confiável, foram demitidos gerentes que se dedicavam a consolidar informações operacionais das suas áreas (vendas, compras, recursos humanos etc.) e repassá-las aos colegas e superiores. Os sistemas integrados mostraram-se mais eficazes e confiáveis do que as pessoas na tarefa de sincronizar metas organizacionais, áreas funcionais e projetos, fortalecendo a adoção de estruturas matriciais em detrimento das puramente hierárquicas, e vindas de encontro a movimentos como *rightsizing*, *downsizing* e redução de níveis hierárquicos.

Nesta nova fase, o controle efetivo sobre as informações relevantes da empresa moveu-se para as mãos dos executivos responsáveis pelo *core business*. Visivelmente, o centro do poder abandonou o CPD a partir do momento em que deixou de propor e tornar efetivos “novos negócios” que faziam a empresa galgar etapas e diferenciar-se no mercado. Salta aos olhos quando a área de tecnologia mostra-se mera hospedeira e mantenedora de dados e *software*, travestida de coadjuvante focada apenas na tarefa de assegurar o nível dos serviços prestados. Perdeu a posição de líder e somente presta serviços para os verdadeiros donos do poder, as áreas fim da empresa.

Chegamos, então, aos anos 1990 e ao início de um novo século presenciando algumas novas magias no jogo da informação e do poder. Computadores e redes de comunicação alcançaram desempenhos jamais imaginados. Sistemas tornaram-se flexíveis e capazes de se ajustar ao desejo individual de cada usuário final, uma liberdade de escolha jamais vista. Não apenas esvaíram-se as previsões catastróficas que gravavam sobre a cabeça dos rebeldes que ousaram afastar-se das rigorosas normas, procedimentos e sistemas impostos pela cúpula administrativa, como também se abriram inúmeros novos horizontes na esteira da internet. O pêndulo do poder desloca-se um pouco mais na direção do usuário final e da vontade do mercado, os verdadeiros detentores das informações relevantes.

3. E hoje?

Mesmo computadores mais simples, adquiridos em supermercados, apresentam desempenho impensável há poucos dias. No prazo de um segundo, duração de uma simples piscadela de olho, equipamentos deste tipo processam dois bilhões de instruções (2.0 GHz), vasculham meio bilhão de caracteres (HD 500 MB), transmitem quase um bilhão de bits (rede gigabit) e podem interagir com um bilhão de computadores (IPv6). São frutos da nanotecnologia, com componentes medidos na escala de um bilionésimo de metro.

Software e dados abandonam os ultrapassados *desktops* e se teletransportam no melhor estilo do Capitão Kirk⁶ para celulares, automóveis, geladeiras, controles de acesso, *outdoors* e equipamentos médicos. Atravessam o mundo na velocidade da luz, saltando de *chip* em *chip*, seus abrigos preferidos, onipresentes em qualquer caminho escolhido, seja em terra firme, nas profundezas dos oceanos ou no espaço sideral.

Como que possuídas, pessoas relegam a vida no mundo dito real e se sentem párias se não passam dia e noite ligadas a um sistema de mensagens, se escasseiam os torpedos ou se não há novos *scraps* em seu perfil. Jovens não podem ser considerados um bom partido enquanto não forem prospectados via *webcam* ou se tiverem poucos amigos virtuais. Governos, empresas e igrejas tornam-se inúteis sem conexões eletrônicas.

Pela primeira vez após milhares de anos, a humanidade abandona o mundo real e pisa com ambos os pés no mundo virtual.

⁶Contos escritos por Gene Roddenberry.

4. Revisitando o velho conflito de interesses

Esta breve sinopse nos ajudou a recordar que, desde a antiguidade, a informação sempre foi personagem de destaque em todas as disputas pelo poder. Mostrou-nos, ainda, que nessa longa jornada o domínio sobre a informação nunca foi pacato; ao contrário, esteve imerso em disputas lancinantes das quais não escaparam ilesos bruxas, Galileu, políticos, renomados executivos ou dedicados funcionários.

Porém, curiosamente, algo diferente parece ocorrer hoje em dia. Fica flanando entre nós um sentimento geral de que neste novo mundo digital não há, ou pelo menos não deveria haver, grandes disputas sobre a criação, posse e uso de informações. Um espírito adolescente de que não haveria necessidade de limites e se pode tudo, afinal o noticiário mostra diariamente que qualquer um invade computadores dos serviços secretos ou opera rádios piratas.

Um olhar mais atento logo percebe que este sentimento não é aderente aos crescentes índices que medem a quantidade de processos judiciais sobre conflitos, erros e procedimentos indevidos e ilícitos praticados por meios eletrônicos. É inexorável que provedores de informações, construtores de *software*, gestores de sistemas e operadores do direito busquem compreender esse aparente paradoxo.

Os grandes pensadores econômicos nos ensinaram, há muito tempo, que os bens são escassos e que, por isso, têm custo de oportunidade e preço de mercado. Em outras palavras, tudo o que vale a pena não escapa da sina de ser almejado e disputado por dois ou mais indivíduos. Este é o real significado do termo "conflito de interesse", a disputa entre dois ou mais indivíduos pela posse e uso de bens escassos, bastando lembrar quantas contendas, latrocínios e guerras já resultaram desta disputa.

O comportamento é conhecido desde a pré-história, uma vez que sempre foi trabalhoso, complexo e demorado reproduzir objetos do dito mundo real, como armas para caçar alimentos, arados, relógios ou hidroelétricas. Imagine quantos insumos são necessários para copiar uma simples bolsa, desde a obtenção de todas as matérias-primas e a realização das sucessivas transformações até que seja obtida uma nova unidade, pronta e embalada. Assim, parece explicável que sejam freqüentes conflitos de interesse relacionados a bens do mundo físico, levados à tutela do Estado.

Todavia, ao contrário do que ocorre no mundo real, replicar um objeto digital, parece ser uma tarefa muito simples, barata e sem riscos. Bastam comandos triviais como "copiar" e "colar", por mais complexo que seja o componente digital reproduzido. Fica o sentimento ingênuo de que podem ser reproduzidos, quase que instantaneamente e de graça, milhões de objeto virtuais, um mundo nababesco com infinita fartura, a verdadeira universalização das benesses ao alcance de um simples clique.

O paradoxo está, então, em saber por qual motivo surgem tantos conflitos de interesse no mundo virtual se, aparentemente, nele existiria imensa fartura objetos digitais? Para ilustrar esta visão, qual motivo poria indivíduos em conflito pela posse do ar atmosférico se ele é um bem largamente disponível e sem preço de mercado, pelo menos por enquanto?

Mentes brilhantes debruçam-se sobre tais temas. Muitos defendem regras e sistemas mais rígidos para proteger e manter motivados criadores e empreendedores que continuamente revolucionam a tecnologia e geram riquezas para a humanidade. Outros pretendem reduzir as restrições legais sobre direitos autorais, marcas e bens universais como o espectro de radiofrequência, afirmando que somos todos piratas à luz da legislação atual. Muitas outras frentes de batalha convivem no mesmo caldeirão virtual, alimentadas por personagens tão heterogêneos como *crackers*, pedófilos, estelionatários, chantagistas, seqüestradores, traficantes, sabotadores, espíões, sócios infiéis, funcionários revoltados, enamorados ciumentos e espertalhões de todo o tipo.

Este confronto conceitual, cultural e financeiro com tempero *high-tech* é cada vez mais palpitante, pois a solução dos conflitos que embutem alta tecnologia jamais será tarefa simples ou rápida. Devemos primeiramente considerar que na análise destes conflitos não pode faltar seu principal elemento diretor: o conceito de nação, intimamente relacionado aos costumes dos seus habitantes e ao conjunto de leis fundamentais que regem a vida e as relações entre governo, pessoas e empresas.

Em segundo lugar, é preciso considerar que a grande velocidade da evolução tecnológica impede que a legislação e até mesmo simples normas técnicas prevejam e definam regras para as novas situações onde podem ocorrer conflitos. Em terceiro lugar, a sobrevivência da humanidade e das empresas depende de existirem con-

tínuas inovações nas relações sociais e nos modelos de negócios, impulsionadas e demandadas ciclicamente pelo próprio avanço tecnológico.

Finalmente, devemos ter presente que os dispositivos digitais tornaram-se essenciais em todas as atividades humanas e passaram a ser foco de tantos interesses distintos que projetos de lei sobre crimes informáticos ficam anos se entrecrocando em intermináveis debates parlamentares. O resultado geral é que se avolumam as questões sobre alta tecnologia a serem resolvidas pelos tribunais com o apoio de especialistas, tanto peritos oficiais dos institutos de criminalística como peritos judiciais nomeados pelos magistrados entre os profissionais acreditados nos tribunais. Mais ainda, este cenário agrava-se rapidamente devido à crescente complexidade dos ambientes a serem examinados, tornando cada vez mais difícil, cara e demorada a missão dos operadores do direito, dos peritos e assistentes técnicos das partes.

Tarefas que antes eram cumpridas por apenas um perito, muitas vezes agora requerem equipes multidisciplinares com profissionais como cientistas da computação, engenheiros de telecomunicações, contabilistas e médicos, afinal tudo se tornou digital. Além disso, não bastam mais as competências pessoais porque os imensos volumes de dados, as inúmeras formas de armazenamento e a completa mobilidade dos dispositivos requerem métodos e ferramentas sofisticados de análise que estão disponíveis apenas nos laboratórios mais bem equipados, muito distantes dos milhares de comarcas espalhadas pelo País.

Como veremos mais adiante, se a tarefa pericial não for corretamente preparada e conduzida, a complexidade inerente à tecnologia da informação e às telecomunicações aumentará muito o risco de que culpados sejam considerados inocentes ou, pior, que inocentes sejam considerados culpados.

5. Computação forense

Em termos gerais, podemos considerar que computação forense⁷ consiste no emprego de conhecimentos sobre computação e telecomunicações para responder questionamentos jurídicos. Trata-se, portanto, do emprego do método científico, um sistema racional para adquirir conhecimento em oposição à mera opinião ou dogma, e do próprio conhecimento resultante desse método, adequadamente organizado e continuamente revisado. Não é marcadamente ciência pura, mas ciência aplicada ou, melhor ainda, um campo interdisciplinar que faz uso das descobertas de outras ciências e áreas como direito e computação para atender necessidades específicas da justiça.

O termo abrange, também, comunidades técnicas e científicas que atuam nas diversas disciplinas e campos de estudos fundamentais ou limítrofes à computação forense, inclusive colaborando com ela por meio de conhecimento prático, não necessariamente científico, e algumas vezes mais próximo às inovações empíricas da indústria e dos costumes policiais e judiciais. Entre as comunidades, podem ser consideradas também as diversas instituições voltadas à comunicação técnica e científica, à manutenção de grupos de pesquisa, aos estudos usualmente em nível técnico ou de pós-graduação, à elaboração de normas e padrões e à certificação de profissionais.

O termo forense⁸ remete à ampla discussão pública sob o comando do direito. Neste caso, dos fatos sobre tecnologia da informação e telecomunicações, em respeito ao princípio constitucional do contraditório que assegura a toda a pessoa em juízo o direito de ampla defesa ou a proteção do direito de quem busca a tutela do Estado. Portanto, fica claro, por exemplo, que não pode ser considerado suficiente para se apurar a verdade dos fatos o simples apontamento de um endereço IP (Internet Protocol) no cabeçalho técnico de uma mensagem ou no log de um computador servidor. É essencial que estes vestígios sejam submetidos à ampla discussão técnica forense para que, por meio de um conjunto de atividades de verificação e demonstração se chegue à verdade dos fatos, à produção das provas.⁹

Ainda com base no exemplo anterior, há alguns anos o debate técnico em busca de evidências possivelmente estaria focado no conjunto de protocolos conhecidos pela sigla TCP/IP¹⁰ utilizados para a comunicação

⁷Forense computacional, entre outros termos.

⁸Do Latim: *forēnsis* – público, relativo aos tribunais; *foro* – lugar onde se discutem os assuntos públicos.

⁹Dinamarca, 2005.

¹⁰TCP: Transmission Control Protocol (Protocolo de Controle de Transmissão); IP: Internet Protocol (Protocolo de Interconexão).

entre computadores em rede, mapeando-se todo o trajeto da mensagem, desde o computador emitente até aquele de destino. Porém, com a ampla disseminação da computação móvel, provavelmente o endereço IP de origem da mensagem apontará apenas para o computador *gateway* da empresa operadora de telecomunicação móvel celular, dado insuficiente para identificar o equipamento celular emitente da mensagem, uma vez que o mesmo sistema pode ser utilizado por diversos usuários ao mesmo tempo.

Novos conhecimentos técnicos, investigações e verificações serão agora necessários para se comprovar a origem da mensagem, pois parte do seu trajeto ocorre por circuitos e tecnologias próprios do sistema móvel celular. A própria determinação da localização geográfica de emissão da mensagem ganha novas dimensões, implicando, especialmente para casos mais críticos, no estudo de elementos técnicos inusitados até então, como estações rádio base, azimutes e reflexão de ondas eletromagnéticas.

6. Princípio de Locard

Edmund Locard, cientista forense e diretor de um dos primeiros laboratórios europeus nesta área, enuncia que, na cena de um crime, sempre existirá algum rastro proveniente da permuta de materiais como fibras ou fios de cabelo, quando houver contato entre itens distintos.

O princípio de Locard aplica-se perfeitamente aos eventos do mundo digital, pois computadores que processam bilhões de instruções por segundo certamente registrarão alguma mudança em função de qualquer contato externo, seja proveniente de uma tecla pressionada, da movimentação do mouse, da conexão de um *pendrive*, da execução de *software* ou de um acesso via rede. A crescente capacidade de processamento e de armazenamento dos computadores fez com que tanto o *software* básico quanto os aplicativos aumentassem muito seu nível de *log*, passando a coletar e registrar automaticamente grande quantidade de informações históricas sobre os eventos que ocorrem no equipamento, material relevante para o investigador forense atento ao princípio de Locard.

7. Heisenberg e a física quântica

Talvez, Locard tenha se inspirado nos estudos de Heisenberg sobre o observador alterar os eventos que observa na dimensão da física quântica. No mundo digital, ocorre algo similar. Por isso, é fundamental recordar que não apenas o suspeito deixa rastros na cena do crime virtual, mas o próprio investigador também deixa ou modifica rastros ao fazer suas observações.

Muitas vezes, cuidados elementares previnem a contaminação da cena do crime, especialmente no volátil e complexo mundo digital. Ao suspeitar que algo indevido ou ilícito possa estar ocorrendo na empresa, seus gestores e funcionários devem saber que averiguar os fatos sem a metodologia correta certamente fará perder evidências essenciais, pela contaminação da cena do crime. O próprio especialista pode ser traído pela urgência de apresentar respostas ao comando da empresa ou repor a operação normal de um sistema afetado. Além da sempre possível perda de vestígios, mesmo aqueles preservados e submetidos à autoridade policial ou ao judiciário terão seu valor probante reduzido se tiverem sido contaminados, situação que pode se revelar durante os debates forenses. Portanto, desde as primeiras investigações até a coleta e exame de evidências, é essencial que sejam adotados métodos e ferramentas adequados e confiáveis.

8. Cadeia de custódia

A metodologia e as melhores práticas periciais determinam que todos os eventos relacionados à investigação de incidentes e à coleta de vestígios devem ser detalhadamente registrados. Esta postura é ainda mais relevante porque algumas vezes é inevitável que o observador contamine ou transforme a cena do crime. O mecanismo para este registro denomina-se cadeia de custódia, um documento onde devem ser claramente e detalhadamente registrados todos os vestígios encontrados, toda e qualquer manuseio que ocorrer e seu objetivo, as pessoas que com eles tiveram contato, além de data, hora e local de cada evento.

A existência de cadeia de custódia confiável é fundamental para que as evidências resultantes não possam ser facilmente contestadas. Um dos elementos importantes na cadeia de custódia de componentes digitais é a geração do código *hash*, um pequeno conjunto de caracteres digitais que representa um conjunto bem maior de

bytes armazenados em um disco rígido ou em um arquivo, por exemplo. Tendo-se o *hash*, é possível demonstrar em qualquer momento posterior que o conjunto original de dados permanece inalterado.

Portanto, tenha sempre muita atenção com evidências que não estejam acompanhadas por registro da cadeia de custódia original e confiável.

9. Quesitos

Quesitos são perguntas formuladas pelo juiz ou pelas partes ao perito para a instrução da causa em questões técnicas. Geralmente, quesitos são apresentados logo após a decisão de se realizar a perícia técnica, um momento preparatório no qual, provavelmente, ainda não são conhecidas todas as variáveis e dificuldades que deverão ser enfrentadas até que se chegue à verdade dos fatos.

Este quadro mostra-se mais grave à medida que os novos computadores possuem capacidade enorme de armazenamento, obrigando o perito a examinar bilhões de *bytes* para tentar encontrar alguns poucos *bytes* de interesse pericial, muitas vezes, travestidos por codificações e formatações inesperadas. Junte-se a isso o frequente cenário de sobrecarga de serviço e falta de ferramentas periciais adequadas. Resulta clara a importância de que quesitos sejam sempre muito bem formulados, pois se forem apresentados quesitos vagos ou incompletos o resultado do trabalho pericial será inaproveitável ou, ainda mais grave, levará o julgador e as partes a erro.

Cumpra sempre recordar que quesitos são perguntas cuja resolução requer esforço mental e trabalho braçal de investigação e análise. Portanto, devem ser adequadamente detalhados para assegurar que os inúmeros componentes de um sistema digital tenham sido efetivamente e corretamente examinados.

10. Exames técnicos

Os exames periciais são procedimentos de investigação técnica e científica que têm por objetivo responder os questionamentos jurídicos sob um prisma tipicamente multidisciplinar. Certamente, por um lado, cabe ao perito restringir-se à determinação judicial e aos quesitos recebidos, sem devaneios ou incursões estranhas à missão que lhe foi confiada pelo magistrado. Por outro lado, é responsável eticamente e tecnicamente, inclusive frente ao seu conselho profissional, pela busca da verdade registrada nas peças examinadas. Nem sempre é fácil compatibilizar estes dois aspectos do trabalho pericial. Muitas vezes, o primeiro vestígio encontrado não revela a verdade real dos fatos e pode até mesmo levar o perito e o julgador a erro.

Por exemplo, ao encontrar erro no código fonte de um *software*, pode haver a tendência imediata de se atribuir a falha ao programador, esquecendo-se que ele não trabalha ou não deveria trabalhar sozinho. Ao contrário, o programador está submetido a uma estrutura técnica de supervisão, treinamento, metodologia, normas, ferramentas, especificações, testes e homologações; portanto, talvez seja aquele com menor responsabilidade pelo problema ocorrido. Percebemos facilmente que a análise pericial pode focar não apenas o componente específico, mas, também, todo o sistema dentro de uma visão multidisciplinar e abrangente, no sentido de reiterar incursões de análise e síntese até que a verdade real seja encontrada.

Outra falha típica ocorre, ainda como exemplo, na avaliação de sistemas de gestão, em embates entre empresas produtoras destes *softwares* e seus clientes. Algumas vezes, o perito limita-se a avaliar se os procedimentos operativos do sistema contestado apresentam interrupções ou erro nos dados ou nas regras de negócio. Mas o principal problema pode estar em níveis bastante distintos. Por exemplo, a própria oferta e contratação podem ter sido inadequados se o sistema tiver um projeto voltado à redução de custos e mão-de-obra, um antigo conceito de 50 anos atrás, e a empresa procurar, ao contrário, um sistema atual de gestão que lhe permita inovar continuamente, isto é, tornar-se uma nova empresa a cada novo dia, saltando etapas e superando os concorrentes. Nesse contexto, parece ter um peso bem maior avaliação da compatibilidade entre os objetivos da empresa e do sistema nas dimensões estratégica e tática.

Ainda no contexto da determinação dos fatos ocorridos e respectivas responsabilidades técnicas, não se pode deixar de avaliar a responsabilidade da estrutura organizacional nos atos inadvertidos, indevidos ou ilícitos que ocorram na empresa. Usualmente, cumpre ao perito a tarefa de apurar não apenas o evento no qual algum recurso da empresa foi utilizado indevidamente, mas, também, se a companhia foi zelosa ao estabelecer contratos, normas de uso, orientação e controle adequados quanto à sua infraestrutura.

Portanto, a investigação pericial torna-se cada vez mais sistêmica, estruturada e multidisciplinar no sentido de apurar a verdade real e as responsabilidades técnicas compartilhadas.

11. Laudo pericial

O objetivo final do laudo pericial é o magistrado, que poderá tomá-lo em consideração para seu convencimento. Cumpre recordar que o Brasil adota o princípio do livre convencimento motivado do julgador, significando que o juiz decide a causa de acordo com o seu livre convencimento, mas deve fundamentar e explicar o que decidiu no contexto do material probatório levado aos autos.

Disto resulta claro que um laudo pericial redigido conforme as melhores práticas da computação forense é elemento essencial para a qualidade da decisão do magistrado e até mesmo para a fundamentação da sua decisão. Infelizmente, não é esta a realidade de muitos laudos periciais apresentados em nossos tribunais. Descrevem os objetivos, as peças submetidas à perícia e as conclusões obtidas, mas falta-lhes a indispensável fundamentação técnica. Com isso, prejudicam ou até mesmo inviabilizam o contraditório, impossibilitam a avaliação da qualidade do trabalho pericial, tornam-se contestáveis e podem levar a graves erros.

Um laudo pericial bem elaborado apresenta fundamentação clara, técnica e facilmente compreensível e verificável até mesmo por leigos. A Associação Brasileira de Normas Técnicas (ABNT) indica que laudo é a peça na qual o perito relata o que observou e avalia fundamentadamente o valor de coisas ou direitos. Já o Conselho Regional de Engenharia e Arquitetura (CREA) esclarece que laudo é uma peça escrita, fundamentada, que expõe as observações e estudos efetuados. O dicionário Aurélio define que laudo é peça escrita, fundamentada, na qual os peritos expõem as observações e estudos que fizeram e registram as conclusões da perícia.

Assim, todas estas definições são unânimes ao impor a presença da fundamentação nos laudos pericial, sendo inaceitável que o perito simplesmente apresente suas conclusões sem que as evidências estejam preservadas, sem que as conclusões estejam fundamentadas e sem que os exames possam ser repetidos para validar os resultados obtidos.

12. Finalmente

Neste nosso breve trabalho, verificamos que a informação alcança valor cada vez maior, por ser elemento essencial para a diferenciação de empresas e das pessoas que sabem inovar, possibilitando-lhes saltar à frente dos concorrentes.

Constatamos que as medidas de segurança devem proteger a empresa, mas não podem bloquear a flexibilidade essencial para que a inovação flua livremente, senão ela sucumbirá rapidamente neste novo mundo virtual. O cenário tecnológico mundial, muito complexo, disperso geograficamente e com pouco comprometimento, aumenta fortemente o risco, impondo maior zelo e vigilância e, portanto, maiores custos com segurança preventiva e com a investigação de incidentes. O sistema judiciário passa a depender cada vez mais da avaliação feita por especialistas em alta tecnologia, contudo, a crescente complexidade dos dispositivos digitais encarece e sujeita o trabalho pericial a graves falhas, impondo à empresa e às pessoas medidas acau-teladoras no sentido de resguardar-se dos riscos digitais.

