

GESTÃO DA
SEGURANÇA
DA **INFORMAÇÃO**

UMA VISÃO EXECUTIVA

MARCOS SÊMOLA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

UMA VISÃO EXECUTIVA

17ª Tiragem



©2003, Elsevier Editora Ltda.

Todos os direitos reservados e protegidos pela Lei nº 9.610 de 19/02/1998.
Nenhuma parte deste livro, sem autorização prévia por escrito da editora,
poderá ser reproduzida ou transmitida sejam quais forem os meios empregados:
eletrônicos, mecânicos, fotográficos, gravação ou quaisquer outros.

Copidesque
Adriana Kramer
Editoração Eletrônica
Estúdio Castellani
Revisão Gráfica
Vânia Maria Martins

Projeto Gráfico
Elsevier Editora Ltda.
Conhecimento sem Fronteiras
Rua Sete de Setembro, 111/16º andar
20050-006 – Centro – Rio de Janeiro – RJ – Brasil

Rua Quintana, 753 – 8º andar
04569-011 – Brooklin – São Paulo – SP – Brasil

Serviço de Atendimento ao Cliente
0800-0265340
sac@elsevier.com.br

ISBN 13: 978-85-352-1191-7

Nota: Muito zelo e técnica foram empregados na edição desta obra. No entanto, podem ocorrer erros de digitação, impressão ou dúvida conceitual. Em qualquer das hipóteses, solicitamos a comunicação ao nosso Serviço de Atendimento ao Cliente, para que possamos esclarecer ou encaminhar a questão.

Nem a editora nem o autor assumem qualquer responsabilidade por eventuais danos ou perdas a pessoas ou bens, originados do uso desta publicação.

CIP-Brasil. Catalogação na fonte.
Sindicato Nacional dos Editores de Livros, RJ

S475s

Sêmola, Marcos
Gestão da segurança da informação: visão executiva da
segurança da informação: aplicada ao Security Officer /
Marcos Sêmola e Módulo Security Solutions S.A. – Rio de
Janeiro: Elsevier, 2003 – 17ª reimpressão.

Inclui bibliografia
ISBN 978-85-352-1191-7

1. Sistema de informação gerencial – Medidas de
segurança. 2. Sistemas de segurança. I. Título.

02-2034.

CDD – 658.4038
CDU – 65.012.4:007

Este livro é dedicado à memória dos meus avós paternos Archimedes Renato Forin Sêmola e Fernanda Sêmola, por seus valores incontestáveis, pela lição de vida que compartilharam, incentivando a busca contínua do conhecimento e da razão, e pelo amor aplicado ao papel educacional que se propuseram a cumprir por nós.

Agradecimentos

Comumente os livros se iniciam com o capítulo de agradecimentos. Seu propósito está intimamente ligado a permitir que o autor torne pública a importância participativa de pessoas e empresas na obra literária. Curioso é que a granularidade e capilaridade dos agradecimentos tendem a diminuir edição a edição, em função da quantidade de obras do autor. Assim, neste livro não será diferente.

Dessa forma, inicio agradecendo à empresa Módulo Security Solutions – onde atuo como Gerente Nacional de Produtos – por sua responsabilidade no meu envolvimento profissional com a área de segurança, pelas oportunidades que me tem sido proveitosas e principalmente, por ser um dos fatores críticos de sucesso para a construção deste livro ao emprestar-me grande parte de seus conceitos e visões aplicadas no dia-a-dia, que aqui se encontram didaticamente organizadas e complementadas por experiências docentes. Ainda no “perímetro Módulo”, agradeço aos colaboradores em geral, à unidade de treinamento MEC – Módulo Education Center, aos integrantes das equipes do Módulo Security Lab, Módulo Consulting Team, Account Managers e também à equipe do Portal, que direta e indiretamente, contribuíram com a divulgação, revisão e organização das informações compartilhadas neste livro. Um agradecimento aos três sócios visionários, que em 1985 souberam identificar a oportunidade e começaram a escrever a história da segurança da informação no Brasil, mas em especial a um deles, Fernando Nery, a quem responsabilizo pelo interesse e entusiasmo que desenvolvi pela Segurança da Informação e pela condição informal de co-autor de muitos dos conceitos e *insights* presentes aqui.

Agradeço à Fundação Getúlio Vargas que teve um importante papel na materialização deste projeto, por acreditar no potencial literário da obra e principalmente no valor que poderia agregar aos cursos de educação continuada MBA (Master in Business Administration). Agradeço aos amigos e mentores da FGV/EPGE, Moisés Glat, Raul Colcher, Bernardo Grinner, Carlos Salles e André Valle que, por acreditarem no meu potencial como educador, viabilizaram – a partir de um convite – a enriquecedora experiência de lecionar a cadeira de Gestão de Segurança da Informação para os cursos nacionais MBA da instituição. À amiga e professora Deana Weikersheimer, um agradecimento especial pelas horas nos saguões dos aeroportos em que trocávamos experiências, enquanto era especialmente motivado a seguir seu exemplo de compartilhar o conhecimento ora distribuído através deste livro.

Sendo rigoroso com a premissa de usufruir deste capítulo para agradecimentos extensivos – principalmente por se tratar da primeira obra – não posso deixar de responsabilizar por uma fatia deste resultado meus colegas do curso MBA em Tecnologia Aplicada/FGV, especialmente ao Marco Aurélio Latge e Luiz Mário Grinner, que foram sempre presentes e incentivadores de meus projetos ambiciosos.

Como não poderia deixar de ser, não me permito esquecer dos principais responsáveis pelo apoio incondicional e a base sólida que viabilizam diretamente o sucesso de mais este projeto, minha família, principalmente meus pais, meus irmãos, minha esposa Adrianny e, agora, aos 45 minutos do segundo tempo do livro, meu primeiro filho, Guilherme, que está sendo aguardado com ansiedade.

Prefácio

Recentemente passei pela desagradável experiência de ser assaltado ao final de um dia de trabalho. O assaltante chegou pedindo o meu “laptop”, em alusão à minha pasta, que eu achava ser discreta e que não se parecia com as pastas tradicionais de notebook. Argumentei que não possuía “laptop” na pasta, aliviado por ter deixado o meu em casa naquele dia, e abri a pasta, por “pedido” dele, mostrando a ausência do equipamento. Ele quis levar a pasta assim mesmo, no que eu instintivamente pedi para que ele me deixasse ficar com minha agenda. Ele desistiu, pediu minha carteira, e depois fugiu em sua moto.

Apesar do susto e do trauma, fiquei pensando nesse episódio com olhos profissionais. De todos os itens que eu possuía comigo naquele momento, talvez a minha agenda estivesse entre os mais baratos. Contudo, por conta de todas as minhas anotações e rabiscos, foi o único item pelo qual eu me arrisquei (louco!) em uma argumentação tensa para poder mantê-lo.

Obviamente, que a minha vida era a maior prioridade, seguido dos documentos pessoais que estavam em uma segunda carteira e não foram levados, mas o que esse episódio ilustrou foi uma situação cotidiana em que informações estavam em risco, mesmo sem haver nenhum aparato tecnológico envolvido.

Extrapolando esse caso, fico pensando: e se um notebook fosse levado? Será que o dono perderia informações? Será que as informações contidas nele estariam protegidas dos olhos de terceiros? Poderia um assalto desses ser contratado por um concorrente inescrupuloso?

Evidentemente, este é apenas um dos vários riscos aos quais, infelizmente, tanto eu quanto o leitor estamos sujeitos enquanto vivermos neste mundo imperfeito e injusto. Mas, olhemos um pouco além: *quantos de nós, como profissionais, executivos e empresários responsáveis que somos, podemos dizer que administramos os riscos a que nossas empresas e negócios estão sujeitos por dependerem de informações?*

Pensemos nos nossos negócios em relação à Informação:

- Quão dependentes somos? Conseguimos ficar uma semana sem nossos computadores e sistemas? Que computadores e que sistemas não podem parar?
- Quão sensíveis somos? Que informações não podem cair nas mãos de nossos concorrentes? Que informações não podem vir a público?
- Quão conhecidos e confiáveis somos? Nossa reputação será afetada se modificarem nossas informações, se terceiros se passarem por nós ou se nossos serviços forem interrompidos sem aviso?
- Onde mora o perigo? Em agentes externos ao nosso negócio, ou entre os nossos quadros funcionais? Na ação deliberada, ou na negligência ou imperícia aplicadas ao nosso dia-a-dia?

Muitas pessoas pensam que Segurança da Informação se resume à compra de equipamentos e softwares caros, como firewalls, sistemas de detecção de intrusos ou antivírus. Outras acham que incluir a adoção de Políticas de Segurança e o estabelecimento de responsabilidades funcionais ao aparato tecnológico é suficiente. Mas nenhuma dessas abordagens consegue prevenir perdas se forem adotadas de forma isolada e inconseqüente.

Segurança da Informação não é uma ciência exata. Se fôssemos classificá-la, ela estaria no campo da gestão de riscos. E para gerir riscos é preciso conjugar vários verbos: Conhecer, Planejar, Agir, Auditar, Educar, Monitorar, Aprender e Gerenciar são apenas alguns deles.

A principal contribuição de Marcos Sêmola com este livro é traduzir em uma linguagem didática diversos conceitos e abordagens comuns no campo da Segurança da Informação. Mais do que isso, o livro permite ter uma visão global dos vários aspectos envolvidos, introduzindo o assunto àqueles que começam, e proporcionando uma estrutura de orientação sintética e fácil para aqueles mais experientes.

O livro se destina a pessoas que, como você que leu este prefácio até aqui, se interessam pelo assunto e estão conscientes da sua importância, e também àquelas que ainda não despertaram para ele. Como auxílio à conscientização, seu texto é um presente valioso.

IVAN ALCOFORADO

Information Security Specialist

Engenheiro de Produção, formado pela UFRJ e pós-graduado pelo Centro de Referência em Inteligência Empresarial (CRIE) da COPPE, e consultor nas áreas de Gestão do Conhecimento e Segurança da Informação.

O Autor

MARCOS SÊMOLA é Gerente da Divisão de Consultoria de Segurança da Informação da multinacional Atos Origin para a América do Sul, Consultor Sênior em Gestão de Segurança da Informação, um dos dez profissionais brasileiros certificados internacionalmente com o título CISM – Certified Information Security Manager. Possui 13 anos de experiência em TI dos quais 6 à frente da gestão de projetos e desenvolvimento de serviços de segurança da informação. É Professor da Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Pós Graduado em Redes e Bacharel em Ciência da Computação. É ainda articulista, colunista do IDGNow, autor do livro Gestão da Segurança da Informação – uma visão executiva, da Editora Campus e eleito SECMASTER, Profissional de Segurança da Informação de 2003 pelo ISACA e Via Forum.

Para entrar em contato com o autor envie um e-mail para:

autor@semola.com.br

Sociedade do Conhecimento

1.1 Informação: ativo cada vez mais valorizado

Há muito, as empresas têm sido influenciadas por mudanças e novidades que, a todo o momento, surgem no mercado e provocam alterações de contexto. A todo momento surgem descobertas, experimentos, conceitos, métodos e modelos nascidos pela movimentação de questionadores estudiosos, pesquisadores e executivos que não se conformam com a passividade da vida e buscam a inovação e a quebra de paradigmas, revelando – quase que freqüentemente, como se estivéssemos em um ciclo – uma nova tendência promissora.

Se resgatarmos a história, veremos diversas fases. Desde as revoluções Elétrica e Industrial, a abertura de mercado e o aumento da competitividade proporcionado por empresas multinacionais, passando pelos momentos relacionados à reengenharia, à terceirização e, mais recentemente, os efeitos da Tecnologia da Informação aplicada ao negócio.

Em todas essas etapas, a informação sempre esteve presente e cumpria importante papel para a gestão do negócio. Claro que, para tal análise, devemos considerar as variáveis culturais, mercadológicas e até macroeconômicas da época, a fim de adequar a projeção dos impactos. Mas é inegável que todas as empresas, independentemente de seu segmento de mercado, de seu *core business* e porte, em todas essas fases de existência, sempre usufruíram da informação, objetivando melhor produtividade, redução de custos, ganho de *market share*, aumento de agilidade, competitividade e apoio à tomada de decisão.

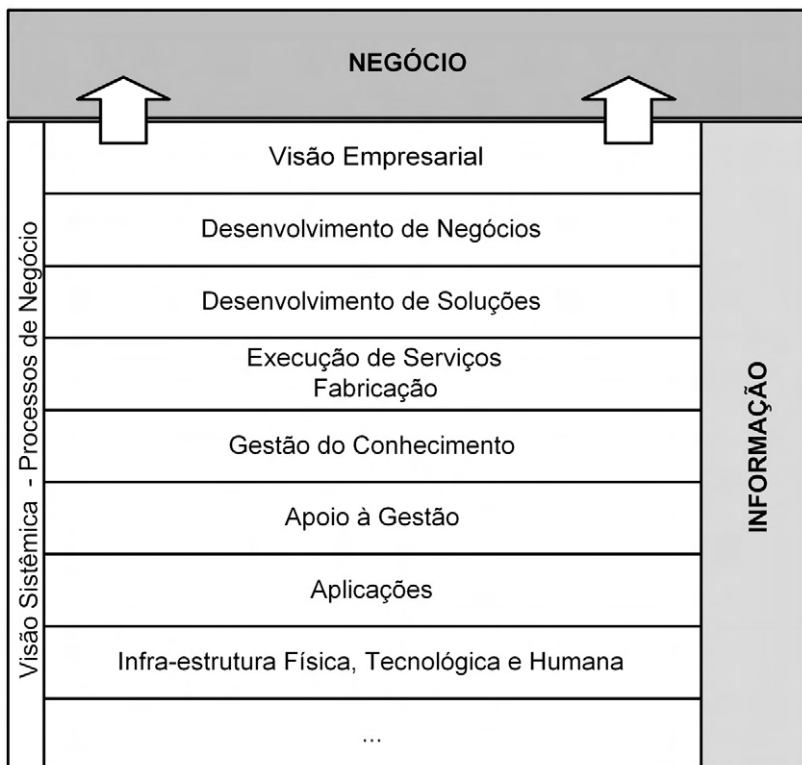


Figura 1-1 *Onipresença da Informação nos principais Processos de Negócio.*

Seja para um supermercadista preocupado com a gestão de seu estoque, seja para uma instituição bancária em busca da automação de suas agências bancárias, ou para uma indústria alimentícia prospectando a otimização da sua linha de produção, todos decidem suas ações e seus planos com base em informações. Segredos de negócio, análise de mercado e da concorrência, dados operacionais históricos e pesquisas, são informações fundamentais e se revelam como um importante diferencial competitivo ligado ao crescimento e à continuidade do negócio.

1.2 Crescimento da Dependência

Se compararmos momentaneamente as fases da evolução corporativa, especificamente a forma com que as empresas usavam a informação e geriam seus negócios, perceberemos nítidas mudanças nas ferramentas com o passar dos anos.

Décadas atrás, as informações eram tratadas de forma centralizada e ainda pouco automatizadas. A tecnologia da informação engatinhava e figurava, primeiramente, apenas como uma nova e promissora ferramenta, principalmente se considerarmos as limitações de armazenamento iniciais e os preços proibitivos dos primeiros grande computadores *mainframes*.

Mas logo os investimentos da indústria de alta tecnologia foram sendo amortizados e seus frutos foram se tornando mais acessíveis. Apesar das empresas terem muita informação em documentos manuscritos, nos conhecidos arquivos de ferro, os *mainframes* foram herdando, gradativamente, a função de central de processamento e armazenamento de dados. Logo veríamos terminais espalhados pelos ambientes da empresa – inicialmente um único por departamento – que permitiam consultas remotas.

Compartilhar informação passou a ser considerada uma prática moderna de gestão e necessária a empresas que buscam maior velocidade nas ações. Diante disso, surgiram em seguida as primeiras redes de computadores e, paralelamente, as informações passaram a ser mais digitalizadas e os processos mais automatizados.

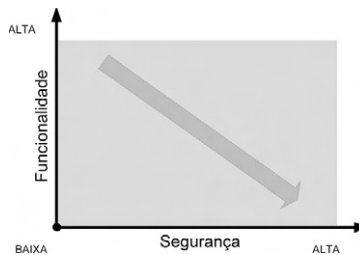


Figura 1-2 Associação direta entre o aumento da funcionalidade operacional e a segurança necessária.

Mais alguns anos e as empresas experimentam e aplicam, como nunca, a tecnologia da informação ao negócio, atingindo altos níveis de conectividade e compartilhamento. Os antigos, mas sobreviventes *mainframes*, não cumprem mais sozinhos a tarefa de armazenar e processar as informações. Os computadores tomam conta dos ambientes de escritório, quebram o paradigma de acesso local à informação, e chegam a qualquer lugar do mundo através dos – cada vez mais portáteis – *notebooks* e da rede mundial de computadores: a Internet.

Simultaneamente, a rede corporativa ganha performance e igualmente se pulveriza. Passa a representar o principal canal de distribuição de informações internas e externas, e de interligação de ambientes e processos, culminando com a integração dos parceiros da cadeia produtiva.

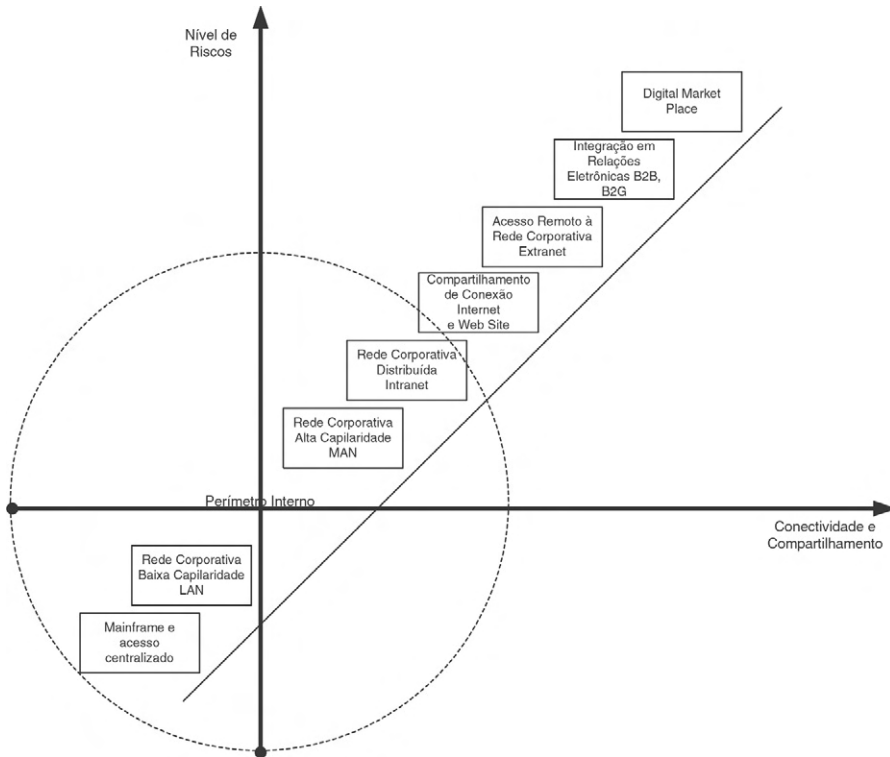


Figura 1-3 Evolução da conectividade e do compartilhamento.

Logo surgem expressões e aplicações comerciais que se utilizam da moderna infra-estrutura de rede e computacional como *business-to-business*, *business-to-consumer*, *business-to-government*, *e-commerce*, *e-procurement*, e os sistemas integrados de gestão ERP – *Enterprise Resource Planning* que prometem melhor organização dos processos de negócio, e passam a representar um dos principais pilares de sustentação da empresa para alcançar o tão sonhado e promissor *digital marketplace*, onde elementos da cadeia produtiva, como fornecedores, parceiros, clientes e o governo passam a interagir também eletronicamente, integrando e compartilhando suas bases de conhecimento.

Esse panorama nos leva a perceber o alto grau de dependência que as empresas têm da informação – muito mais digitalizada, compartilhada e distribuída – além, conseqüentemente, de todos os elementos da infra-estrutura que a mantém.

1.3 Visão holística do Risco

Realizando uma análise análoga ao corpo humano, é possível extrair um valioso aprendizado a fim de ratificar o cenário atual vivido pelas empresas diante do aumento exponencial da dependência da informação.

Pense no ser humano como uma máquina complexa, ímpar, imprevisível e sujeita a mudanças físicas e emocionais a qualquer momento, muitas motivadas por fatores externos. Agora reflita sobre as similaridades com a sua empresa. Sujeita a influências de variáveis mercadológicas, macroeconômicas, políticas, setoriais, físicas e tecnológicas.

Pense nas características estratégicas, desafios, missão, visão, produtos e serviços. Por mais que outras empresas se pareçam com a sua, assim como no corpo humano, todas têm suas diferenças que as tornam únicas, cada um com suas características personalizadas e certamente com sensibilidades distintas.

O que aconteceria com dois indivíduos – aparentemente semelhantes, se considerarmos a similaridades anatômica dos membros, órgãos etc – consumindo açúcar em exagero, sendo um deles diabético? Teriam sensibilidades iguais, provocando os mesmos efeitos?

Agora pense na sua empresa novamente. Aparentemente similar a um concorrente por atuarem no mesmo segmento, com os mesmos produtos e até possuindo processos de negócio semelhantes. Imagine, então, ambas sendo contaminadas por um vírus de computador ou tendo sua conexão à Internet fora do ar momentaneamente. Teriam sofrido os mesmo efeitos? Teriam tido impactos financeiros idênticos?

Estou certo de que não, pois cada instituição possui diferenças físicas, tecnológicas, humanas – além dos fatores externos que influenciam direta e indiretamente – que interferem nas variações de sensibilidade e, conseqüentemente, nos impactos resultantes.

Por fim, pense nos nossos membros. Cada qual com sua função e importância para a manutenção e o funcionamento do nosso corpo.

Com similar papel, aparecem os processos de negócio para a empresa, cada um com objetivos distintos que, integrados, permitem seu crescimento e operação. Contudo, para que tenhamos vida e sejamos capazes de manter o organismo vivo, precisamos de um elemento vital: o sangue. Ele transporta e compartilha oxigênio a cada célula espalhada pela massa corporal. Leva alimento a todos os membros e circula incessantemente da cabeça aos pés.

Agora a empresa, que, em virtude dos altos níveis de informatização e compartilhamento de informações, nos permitiu realizar este comparativo...

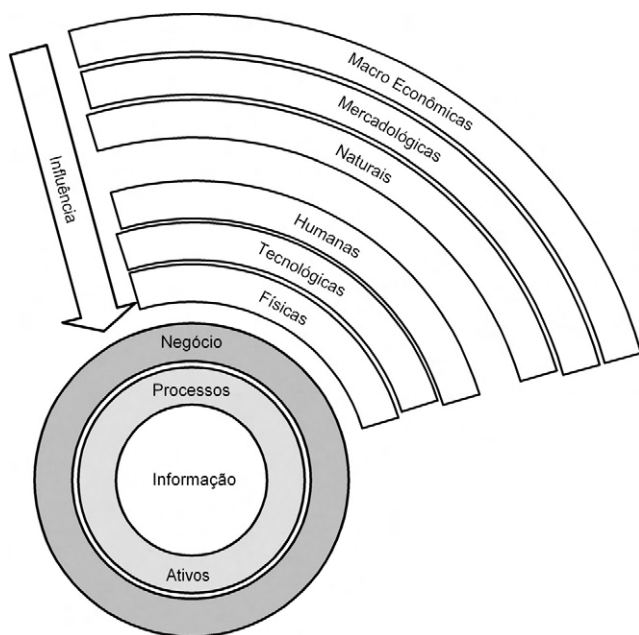


Figura 1-4 *Influência das variáveis internas e externas que personalizam o problema da segurança da informação.*

O sangue da empresa é a informação. Distribuída por todos os processos de negócio, alimentando-os e circulando por diversos ativos (tudo que manipula direta ou indiretamente a informação, inclusive ela própria), ambientes e tecnologias, a informação cumpre o importante papel de fornecer instrumentos para gestão do negócio. Apesar de ter grande volume momentaneamente armazenado e processado de forma centralizada nos grandes computadores e servidores – similar ao coração no corpo humano – toda a informação está acessível dos

pontos mais distantes através da tecnologia de rede *Internet*, *Intranet*, *Extranet*, acessos remotos, culminando com as novas tecnologias de fio WAP e *Wireless*.

Fica fácil perceber como o nível de risco tem crescido com base nesta análise, como sugere o exemplo a seguir:

Na condição de correntista de uma instituição bancária, há pouco era necessário ir a uma agência bancária a fim de movimentar sua conta, pois as informações estavam parcialmente compartilhadas e só eram acessíveis através dos caixas ou terminais de auto-atendimento *ATM*. Esta situação agregava, simultaneamente, maior controle e segurança à informação por estar mais centralizada.

Atualmente, usando o mesmo cenário, não somos mais obrigados a um deslocamento físico para movimentar nossa conta. Muitos dos serviços prestados *on site*, estão agora disponíveis através do telefone, bastando digitar algumas informações – inclusive a senha – ou através dos serviços eletrônicos *Internet Banking* a partir de qualquer ponto de acesso à *Web* no mundo, ou ainda, através do aparelho móvel celular.

Notadamente, essas novas e modernas condições elevam o risco das empresas a níveis nunca antes vividos, fazendo-as perceber a necessidade de ações corporativas integradas em busca de mecanismos de controle que permitam reduzi-lo e torná-lo administrável e viável.

No ambiente corporativo, muitos outros processos de tratamento do risco estão amadurecidos, como: risco jurídico, risco de crédito, risco financeiro, risco de pessoal etc. Mas ainda há muito a desenvolver no campo do risco da informação.

1.4 Receita explosiva

Ao tentar compreender e construir uma visão única do cenário, podemos lançar mão de um didático exercício que encara a situação de segurança vivida pelas empresas como se tudo fosse uma receita gastronômica. Como se misturássemos diversos ingredientes e o resultado pudesse representar, mesmo que simbolicamente, uma fotografia ou um diagnóstico.

Comece reunindo:

- Crescimento sistemático da digitalização de informações.
- Crescimento exponencial da conectividade da empresa.
- Crescimento das relações eletrônicas entre empresas.

- Crescimento exponencial do compartilhamento de informações.
- Barateamento do computador, facilitando sua aquisição.
- Gratuidade do acesso à Internet.
- Baixo nível de identificação do usuário no acesso gratuito à Internet.
- Acesso a conexões Internet em banda larga.
- Alto compartilhamento de técnicas de ataque e invasão.
- Disponibilidade de grande diversidade de ferramentas de ataque e invasão.
- Facilidade de uso de ferramentas de ataque e invasão.
- Carência de mecanismos legais de responsabilização em ambiente virtual.
- Carência de conscientização da similaridade entre o crime real e o virtual.
- Carência de jurisprudência que tenha regulado sobre atos ilícitos em meio eletrônico.
- Comunicação de massa exaltando o jovem invasor pelo mérito da invasão.
- Criação do estereótipo do gênio e herói que obteve êxito em invasão.
- Associação equivocada entre Inteligência Competitiva e Espionagem Eletrônica.
- Diversificação dos perfis da ameaça: concorrente, sabotador, especulador, adolescente, *hacker*, funcionário insatisfeito etc.
- Crescente valorização da informação como principal ativo de gestão das empresas.

Misturados os ingredientes, salvaguardando as devidas proporções inerentes à culinária peculiar proposta, teremos como produto final um bolo amargo, difícil de digerir e que nos reserva um cenário de grande risco, se não houver preparação adequada para geri-lo a fim de tornar viável a operação do negócio.

1.5 Ciclo de Vida da Informação

Agora sabemos o quão valiosa é a informação para o negócio, mas temos de dissecar todos os aspectos ligados à segurança, as propriedades que devem ser preservadas e protegidas para que a informação esteja efetivamente sob controle, e, principalmente, os momentos que fazem parte de seu ciclo de vida.

Toda informação é influenciada por três propriedades principais: Confidencialidade, Integridade e Disponibilidade, além dos aspectos Autenticidade, Legalidade que complementam esta influência.*

O Ciclo de Vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Os momentos são vivenciados justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa.

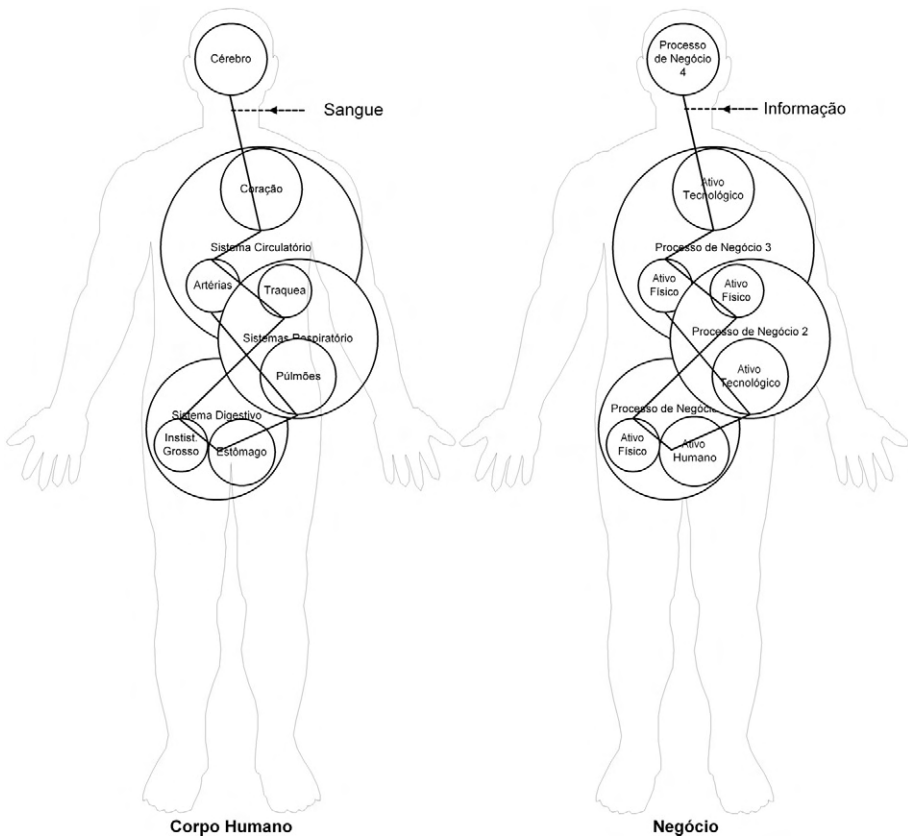


Figura 1-5 Analogia com o funcionamento do corpo humano.

Mais uma vez, é como o funcionamento do nosso corpo, onde os órgãos (analogamente, ativos físicos, tecnológicos e humanos), se utilizam de sangue (analogamente, informação), para pôr em funcionamento os sistemas digestivo, respiratório etc. (analogamente, processos de negócio), para, conseqüentemente, manter a consciência e a vida do indivíduo (analogamente, a continuidade do negócio).

Correspondendo às situações em que a informação é exposta a ameaças que colocam em risco suas propriedades, atingindo a sua segurança, o diagrama revela todos os 4 momentos do ciclo de vida que são merecedores de atenção.

Independentemente da forma como a informação é representada – seja por átomos ou por bits –, todos os momentos se aplicam.

Manuseio

Momento em que a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou, ainda, ao utilizar sua senha de acesso para autenticação, por exemplo.

Armazenamento

Momento em que a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda, em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo.

Transporte

Momento em que a informação é transportada, seja ao encaminhar informações por correio eletrônico (e-mail), ao postar um documento via aparelho de fax, ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.

Descarte

Momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador de mesa, ou ainda, ao descartar um CD-ROM usado que apresentou falha na leitura.

Agora pense na segurança como um todo, cujo alvo é a informação. Do que adiantaria garantir 3 dos 4 conceitos?

Imagine...você gera, em reunião, uma nova definição: informação estratégica confidencial. A mesma é anotada em papel e armazenada posteriormente em um cofre adequado. No momento imediatamente posterior, você delega à secretária que digite tal informação e a envie por correio eletrônico aos envolvidos. Pense agora que, depois de completada a tarefa, a secretária não tenha adotado os procedimentos adequados de descarte, e conseqüentemente, tenha jogado, sem qualquer critério e tratamento, o material original em papel na lixeira mais próxima. Neste exato momento, instaurou-se uma vulnerabilidade ou um furo de segurança! Agora imagine que haja efetivamente uma ameaça potencial pronta para explorar esta vulnerabilidade. Por exemplo: um outro funcionário no perímetro físico da secretária, interessado, mas que não participara da reunião e tenha objetivos obscuros.

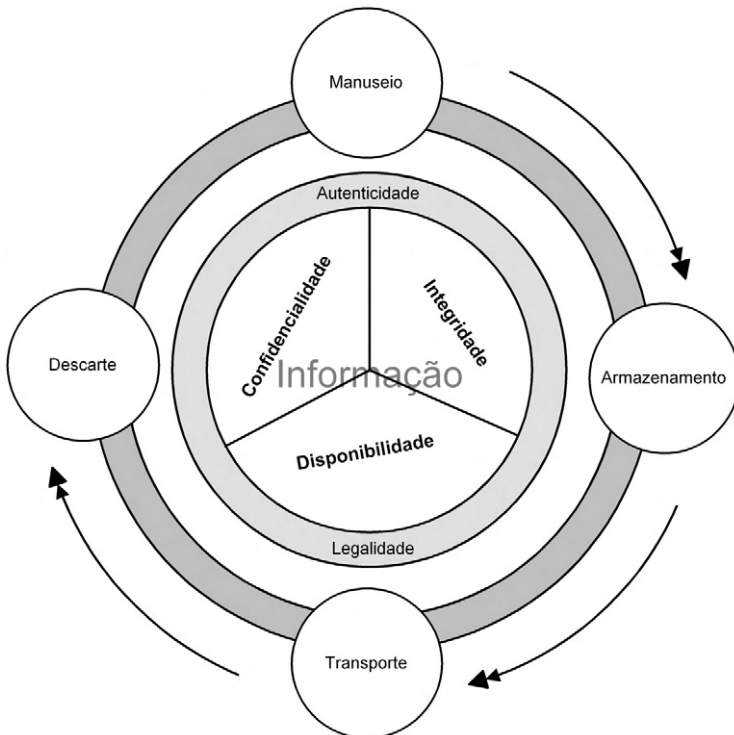


Figura 1-6 Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos da segurança e os aspectos complementares.

Pronto! Por mais que tenham adotado um comportamento controlado e alinhado à política de segurança nos momentos de Manuseio, Armazenamento e Transporte, a informação – alvo e motivo de todo o trabalho – estivera exposta no momento do descarte, comprometendo todos os demais, e ainda pondo toda a segurança do negócio a perder. (Consulte a Figura 1-6.)

* Conceitos e aspectos oportunamente discutidos em capítulo posterior.

Desafios

2.1 Anatomia do Problema

Em qualquer iniciativa de solução é preciso identificar primeiramente o problema com requinte de detalhes e segmentá-lo de forma a permitir maior profundidade na análise de suas características. Quando o assunto é Segurança da Informação, este desafio cresce exponencialmente, pois são muitos os fatores associados ao tema.

Temos de compreender que o alvo é a informação, e que a mesma não se encontra mais confinada a ambientes físicos específicos, ou a processos isolados. A informação circula agora por toda a empresa, alimenta todos os processos de negócio, e está sujeita a variadas ameaças, furos de segurança ou vulnerabilidades, e é sensível a impactos específicos.

A empresa virou uma grande teia de comunicação integrada, dependente do fluxo de informações que por ela são distribuídas e compartilhadas. Essas mesmas informações, agora sujeitas a vulnerabilidades que transcendem os aspectos tecnológicos, são alvos também de interferências provocadas por aspectos físicos e humanos.

Ainda hoje, muitas empresas e seus executivos são surpreendidos por essa afirmação, pois ainda mantêm uma deficiência de percepção do problema que costumo chamar de “Visão do Iceberg”. Simpatizo por adotar este rótulo, pois muito se parece com o problema. A porção de gelo que vemos fora da linha d’água é comumente correspondente a apenas 1/5 de todo o bloco do gelo que permanece submerso e, portanto, escondido dos nossos olhos. Esta é justamente a semelhança.

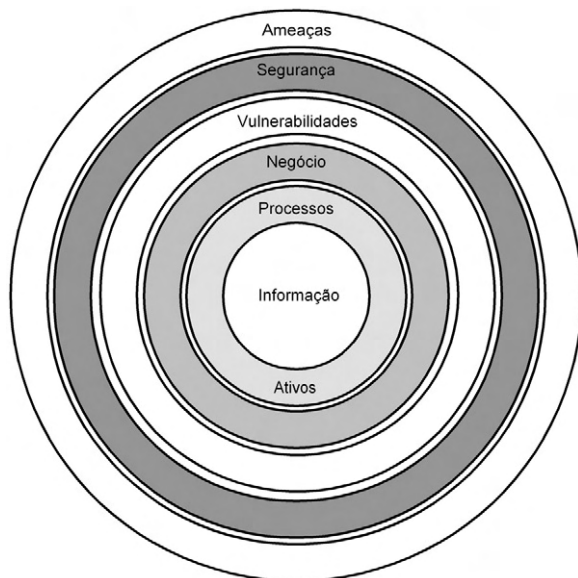


Figura 2-1 *Perímetros. O alvo é a informação.*

Comumente, a fatia representativa do mercado e seus executivos possuem esta “miopia”, percebendo apenas uma pequena fração do problema da segurança: os aspectos tecnológicos. Normalmente associam os riscos apenas a redes, computadores, vírus, *hackers* e Internet, enquanto ainda há muitos outros, tão importantes e relevantes para a segurança do negócio.

É fator crítico de sucesso para a anatomia do problema, que se identifique os elementos internos e externos que interferem nos riscos à segurança da informação. É o momento de mapear as características físicas, tecnológicas e humanas da empresa, do mercado em que atua, dos concorrentes, além de considerar os planos e definições estratégicas do negócio.

Mais uma vez adotando a analogia com o corpo humano, podemos comparar o papel do médico ao consultar o paciente antes de receitar um tratamento, ao desafio de definir e modelar uma solução de segurança da informação para a empresa.

O profissional precisa realizar uma série de exames que revelem a situação atual do paciente, por mais que este possua sintomas similares a outros pacientes, pois a origem poderá divergir. Tudo isso tem por objetivo equacionar o problema e recomendar um tratamento e medicamento adequados capazes de sanar especificamente a enfermi-

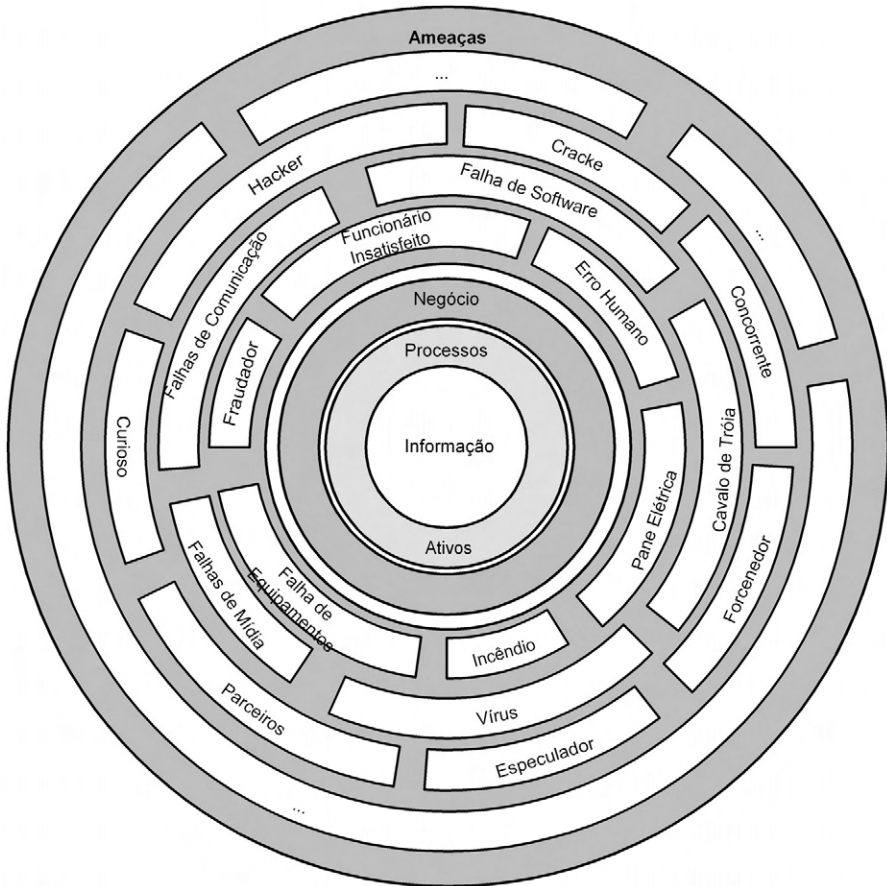


Figura 2-2 *Diversidade panorâmica das ameaças que põem o negócio em risco.*

dade. Ainda nesta dimensão, temos de considerar a possibilidade de um tratamento ou medicamento equivocados. Uma dose alta poderia gerar efeitos colaterais, e uma dose aquém da necessidade poderia não curá-lo.

Na empresa a situação é similar. O desafio é realizar ações que mapeiem e identifiquem a situação atual da empresa, suas ameaças, vulnerabilidades, riscos, sensibilidades e impactos, a fim de permitir o adequado dimensionamento e modelagem da solução. O que ocorre com o medicamento, ocorre com a empresa. Cada empresa possui características particulares que levarão à aplicação de uma solução personalizada capaz de levá-la a um nível de segurança também personalizado.

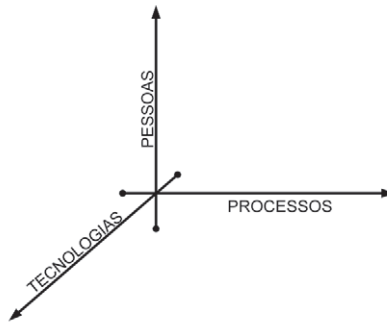


Figura 2-3 *Macroaspectos considerados na análise do contexto de segurança.*

Diferente do que muito pensam, não existe segurança total e, com base no exemplo, cada empresa precisará de um nível distinto. Se o nível for alto demais, poderá gerar efeitos colaterais, como a perda de velocidade em função da burocratização de processos, a perda do **time-to-market*, a insatisfação de clientes e parceiros, e até o desinteresse de possíveis investidores.

Cai o mito de que é possível operar com risco zero. Sempre haverá risco, e ele deve ser ajustado à natureza do negócio, considerando todas as variáveis internas e externas apontadas anteriormente a fim de viabilizar a operação da empresa.

2.2 Visão Corporativa

Por que eu preciso de segurança? Você já se fez essa pergunta alguma vez? Já parou ao menos uma dezena de minutos para avaliar e verificar por que precisa de segurança?

Vamos aproveitar um pequeno e comum exemplo do nosso dia-a-dia para entendermos melhor do que estamos falando, e, ainda, como acabamos replicando erros de caráter pessoal nas atividades profissionais, levando-os para a empresa.

Pense na sua residência. Uma casa ou apartamento que, na maioria dos casos, possui duas únicas portas de entrada, costumeiramente chamadas de porta social e porta de serviço. Elas cumprem um papel importante. Você já parou para pensar nisso? Sabe qual é?

Assumindo que seu comportamento diante dessa pergunta siga o da grande maioria, você realmente nunca parou sequer alguns minu-

tos para avaliar a importância e o papel que as portas cumprem. Pois elas são dispositivos instalados para prover acesso físico ao seu apartamento. São mecanismos de controle que podem ser abertos e fechados de acordo com a vontade do proprietário, permitindo ou impedindo que obtenham acesso ao interior da sua residência.

De forma generalizada, as portas oferecem resistência aos que insistem em acessar fisicamente o seu ambiente e, conseqüentemente, protegem todos os demais bens que estão lá dentro. Não pense apenas em tentativas de roubo; afinal, quem nunca se viu na situação de ter esquecido a chave da própria casa, certo?

A grande essência desta comparação está na inconsistência desses controles, comumente encontrados na maioria das residências. Acompanhe o raciocínio...

Você dispõe de documentos, equipamentos de informática, móveis, eletrodomésticos, roupas, jóias e até dinheiro em espécie – relembrando os áureos tempos da estabilidade, por exemplo. Além dos bens materiais, ainda mantém em seu interior as pessoas que ama: sua família.

O curioso é que, apesar de serem os mecanismos que protegem e oferecem resistência e, conseqüentemente, segurança para os seus principais ativos, as portas das residências não dispõem dos mesmos mecanismos de acesso físico, das mesmas trancas e alarmes, ou até não são feitas do mesmo material. Isso revela que as portas social e de serviço acabam por oferecer níveis de segurança diferentes e que, portanto, os investimentos não foram adequadamente distribuídos, resultando em um retorno menor do que o normalmente esperado.

De que adianta possuir duas trancas na porta social, se a outra, que permite acesso ao mesmo ambiente, só possui uma?

O que se vê aqui são dois pontos com objetivos comuns; porém, cumprindo-os de forma diferente e desbalanceada. É como sair de férias, calibrar 3 pneus e esquecer o quarto vazio ou furado.

Se cometemos erros simples e impactantes como estes em casa, não estaríamos replicando-os ao praticar a segurança da informação dentro de nossas empresas?

Não estaria sua equipe de segurança voltada apenas para os aspectos tecnológicos da segurança e, conseqüentemente, esquecendo dos aspectos físicos e humanos?

Será que os investimentos realizados em segurança estão alinhados com os objetivos estratégicos da empresa, a fim de propiciar o melhor retorno sobre o investimento?

Suas ações estão orientadas por um Plano Diretor de Segurança, ou continuam ocorrendo de acordo com demandas reativas em caráter emergencial?

Estaria sua empresa operando em terreno de alto risco, encorajada por mecanismos de controle que lhe dão uma falsa sensação de segurança, apesar de continuar com as “portas trancadas”, mas as “janelas ainda abertas”?

O nível de segurança de uma empresa está diretamente associado à segurança oferecida pela 'porta' mais fraca. Por isso, é preciso ter uma visão corporativa capaz de viabilizar uma ação consistente e abrangente, levando a empresa a atingir o nível de segurança adequado à natureza do seu negócio.

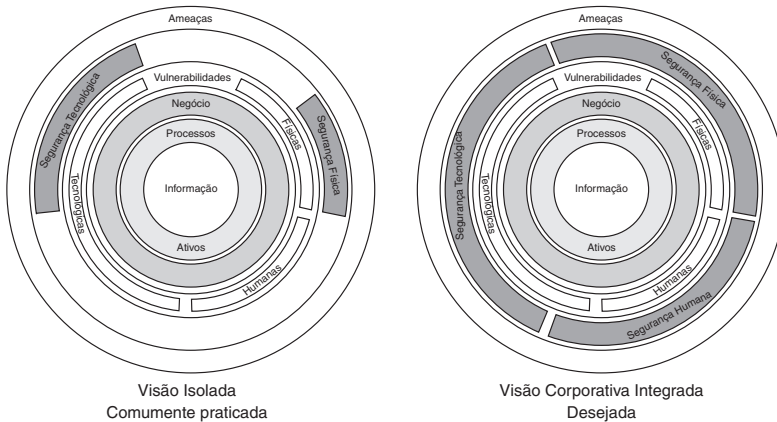


Figura 2-4 Cenário Atual x Cenário Desejado: abrangência da solução de segurança considerando todos os 3 aspectos.

Vulnerabilidades x Ameaças

A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada.

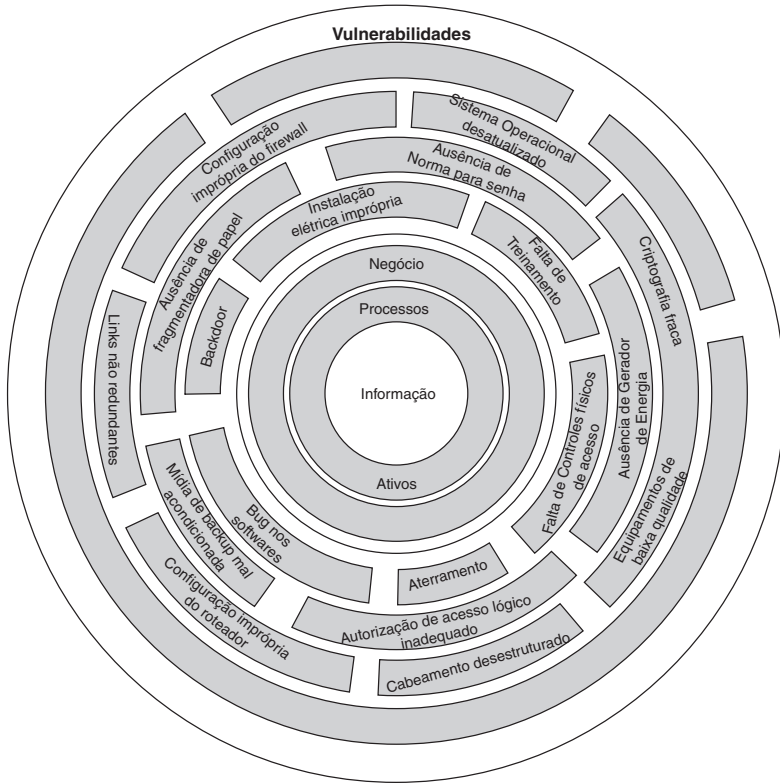


Figura 2-5 Diversidade panorâmica das vulnerabilidades que expõem o negócio a ameaças associadas.

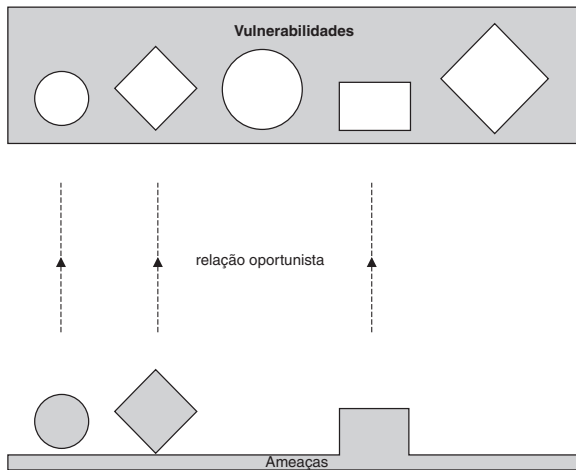


Figura 2-6 Como peças que se encaixam, ameaças específicas exploram vulnerabilidades compatíveis.

2.3 Pecados praticados

Muitos são os erros comumente praticados na hora de pensar em segurança da informação, provocados pela visão míope do problema e a percepção distorcida da questão. Fica fácil entender este equívoco quando o comparamos a um *iceberg*; isso mesmo, aquele grande bloco de gelo que flutua solto no oceano. Pois saiba que o que é visto fora d'água corresponde apenas a uma pequena fatia de todo o bloco, cerca de 15%, portanto, existe muito mais gelo submerso que não pode ser visto. É justamente assim que muitos percebem os aspectos da segurança, considerando e enxergando apenas os problemas associados à tecnologia, mais precisamente Internet, redes, computador, email, vírus e hacker. Em função desse entendimento parcial, muitos pecados são praticados e vêm refletir negativamente no negócio.

- Atribuir exclusivamente à área tecnológica a segurança da informação.
- Posicionar hierarquicamente essa equipe abaixo da diretoria de TI.
- Definir investimentos subestimados e limitados à abrangência dessa diretoria.
- Elaborar planos de ação orientados à reatividade.
- Não perceber a interferência direta da segurança com o negócio.
- Tratar as atividades como despesa e não como investimento.
- Adotar ferramentas pontuais como medida paliativa.
- Satisfazer-se com a sensação de segurança provocada por ações isoladas.
- Não cultivar corporativamente a mentalidade de segurança.
- Tratar a segurança como um projeto e não como um processo.

2.4 Conscientização do Corpo Executivo

Por se tratar de um problema generalizado e corporativo, envolvendo os aspectos físicos, tecnológicos e humanos que sustentam a operação do negócio, torna-se condição *sine qua non*, que se inicie os trabalhos no formato *top down*, ou seja, mobilizando os executivos da diretoria da empresa, para depois atingir os demais na hierarquia. Esta condição

é fundamental, pois não haverá possibilidade de atingir simultaneamente, e com igualdade, as vulnerabilidades de todos os ambientes e processos distribuídos da empresa, se não houver uma ação coordenada e principalmente apoiada pela cúpula.

Entende-se por apoio não só a sensibilização e percepção adequada dos riscos e problemas associados, mas também da conseqüente priorização das ações e definição orçamentária à altura.

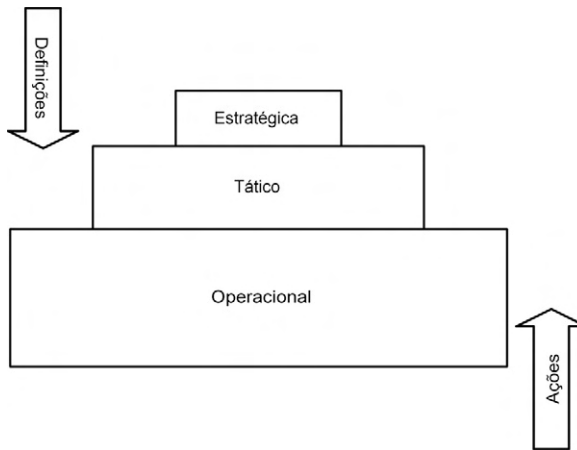


Figura 2-7 Ação coordenada por definições estratégicas resultando em ações operacionais.

Não é tarefa fácil encontrar uma linguagem adequada e elementos capazes de traduzir de forma executiva as necessidades de investimento, e, principalmente, os benefícios diretamente ligados à segurança. Afinal, há um alto grau de subjetividade nas ações, além de se tratar de um investimento que comumente não se materializa facilmente e só mostra retorno quando há algum evento que põe à prova os mecanismos de controle.

Apesar disso, algumas experiências bem-sucedidas, anteriormente vividas pelos executivos, corroboram hoje com o desafio da segurança em função de sua similaridade e convergência.

Em tempo do desafio de reduzir os riscos proporcionados pelo *Bug do Ano 2000*, todo o alto escalão foi envolvido e conscientizado dos riscos e da necessidade de investir a fim de superar a ameaça. Realizaram análises e extraíram características importantes que também se aplicam à segurança da informação. O mesmo ocorreu quando busca-

ram organizar seu sistema corporativo de gestão de forma integrada, através de *softwares* ERP – *Enterprise Resource Planning*. Se repetindo no momento de se adequarem aos padrões de qualidade proporcionados pela certificação ISO 9000.

Bug do Ano 2000

- Problema generalizado
- Ação corporativa
- Conformidade

ERP

- Visão estratégica
- Mudança de processos
- Controle centralizado

ISO 9000

- Conscientização da alta administração
- Criação de normas e procedimentos
- Implementação, certificação e administração

Em tempo de resolver o problema dos sistemas para a virada do ano 2000, concluíram que se tratava de um problema generalizado, necessitava de uma ação corporativa e que precisavam ser complacentes com o *bug*. No momento de otimizar seu modelo de gestão com as soluções ERP, concluíram com a análise que, para obter sucesso, necessitavam ter uma visão estratégica, mudar e adaptar os processos e, ainda, manter o controle centralizado. Já na iniciativa de certificação de qualidade ISO, perceberam a dependência da conscientização da alta administração, a criação de normas e procedimentos, a certificação, a implantação e a administração constante.

Esses nove pontos, identificados como fatores críticos de sucesso em ações distintas, são igualmente importantes para superar o desafio da segurança e configuram modelos mentais já vividos e absorvidos pelos mesmos executivos que hoje estão diante deste novo desafio.

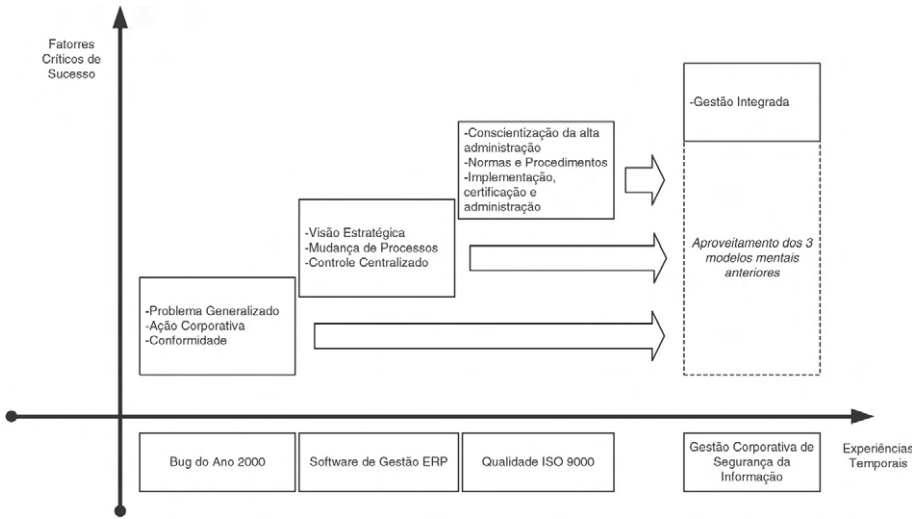


Figura 2-8 Absorção dos modelos mentais.

Somados a isso, para que se consiga atingir o nível de conscientização adequado do corpo executivo, não se pode abrir mão do exercício do ROI ou Retorno Sobre o Investimento. É a linguagem mais intimamente ligada ao perfil executivo de avaliação de custo, rentabilidade, receita, lucro, dividendos, ganho de *mind share* e valorização das ações.

2.5 Retorno sobre o Investimento

ROI ou Retorno sobre o Investimento é uma ferramenta antiga e velha conhecida dos empreendedores, investidores e executivos atentos ao mercado e às oportunidades. Construída através do cruzamento de dados reais relacionados a custos diretos, indiretos e intangíveis, com a projeção de investimentos obtêm-se um ótimo instrumento para nor-tear as ações desses executivos.

Parece, em um primeiro momento, instrumento essencial para apoiar uma tomada de decisão, e realmente o é. Analisando-o, consegue-se muitas vezes, justificar altos investimentos, mudanças de rumo e estratégia; afinal, torna-se possível projetar o retorno do investimento.

Não existe um único modelo de ROI, nem tampouco um modelo certo ou errado. O que existe são abordagens e visões diferentes do mesmo objeto. A profundidade da análise interfere diretamente neste

modelo, agregando um número ainda maior de variáveis e refinamentos. Contudo, todas buscam uma resposta mágica para a pergunta: devo realizar este investimento?

Pode soar estranho para muitos, mas a mesma pergunta se aplica também a investimentos na área tecnológica, você sabia? Foi-se a época em que investimentos desse gênero eram vistos como um “mal necessário”. É época em que se realizavam grandes aquisições – de última tecnologia – e não se preocupavam em medir resultados, projetar o tempo de colher os louros do investimento. É época em que tais despesas (pois assim é que eram vistos os investimentos), seriam repassadas através do produto ou serviço ao consumidor final, ou diluídas em aventuras na ciranda financeira.

Chegou a hora de planejar, projetar, medir e cobrar os resultados da integração entre tecnologia e negócio. Mas também é hora de exercitar mais o ROI em subcategorias, com maior detalhamento. Não basta modelar um macro ROI tecnológico; é preciso abordar tecnologias e problemas mais específicos como a segurança da informação.

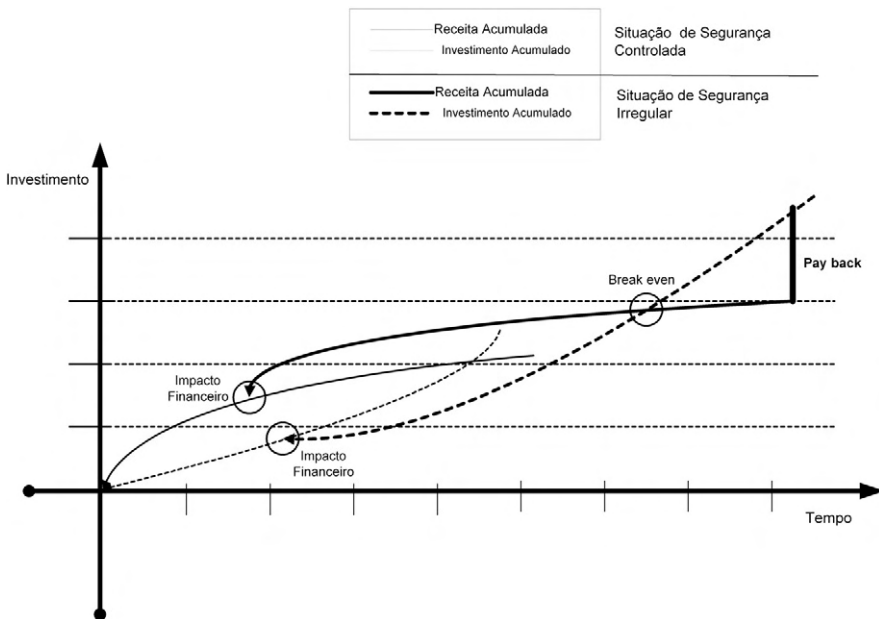


Figura 2-9 Análise dos reflexos de retardamento do *Pay back no ROI, oriundo da ausência de um processo de segurança.

O gargalo desse trabalho é notoriamente entender, conhecer e mapear os problemas corporativos, pois, sem essas informações, não seria possível desenvolver uma ferramenta de ROI coerente, confiável e pronta para apoiar a priorização das ações e as tomadas de decisão.

O ROI da segurança tem especialmente muitas respostas elucidativas que nos ajudam a reverter a velha imagem de despesa, convertendo-a em investimento e, diga-se de passagem, um ótimo investimento!



Figura 2-10 *Percepções do ROI da Segurança.*

Vamos exercitar tratando primeiro os custos diretos. Se cruzarmos o número de contaminações por vírus de computador em um ano, o percentual de funcionários atingidos, o tempo perdido com a paralisação e o custo homem/hora, perceberemos com nitidez o impacto direto no negócio.

Ao analisarmos o tempo de trabalho consumido pelos funcionários com acesso livre à Internet, acessando informação que não estão associadas à atividade profissional, e novamente com o custo homem/hora, podemos projetar o impacto na produtividade dos recursos humanos.

Se ainda por ocasião de um desastre, houver a indisponibilidade de um serviço – por exemplo, de Internet Banking – multiplique o número de correntistas que o acessam por hora, a economia que a empresa tem, por seus correntistas evitarem as agências e migrarem para a Internet e, assim, terá o impacto direto.

Falando agora de impactos indiretos, usando as mesmas situações, podemos realçar os custos relacionados à mobilização de equipes para remover os vírus que infectaram os computadores da rede, o tempo necessário para reconstruir arquivos e informações que se perderam com a contaminação, e ainda possíveis restaurações de cópias de segurança (se existirem). Seguindo os exemplos anteriores, o acesso indiscriminado e sem controle à Internet, pode provocar uma sobrecarga da banda de rede, antecipando investimentos e causando indisponibilidade. Além disso, pode permitir a contaminação por vírus de toda a rede com a execução de programas copiados da Internet e, pior: expor a empresa a sanções legais relacionadas à pirataria de software, pedofilia e crimes virtuais.

E os problemas não param por aí: a indisponibilidade dos serviços pode atingir profundamente você e o seu cliente. Primeiro você, pelo fato de o cliente não ter conseguido realizar uma transação financeira, um investimento ou uma solicitação de cartão de crédito etc. Agora o cliente, que deverá ser reparado através de uma ligação do telemarketing, de campanhas de marketing direto etc.

Agora vem o pior. Custos intangíveis e incalculáveis que põem verdadeiramente em risco a continuidade do negócio. O impacto de uma invasão, seja interna ou externa, causando o roubo de informações, não é fácil de ser calculado. Muitas vezes não se sabe que fim levou aquela informação e, muito menos, como ela será explorada. Será que estará na mão de um concorrente? Ou ainda na mão da imprensa, pronta para um furo de reportagem?

Trata-se de um problema sem dimensão definida. O impacto à imagem é coisa séria e custosa para ser revertida. Gasta-se muito mais recurso tentando reconstruir uma imagem sólida, segura, eficiente e compromissada com o cliente, do que o que foi gasto para construí-la.

Ah! Ainda temos que pensar nos novos negócios que estão por vir e que dependerão da segurança para sua viabilidade. Afinal, que empresa não gostaria de ser o empreendimento que faz acontecer, em vez de apenas ver o que acontece?

O estudo de ROI definitivamente já faz parte do dia-a-dia dos executivos de tecnologia, e a segurança da informação, em especial, já é pauta certa de reunião e motivo de sobra para ser considerada um investimento. Resta, antes de tudo, gerar e implantar mecanismos de controle que, preliminarmente, reúnam informações que sinalizem os eventos em que há quebra de segurança e registrem os efeitos ao longo

do tempo. Com estes números, somados à projeções e simulações, será possível gerar um estudo de ROI capaz de traduzir na linguagem executiva o que ele realmente precisa entender: segurança é um investimento importante, necessário, mensurável e justificável.

Importantíssimo ressaltar, neste momento, que todo investimento tem seu ponto de inflexão, ou seja, um ponto na curva onde o retorno já não é proporcional ao esforço empregado. Esta situação é indesejada e deve ser alvo de atenção para evitar sua ocorrência. Seria o mesmo que investir em segurança um montante maior do que o próprio valor do bem protegido, considerando e ponderando, é claro, todos os aspectos associados à operação do negócio.

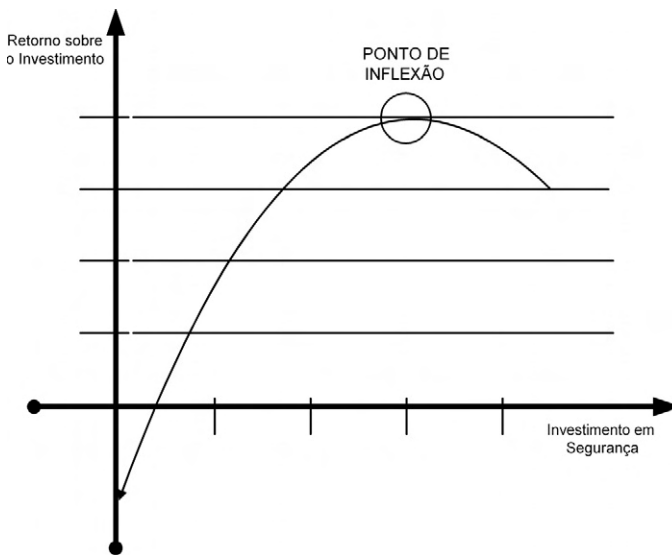


Figura 2-11 *Análise do ponto de inflexão dos investimentos em segurança x ROI.*

2.6 Posicionamento Hierárquico

Diante da abrangência dos desafios associados à Segurança da Informação, torna-se fundamental reorganizar a estrutura hierárquica da empresa a fim de suprir as novas demandas. É comum haver imediata confusão ao associar as atividades e a responsabilidade da gestão de segurança à área tecnológica. Muitas empresas insistem em relacionar e, muitas vezes, encapsular o orçamento e as ações de segurança ao Plano Diretor de Informática ou Plano Estratégico de TI.

Se considerarmos a diversidade das vulnerabilidades, ameaças e impactos que incidem sobre todos os ambientes e processos da empresa, veremos que tal modelo não cumpre o papel. Dessa forma, a empresa passaria a ter uma coordenação da segurança voltada para o aspecto tecnológico, decerto importante, mas não o único a merecer atenção, pois os demais aspectos físico e humano estariam sendo esquecidos e potencializariam os riscos.

As ações precisam estar intimamente alinhadas às diretrizes estratégicas da empresa e, para isso, é necessário ter uma visão corporativa, global e ampla, capaz de criar sinergia entre as atividades e, principalmente, maior retorno sobre o investimento. Este último, conseguido principalmente pela eliminação de ações redundantes e, muitas vezes conflitantes, que depreciam o plano corporativo de segurança da informação.

Herdando a importância e a participação já praticadas pelo Comitê de Auditoria, um Comitê Corporativo de Segurança da Informação deve ser criado. Posicionada no segundo nível hierárquico, ao lado do Comitê Executivo que reúne o CIO, CEO e conselheiros, esta unidade deve ser multidepartamental, coordenada e mediada pelo *Security Officer*, mas com forte representatividade das diretorias da empresa.

Considerando o porte e o modelo organizacional da empresa, poderá ser necessária a criação de Comitês Interdepartamentais de Segurança que irão se reportar ao Comitê Corporativo. Estes movidos por representantes de perfil gerencial – sintonizados com o *Security Officer* – que estarão segmentando as ações a partir de atividades tático-operacionais. Simultaneamente, atuarão como consolidadores de resultados parciais e finais, desempenhando funções de coordenação, controle, planejamento/avaliação e execução, fazendo-os chegar ao Comitê Corporativo a fim de realimentar o processo de gestão.

2.7 Gerência de Mudanças

Mudar é a única certeza. Esta frase já está mais do que desgastada, mas continua válida quando aplicada ao desafio das empresas diante da Segurança da Informação.

Muitas são as variáveis que interferem direta e indiretamente nos riscos operacionais do negócio. Mudanças mercadológicas, novos mercados, inovações tecnológicas, expansão física e crescimento dos recursos humanos são exemplos que acabam mexendo na equação do risco, fazendo-o oscilar e sair de seu ponto de equilíbrio. (Consulte a Figura 2-13, na página 30.)

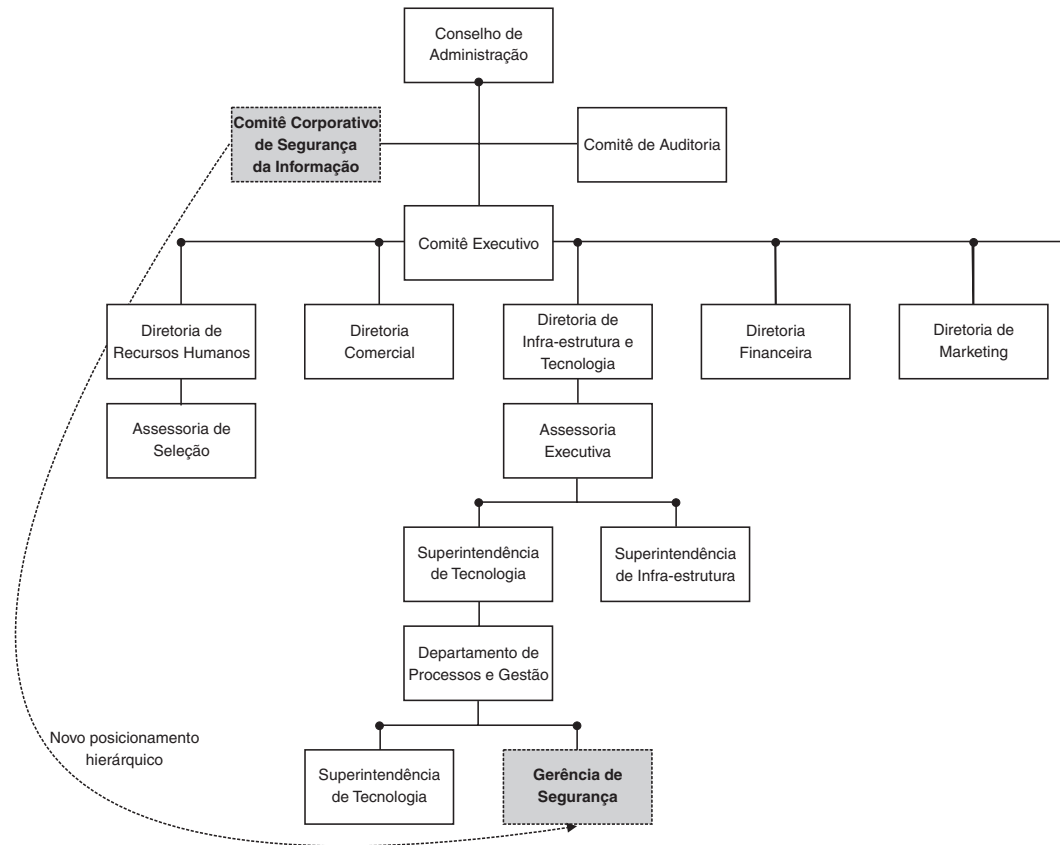


Figura 2-12 *Posicionamento hierárquico adequado aos desafios com amplitude corporativa.*

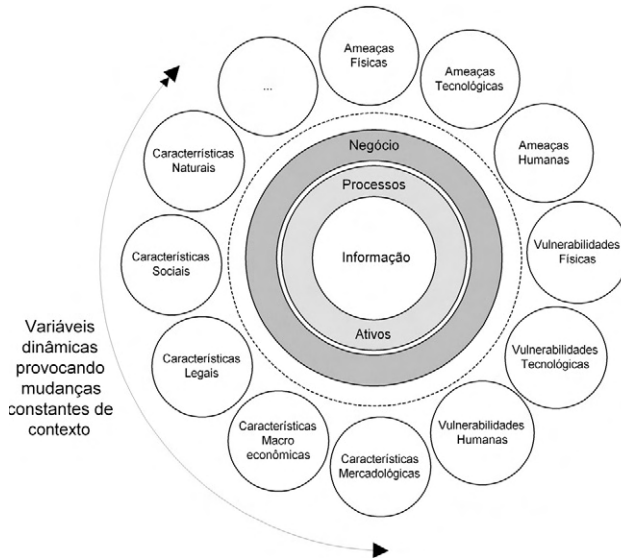


Figura 2-13 Percepção do dinamismo do contexto em que a empresa está inserida.

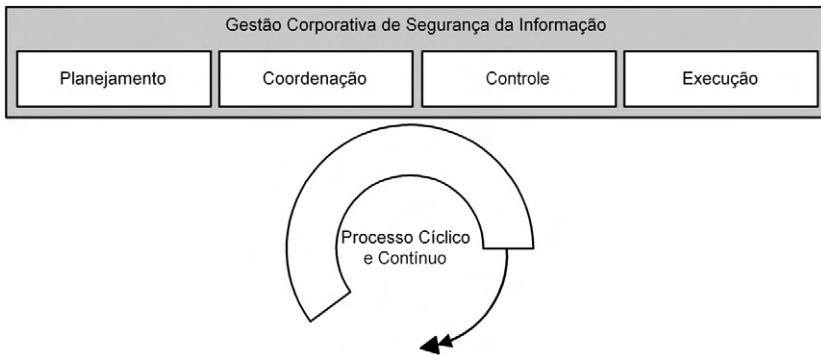


Figura 2-14 Visão macro do processo de gestão.

Diante do dinamismo dessas variáveis, muitas das quais imprevisíveis e incontroláveis, as empresas não poderão se deixar encurralar por estarem respaldadas por uma solução de segurança que represente apenas um projeto com início, meio e fim. Todas precisarão de algo igualmente dinâmico, um processo, capaz de acompanhar com velocidade as variações do ambiente e ajustar os controles para manter o nível de risco adequado.

A segurança que todas deverão buscar deve ser mantida por um verdadeiro processo de Gestão Corporativa de Segurança da Informação, sustentado por subprocessos retroalimentados, que interajam

tudo o tempo com as variáveis e estejam constantemente sendo ajustados às diretrizes estratégicas do negócio.

Pense neste exato momento em sua empresa. Não poderia estar ocorrendo agora uma nova contratação de recursos humanos? O *upgrade* ou a atualização de um servidor e seu sistema operacional? A implantação de um novo sistema de gestão, aplicação, conexão à Internet, ou, ainda, a ocupação de uma nova sala comercial ou prédio? Não poderia estar sofrendo os efeitos de um regime de perigosas tempestades, ou a aparição de um novo e voraz concorrente?

Pois estes fatos representariam mudanças que interfeririam nos seus riscos operacionais, gerando a necessidade de uma análise minuciosa dos reflexos que posteriormente serviriam para subsidiar a definição das próximas ações. Você precisa de um Modelo de Gestão Corporativo de Segurança da Informação!

2.8 Modelo de Gestão Corporativa de Segurança

Não basta criar um novo departamento ou unidade administrativa e chamá-lo de Comitê Corporativo de Segurança da Informação. É preciso ter uma visão clara de todas as etapas que compõem o desafio corporativo da segurança e formalizar os processos que darão vida e dinamismo à gestão.

Estamos falando de um Modelo de Gestão Corporativa de Segurança da Informação cíclico e encadeado, formado pelas etapas:

- Comitê Corporativo de Segurança da Informação
- Mapeamento de Segurança
- Estratégia de Segurança
- Planejamento de Segurança
- Implementação de Segurança
- Administração de Segurança
- Segurança na Cadeia Produtiva

Cada uma dessas etapas cumpre um papel importante no ciclo e gera resultados finais que deverão estar devidamente formatados e prontos para alimentar a etapa subsequente. Desta forma será possível reagir com velocidade às mudanças que, inevitavelmente, ocorrerão na operação do negócio, fazendo o risco oscilar.

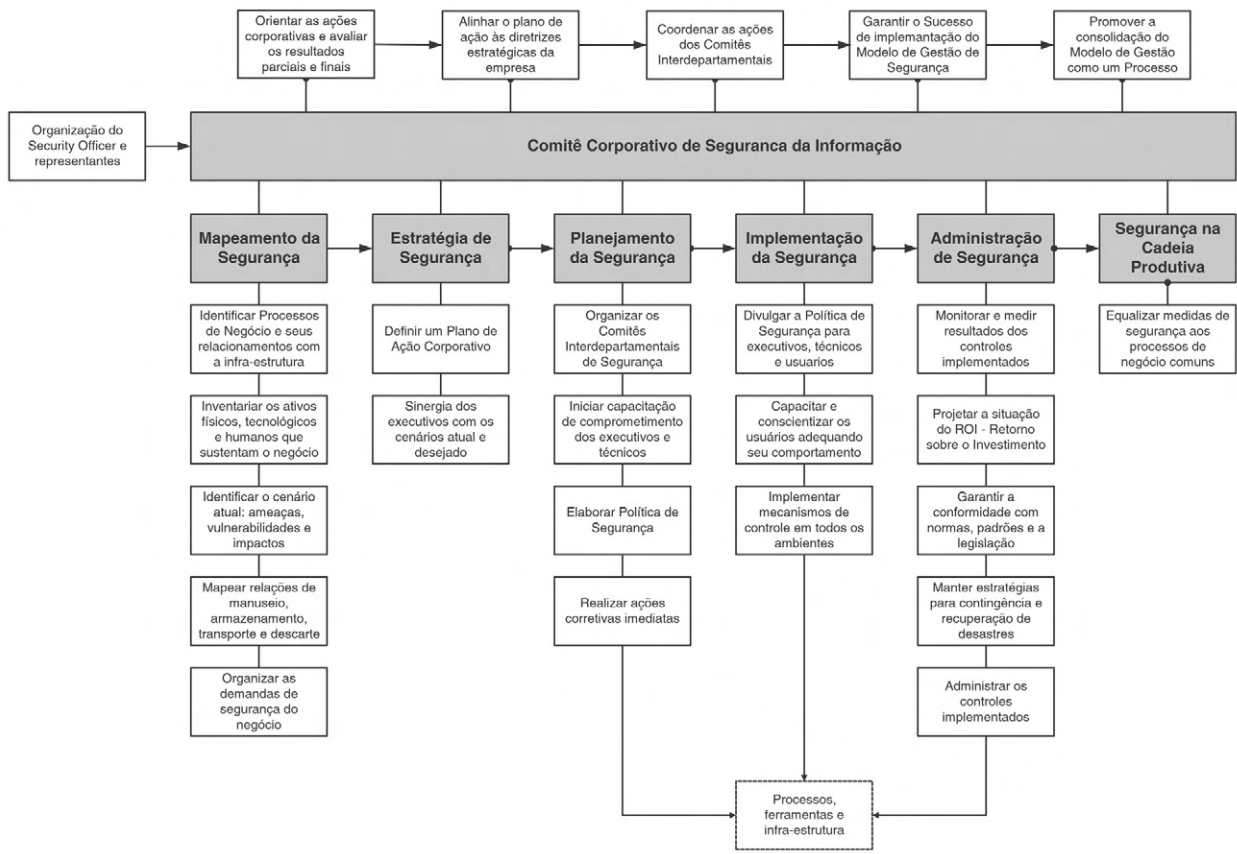


Figura 2-15 Diagrama do Modelo de Gestão Corporativo de Segurança da Informação

Comitê Corporativo de Segurança da Informação

- Orientar as ações corporativas de segurança e todas as etapas do modelo, além de medir os resultados parciais e finais com o intuito de reparar desvios de foco.
- Alinhar o plano de ação às diretrizes estratégicas do negócio, buscando agregar valor e viabilizar o melhor retorno sobre o investimento.
- Coordenar os agentes de segurança em seus Comitês Interdepartamentais, a fim de sintonizá-los quanto a possíveis ajustes no plano de ação.
- Garantir o sucesso de implantação do Modelo de Gestão Corporativo de Segurança da Informação, que irá preparar e dar autonomia à empresa para gerir seus atuais e futuros desafios associados.
- Promover a consolidação do Modelo de Gestão Corporativo de Segurança da Informação como um processo dinâmico autogerido.

Mapeamento de Segurança

- Identificar o grau de relevância e as relações diretas e indiretas entre os diversos processos de negócio, perímetros, infra-estruturas.
- Inventariar os ativos físicos, tecnológicos e humanos que sustentam a operação da empresa, considerando também as demais variáveis internas e externas que interferem nos riscos da empresa, como: mercado, nicho, concorrência, expansão etc.
- Identificar o cenário atual – ameaças, vulnerabilidades e impactos – e especular a projeção do cenário desejado de segurança capaz de sustentar e viabilizar os atuais e novos negócios da empresa.
- Mapear as necessidades e as relações da empresa associadas ao manuseio, armazenamento, transporte e descarte de informações.
- Organizar as demandas de segurança do negócio.

Estratégia de Segurança

- Definir um plano de ação, comumente plurianual, que considere todas as particularidades estratégicas, táticas e operacionais do negócio mapeadas na etapa anterior, além dos aspectos de risco físicos, tecnológicos e humanos.

- Criar sinergia entre os cenários atual e desejado, além da sintonia de expectativas entre os executivos, a fim de ganhar comprometimento e apoio explícito às medidas previstas no plano de ação.

Planejamento de Segurança

- Organizar os Comitês Interdepartamentais, especificando responsabilidades, posicionamento e escopo de atuação, oficializando seu papel diante de ações locais em sintonia com ações globais coordenadas pelo Comitê Corporativo de Segurança da Informação.
- Iniciar ações preliminares de capacitação dos executivos e técnicos, a fim de melhor orientá-los quanto aos desafios, envolvendo-os nos resultados e compartilhando com eles a responsabilidade pelo sucesso do modelo de gestão.
- Elaborar uma Política de Segurança da Informação sólida, considerando com extrema particularização e detalhamento as características de cada processo de negócio, perímetro e infra-estrutura, materializando-a através de Diretrizes, Normas, Procedimentos e Instruções que irão oficializar o posicionamento da empresa ao redor do tema e, ainda, apontar as melhores práticas para o manuseio, armazenamento, transporte e descarte de informações na faixa de risco apontada como ideal.
- Realizar ações corretivas emergenciais em função do risco iminente percebido nas etapas de mapeamento e atualmente, na elaboração dos critérios definidos na Política de Segurança.

Implementação de Segurança

- Divulgar corporativamente a Política de Segurança, a fim de torná-la o instrumento oficial, de conhecimento de todos, que irá nortear os executivos, técnicos e usuários quanto às melhores práticas no relacionamento com a informação.
- Capacitar conscientizando os usuários no que se refere ao comportamento diante do manuseio, armazenamento, transporte e descarte da informação, incluindo o conhecimento dos critérios, proibições e responsabilizações inerentes ao assunto.

- Implementar mecanismos de controle físicos, tecnológicos e humanos que irão permitir a eliminação das vulnerabilidades ou a sua viável administração, a fim de conduzir o nível de risco a um patamar desejado de operação.

Administração de Segurança

- Monitorar os diversos controles implementados, medindo sua eficiência e sinalizando mudanças nas variáveis que interferem direta e indiretamente no nível de risco do negócio.
- Projetar a situação do ROI – Retorno sobre o Investimento, com base nas medições realizadas, permitindo identificar resultados alcançados e, ainda, viabilizar novas necessidades que surgirem por demandas do negócio.
- Garantir a adequação e a conformidade do negócio com normas associadas, regras internas, regras do segmento de mercado, padrões e legislação incidente.
- Manter planos estratégicos para contingência e recuperação de desastres, objetivado garantir o nível de disponibilidade adequado e a conseqüente continuidade operacional do negócio.
- Administrar os controles implementados, adequando suas regras de operação aos critérios definidos na Política de Segurança, ou ainda, preparando-as para atender novas necessidades provocadas por mudanças de contexto ou variáveis internas e externas.

Segurança na Cadeia Produtiva

- Equalizar as medidas de segurança adotadas pela empresa aos Processos de Negócio comuns, mantidos junto aos parceiros da cadeia produtiva: fornecedores, clientes, governo etc; a fim de nivelar o fator de risco sem que uma das partes exponha informações compartilhadas e represente uma ameaça à operação de ambos os negócios.

Como se pode ver, o que chamamos de segurança da informação deve assumir a forma de um conjunto de processos integrados que têm objetivos locais específicos, mas estão intimamente alinhados a um único objetivo corporativo: gerir dinamicamente mecanismos de con-

trole abrangentes – considerando os processos, tecnologias e pessoas – que agreguem valor ao negócio, permitindo sua operação com risco controlado.

2.9 Agregando Valor ao Negócio

A análise do Retorno sobre o Investimento já deve ter dado pistas sobre os resultados mensuráveis associados ao Modelo de Gestão Corporativa de Segurança; mas é conveniente chamarmos a atenção também aos benefícios da gestão integrada sob a ótica do executivo e seu negócio.

- Valoriza as ações da empresa.
- Viabiliza novos negócios.
- Viabiliza a exploração para novos mercados.
- Viabiliza novas fontes de receita.
- Aumenta o *market-share*.
- Aumenta o *share of mind*.
- Consolida a imagem de modernidade.
- Consolida a imagem de saúde administrativa.
- Consolida o diferencial competitivo proporcionado pela tecnologia aplicada.
- Aumenta a satisfação dos clientes.
- Aumenta a produtividade dos usuários.
- Aumenta a receita.
- Aumenta a lucratividade.
- Aumenta a agilidade na adaptação à mudanças.
- Aumenta os níveis de disponibilidade operacional.
- Reduz os custos provocados por ameaças que exploram as falhas de segurança.
- Reduz os custos provocados pela má utilização dos recursos tecnológicos.
- Reduz os riscos operacionais.

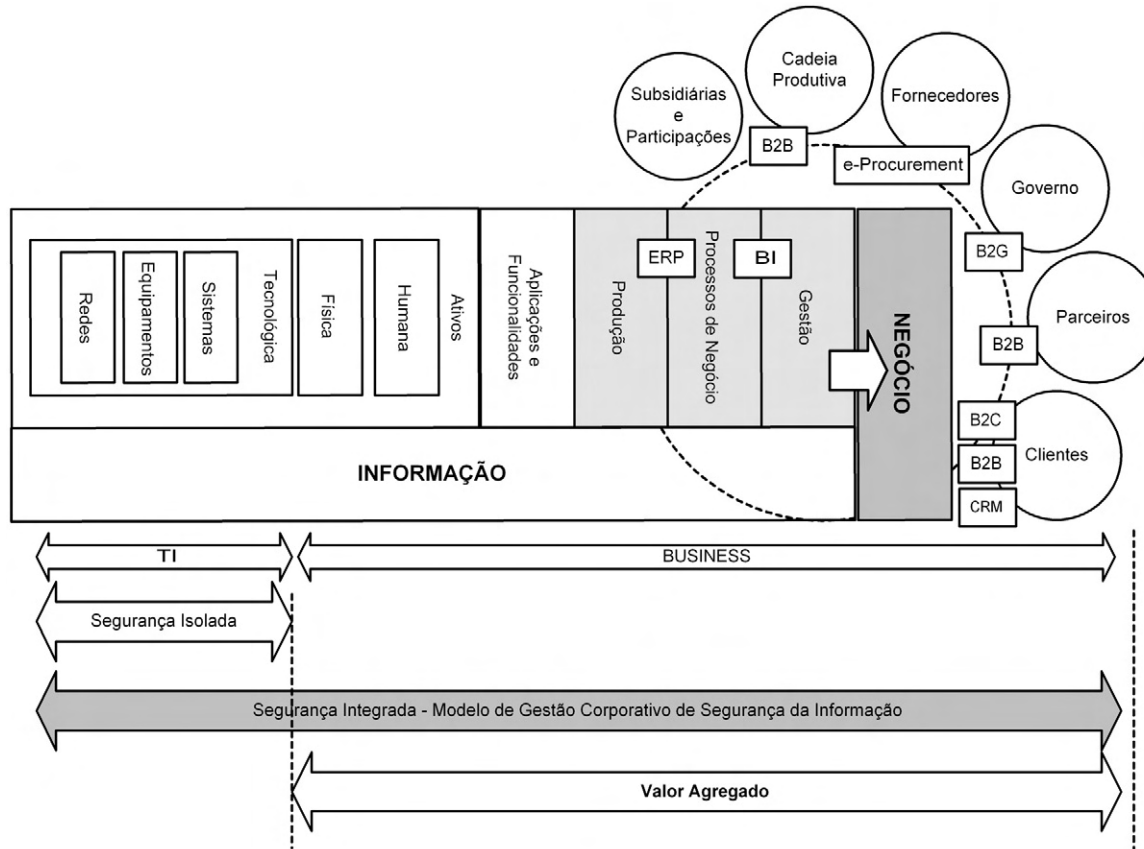


Figura 2-16 Percepção do valor agregado promovido pelo modelo de gestão integrada.

- Prepara a empresa para os desafios atuais.
- Prepara a empresa para reagir aos desafios futuros.
- Preserva a imagem da empresa.
- Integra segurança ao negócio.

A gestão integrada é um dos benefícios tangíveis mais relevantes proporcionado pelo modelo, pois é o responsável por evitar investimentos redundantes, ações desencontradas, atividades contrárias ou conflitantes e, principalmente, por proporcionar a canalização de esforços que vão ao encontro de um objetivo comum: o *business* da empresa.

Knowledge Checkpoint 1

Este ponto de checagem de conhecimento é uma breve e objetiva consolidação dos conceitos abordados em cada seção do livro com o objetivo de reforçar o processo de absorção do conteúdo relevante.

Informação: ativo cada vez mais valorizado

CONCEITO: “A Informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa”.

Crescimento da Dependência

CONCEITO: “Os riscos são inerentes e proporcionais aos índices de dependência que a empresa tem da informação e da complexidade da estrutura que suporta os processos de automação, informatização e compartilhamento de informações”.

Visão holística do Risco

CONCEITO: “Considerar os planos e identificar os desafios e as características específicas do negócio são os primeiros passos para modelar uma solução de segurança adequada”.

Receita explosiva

CONCEITO: “Olhar ao redor e projetar novas situações devem ser uma prática para as empresas preocupadas em construir uma solução sólida”.

da, mas adequadamente flexível para se ajustar às mudanças que, inevitavelmente, ocorrerão no ambiente”.

Ciclo de Vida da Informação

CONCEITO: “A visão corporativa da segurança da informação deve ser comparada a uma corrente, em que o elo mais fraco determina seu grau de resistência e proteção. A invasão ocorre onde a segurança falha!”

Desafios

Anatomia do Problema

CONCEITO: “Segurança é implementar controles que reduzam o risco a níveis adequados, viáveis e administráveis”.

Visão Corporativa

CONCEITO: “As empresas são diferentes e precisarão mapear o seu risco através da ponderação de ameaças, vulnerabilidades físicas, tecnológicas e humanas, e impactos, em busca da especificação da solução ideal”.

Pecados praticados

CONCEITO: “Aprender com as experiências e erros cometidos por terceiros faz parte do processo de crescimento; mas aprender com os próprios deve fazer parte do seu processo de sobrevivência”.

Conscientização do Corpo Executivo

CONCEITO: “Somente com apoio executivo as ações de segurança ganharão autonomia e abrangência capazes de incidir corporativamente sobre os furos de segurança”.

Retorno sobre o Investimento

CONCEITO: “Projetar o ROI de ações integradas e alinhadas com as diretrizes estratégicas da empresa representará eficaz ferramenta de conscientização e sensibilização do executivo, a fim de ganhar seu comprometimento”.

Posicionamento Hierárquico

CONCEITO: “Autonomia e posicionamento estratégico são condições primordiais para sustentar um processo dinâmico de administração de segurança eficiente”.

Gerência de Mudanças

CONCEITO: “Segurança deve ser tratada como um processo corporativo capaz de considerar e reagir dinamicamente às inevitáveis mudanças físicas, tecnológicas, humanas e contextuais”.

Modelo de Gestão Corporativa de Segurança

CONCEITO: “O fato de existir agora um modelo de gestão que sirva de bússola, não garante o sucesso de sua implantação. É preciso ter uma estrutura humana multiespecialista, dedicada e embasada conceitualmente, sempre em busca de atualização”.

Agregando Valor ao Negócio

CONCEITO: “Diferente do que se pensava, toda a iniciativa de segurança da informação deve ter como alvo principal o negócio e, conseqüentemente, suas ações devem estar totalmente convergentes, alinhadas e focadas nos desafios do negócio”.

Segurança da Informação

4.1 Conceitos de Segurança

Já dissecamos os desafios associados à segurança com superficialidade executiva, mas nenhuma expectativa será atingida se as ações não estiverem consistentemente embasadas por conceitos sólidos e amplamente reconhecidos.

Evitando reinventar a roda e dar nova interpretação que desprezasse as já bem realizadas e consolidadas, tomei emprestada a base de conhecimento chamada de Módulo *Security Body of Knowledge*, de propriedade da empresa brasileira líder em soluções corporativas de segurança de informação: Módulo Security Solutions.

Segurança da Informação

Podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

De forma mais ampla, podemos também considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. Desta forma, estaríamos falando da definição de regras que incidiriam sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades.

O Modelo de Gestão Corporativo de Segurança da Informação empresta à expressão um sentido mais amplo, considerando em primeiro plano os desafios do negócio como um todo. Diante desta abrangente orientação, ganham autonomia mais dois conceitos de segurança: autenticidade e legalidade, originalmente extraídos dos três precursores em função de suas importâncias dentro no contexto atual.

Estes, por sua vez, cumprem, respectivamente, o papel de sinalizar o comprometimento dos aspectos associados à autenticidade das partes envolvidas em troca de informações e a conformidade com a legislação associada vigente.

A expressão “Segurança da Informação” é, por si só, um termo ambíguo, podendo assumir dupla interpretação:

1. Segurança como uma prática adotada para tornar um ambiente seguro (atividade, ação, preservação dos princípios), de caráter interdisciplinar, composta de um conjunto de metodologias e aplicações que visam estabelecer: controles de segurança (por exemplo: de autenticação, autorização e auditoria) dos elementos constituintes de uma rede de comunicação e/ou que manipulem a informação; e procedimentos para garantir a continuidade de negócios na ocorrência de incidentes.
2. Resultado da prática adotada, objetivo a ser alcançado. É a característica que a informação adquire ao ser alvo de uma prática da segurança (segura – adjetivo, objetivo da prática).

Logo, ao se utilizar este termo, deve-se ter consciência desta ambigüidade, a fim de se identificar o conceito mais apropriado a ser abordado. Por exemplo:

Segurança como “meio” – A segurança da informação visa garantir a confidencialidade, integridade e disponibilidade da informação, a impossibilidade de que agentes participantes em transações ou na comunicação repudiem a autoria de suas mensagens, a conformidade com a legislação vigente e a continuidade dos negócios.

Segurança como “fim” – A segurança da informação é alcançada por meio de práticas e políticas voltadas a uma adequada padronização operacional e gerencial dos ativos, e processos que manipulam e executem a informação.

Conceitos básicos da Segurança da Informação

A segurança da informação tem como objetivo a preservação de três princípios básicos pelos quais se norteiam a implementação desta prática.

Confidencialidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.

Integridade – Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.

Disponibilidade – Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Informação

Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários).

A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvo de proteção da segurança da informação.

Ativo

Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

O termo ativo possui esta denominação, oriunda da área financeira, por ser considerado um elemento de valor para um indivíduo ou organização, e que, por esse motivo, necessita de proteção adequada (ISO/IEC-17799).

Existem muitas formas de dividir e agrupar os ativos para facilitar seu tratamento, mas um modelo em especial tem minha simpatia: equipamentos, aplicações, usuários, ambientes, informações e pro-

cessos. Desta forma, torna-se possível identificar melhor as fronteiras de cada grupo, tratando-os com especificidade e aumentando qualitativamente as atividades de segurança.

Aspectos da Segurança da Informação

Alguns elementos são considerados essenciais na prática da segurança da informação, dependendo do objetivo que se pretende alcançar.

Autenticação – processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controles de identificação desses elementos.

Legalidade – característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

Aspectos associados

Autorização – concessão de uma permissão para o acesso às informações e funcionalidades das aplicações aos participantes de um processo de troca de informações (usuário ou máquina), após a correta identificação e autenticação dos mesmos.

Auditoria – processo de coleta de evidências de uso dos recursos existentes, a fim de identificar as entidades envolvidas num processo de troca de informações, ou seja, a origem, destino e meios de tráfego de uma informação.

Autenticidade – garantia de que as entidades (informação, máquinas, usuários) identificadas em um processo de comunicação como remetentes ou autores sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação. Normalmente, o termo autenticidade é utilizado no contexto da certificação digital, onde recursos de criptografia e *hash* são utilizados para atribuir um rótulo de identificação às mensagens ou arquivos enviados entre membros de uma infra-estrutura de chave pública, visando garantir os

princípios/aspectos de: irretratabilidade, identidade, autenticidade, autoria, originalidade, integridade e confidencialidade.

Severidade – gravidade do dano que um determinado ativo pode sofrer devido à exploração de uma vulnerabilidade por qualquer ameaça aplicável.

Relevância do ativo – grau de importância de um ativo para a operacionalização de um processo de negócio.

Relevância do processo de negócio – grau de importância de um processo de negócio para o alcance dos objetivos e sobrevivência de uma organização.

Criticidade – gravidade referente ao impacto ao negócio causado pela ausência de um ativo, pela perda ou redução de suas funcionalidades em um processo de negócio, ou pelo seu uso indevido e não autorizado.

Irretratabilidade – característica de informações que possuem uma identificação do seu emissor que o autentica como o autor de informações por ele enviadas e recebidas. Sinônimo de não-repúdio.

Ameaças

Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, conseqüentemente, causando impactos aos negócios de uma organização.

Classificando as ameaças quanto a sua intencionalidade, elas podem ser divididas nos seguintes grupos.

Naturais – Ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.

Involuntárias – Ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia etc.

Voluntárias – Ameaças propositais causadas por agentes humanos como *hackers*, invasores, espões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

Vulnerabilidades

Fragilidade presente ou associada a ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

As vulnerabilidades por si só não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou condição favorável, que são as ameaças.

Exemplos de vulnerabilidades:

Físicas – Instalações prediais fora do padrão; salas de CPD mal planejadas; falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em sala com armários e fichários estratégicos; risco de explosões, vazamentos ou incêndio.

Naturais – Computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e outros, como falta de energia, acúmulo de poeira, aumento de umidade e de temperatura etc.

Hardware – Falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.

Software – Erros na instalação ou na configuração podem acarretar acessos indevidos, vazamento de informações, perda de dados ou indisponibilidade do recurso quando necessário.

Mídias – Discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.

Comunicação – Acessos não autorizados ou perda de comunicação.

Humanas – Falta de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, erros ou omissões; ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismo, roubo, destruição da propriedade ou dados, invasões ou guerras.

Medidas de Segurança

São as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, a redução das vulnerabilidades, a limitação do impacto ou minimização do risco de qualquer outra forma. As medidas de segurança são consideradas controles que podem ter as seguintes características:

Preventivas – medidas de segurança que tem como objetivo evitar que incidentes venham a ocorrer. Visam manter a segurança já implementada por meio de mecanismos que estabeleçam a conduta e a ética da segurança na instituição. Como exemplos podemos citar as políticas de segurança, instruções e procedimentos de trabalho, especificação de segurança, campanhas e palestras de conscientização de usuários; ferramentas para implementação da política de segurança (*firewall*, antivírus, configurações adequadas de roteadores e dos sistemas operacionais etc.)

Detectáveis – medidas de segurança que visam identificar condições ou indivíduos causadores de ameaças, a fim de evitar que as mesmas explorem vulnerabilidades. Alguns exemplos são: análise de riscos, sistemas de detecção de intrusão, alertas de segurança; câmeras de vigilância, alarmes, etc.

Corretivas – ações voltadas à correção de uma estrutura tecnológica e humana para que as mesmas se adaptem às condições de segurança estabelecidas pela instituição, ou voltadas à redução dos impactos: equipes para emergências, restauração de *backup*, plano de continuidade operacional, plano de recuperação de desastres.

Note que muitas das medidas de segurança podem possuir mais de uma característica, isto é, um plano de continuidade de negócios é tan-

to uma ação preventiva (quando da sua criação) quanto uma ação corretiva (quando da sua aplicação). Logo, esta categorização serve apenas para a identificação do foco que o trabalho de segurança está se propondo, quando o mesmo está sendo realizado.

Riscos

Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, causando, possivelmente, impactos nos negócios.

Impacto

Abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio.

Incidente

Fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: confidencialidade, integridade e disponibilidade.

Um incidente gera impactos aos processos de negócio da empresa, sendo ele o elemento a ser evitado em uma cadeia de gestão de processos e pessoas.

A gravidade de um incidente pode ser analisada em termos qualitativos e quantitativos, sendo medida pelo seu impacto. (Consulte a Figura 4-1.)

A partir deste diagrama de visão condensada, pode-se ter a real noção da amplitude do desafio corporativo da Segurança da Informação.

4.2 Teoria do Perímetro

Não há nada de novo para a área de segurança, principalmente a patrimonial, em falar de perímetro. Esta estrutura de segmentação de ambientes físicos é considerada estratégia militar de defesa e também se aplica ao cenário atual das empresas, mesmo que tenhamos de ultrapassar os aspectos físicos e aplicá-los para segmentar ambientes lógicos. Certamente o grande segredo para obter o melhor retorno dos mecanismos que garantam os níveis de proteção da informação está na segmentação inteligente dos ativos. Desta forma, torna-se possível aplicar os controles adequados – cada um oferecendo um nível previa-

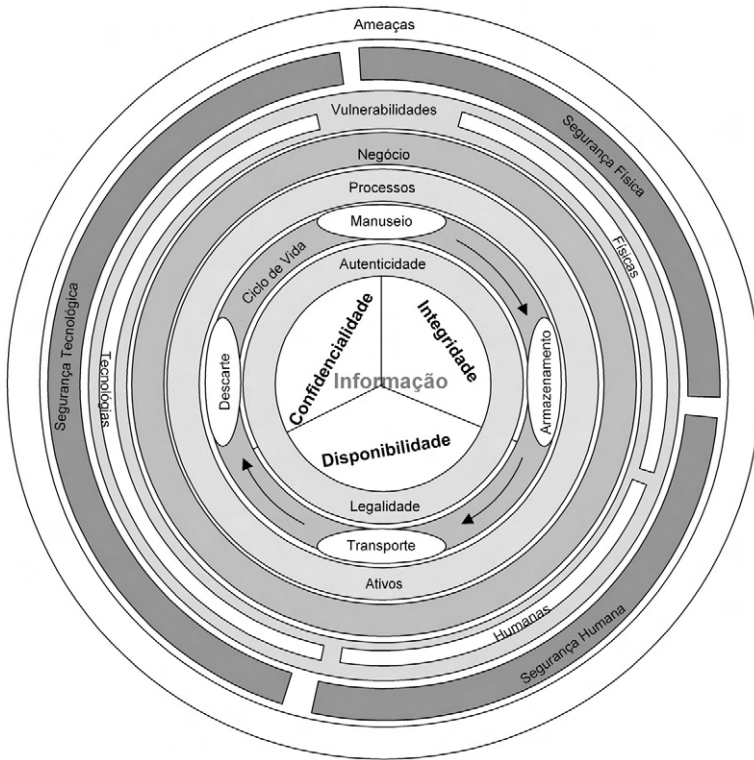


Figura 4-1 *Visão condensada dos desafios.*

mente dosado de proteção – sem que exceda os limites e nem fique aquém das necessidades.

Pensemos, por exemplo, sobre os recursos de auditoria restritiva de acesso à Internet. Se os funcionários não forem logicamente segmentados nos sistemas de acesso à rede, misturando departamentos e pessoas autorizadas pela necessidade imposta pela natureza da atividade, e outros funcionários cujo acesso é controlado ou totalmente proibido, perde-se a propriedade de aplicar os controles adequados a cada um dos perfis. Desta forma, elevam-se as chances de exceder o nível de controle para uns ou oferecer-lhes um nível aquém de suas necessidades, expondo, então, as informações desnecessariamente. (Consulte a Figura 4-2.)

Além de o perímetro estar associado à compartimentalização de espaços físicos e lógicos, ele também cumpre o importante papel de alerta e de mecanismo de resistência distribuído por áreas, a fim de permitir que tentativas de acesso indevido e invasão gerem sinais de alerta e

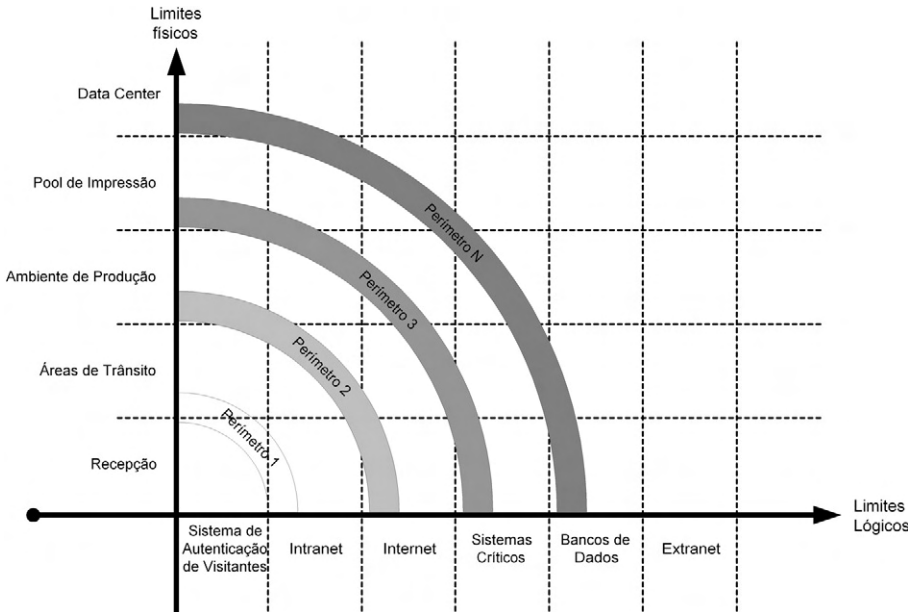


Figura 4-2 Ilustração representando perímetros físicos e lógicos.

se deparem com a resistência que propiciará tempo para que medidas contingenciais sejam tomadas antes da ação avançar ainda mais em direção do alvo.

4.3 Barreiras da Segurança

Conceitualmente, diante da amplitude e complexidade do papel da segurança, é comum estudarmos os desafios em camadas ou fases, particionando todo o trabalho para tornar mais claro o entendimento de cada uma delas. Chamamos esta divisão de barreiras. As seis barreiras de segurança.

Cada uma delas tem uma participação importante no objetivo maior de reduzir os riscos, e por isso, deve ser dimensionada adequadamente para proporcionar a mais perfeita interação e integração, como se fossem peças de um único quebra-cabeça. Note que este modelo conceitual implementa a teoria do perímetro, segmentando perímetros físicos ou lógicos, e oferecendo níveis de resistência e proteção complementares e tendenciosamente crescentes.

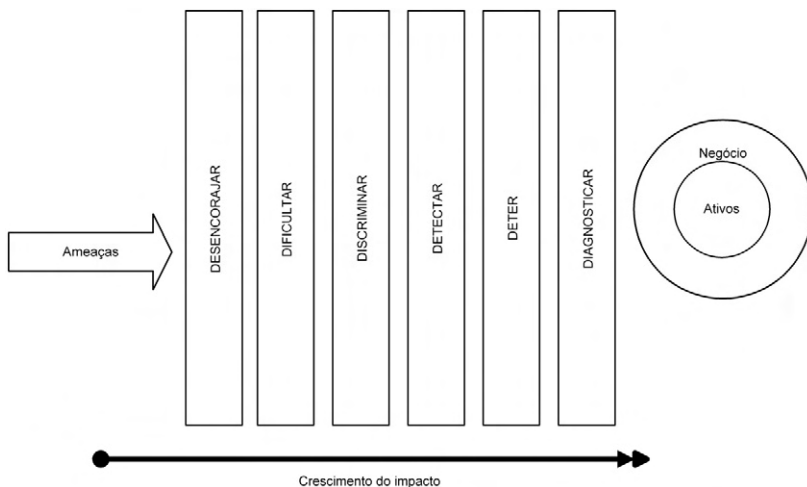


Figura 4-3 Diagrama representativo das barreiras de segurança.

Barreira 1: Desencorajar

Esta é a primeira das cinco barreiras de segurança e cumpre o papel importante de desencorajar as ameaças. Estas, por sua vez, podem ser desmotivadas ou podem perder o interesse e o estímulo pela tentativa de quebra de segurança por efeito de mecanismos físicos, tecnológicos ou humanos. A simples presença de uma câmera de vídeo, mesmo falsa, de um aviso da existência de alarmes, campanhas de divulgação da política de segurança ou treinamento dos funcionários informando as práticas de auditoria e monitoramento de acesso aos sistemas, já são efetivos nesta fase.

Barreira 2: Dificultar

O papel desta barreira é complementar à anterior através da adoção efetiva dos controles que irão dificultar o acesso indevido. Como exemplo, podemos citar os dispositivos de autenticação para acesso físico, como roletas, detectores de metal e alarmes, ou lógicos, como leitores de cartão magnético, senhas, *smartcards* e certificados digitais, além da criptografia, *firewall* etc.

Barreira 3: Discriminar

Aqui o importante é se cercar de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os siste-

mas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e bancos de dados. Os processos de avaliação e gestão do volume de uso dos recursos, como email, impressora, ou até mesmo o fluxo de acesso físico aos ambientes, são bons exemplos das atividades desta barreira.

Barreira 4: Detectar

Mais uma vez agindo de forma complementar às suas antecessoras, esta barreira deve munir a solução de segurança de dispositivos que sinalizem, alertem e instrumentem os gestores da segurança na detecção de situações de risco. Seja em uma tentativa de invasão, uma possível contaminação por vírus, o descumprimento da política de segurança da empresa, ou a cópia e envio de informações sigilosas de forma inadequada.

Entram aqui os sistemas de monitoramento e auditoria para auxiliar na identificação de atitudes de exposição, como o antivírus e o sistema de detecção de intrusos, que reduziram o tempo de resposta a incidentes.

Barreira 5: Deter

Esta quinta barreira representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio. O acionamento desta barreira, ativando seus mecanismos de controle, é um sinal de que as barreiras anteriores não foram suficientes para conter a ação da ameaça. Neste momento, medidas de detenção, como ações administrativas, punitivas e bloqueio de acessos físicos e lógicos, respectivamente a ambientes e sistemas, são bons exemplos.

Barreira 6: Diagnosticar

Apesar de representar a última barreira no diagrama, esta fase tem um sentido especial de representar a continuidade do processo de gestão de segurança da informação. Pode parecer o fim, mas é o elo de ligação com a primeira barreira, criando um movimento cíclico e contínuo. Devido a esses fatores esta é a barreira de maior importância. Deve ser conduzida por atividades de análise de riscos que considerem tanto os aspectos tecnológicos quanto os físicos e humanos, sempre orientados

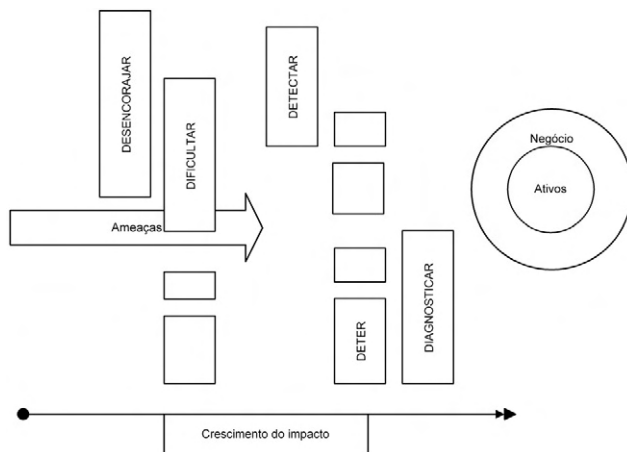


Figura 4-4 Ilustração simbólica de uma ação de segurança orientada por um diagnóstico inadequado.

às características e às necessidades específicas dos processos de negócio da empresa.

Importante notar que um trabalho preliminar de diagnóstico mal conduzido ou executado sem metodologia e instrumentos que confirmam maior precisão ao processo de levantamento e análise de riscos, poderá distorcer o entendimento da situação atual de segurança e simultaneamente a situação desejada. Desta forma, aumenta a probabilidade de se dimensionar inadequadamente estas barreiras, distribuindo os investimentos de forma desproporcional, redundante muitas vezes, e pior, de forma ineficaz. O retorno sobre os investimentos não corresponderá às expectativas e a empresa não atingirá o nível de segurança adequado à natureza de suas atividades.

4.4 Equação do Risco

Cada negócio, independente de seu segmento de mercado e seu *core business*, possui dezenas, talvez centenas, de variáveis que se relacionam direta e indiretamente com a definição do seu nível risco. Identificar estas variáveis passa a ser a primeira etapa do desafio.

Interpretação da equação

O risco é a probabilidade de que agentes, que são as **ameaças**, explorem **vulnerabilidades**, expondo os **ativos** a perdas de confidencialida-

de, integridade e disponibilidade, e causando impactos nos negócios. Estes impactos são limitados por medidas de segurança que protegem os ativos, impedindo que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco.

$$\begin{array}{ccccccc}
 \mathbf{R} & = & \mathbf{V} & \times & \mathbf{A} & \times & \mathbf{I} \\
 \text{RISCO} & & \text{VULNERABILIDADES} & & \text{AMEAÇAS} & & \text{IMPACTOS} \\
 & & \hline
 & & \mathbf{M} & & & & \\
 & & \text{MEDIDAS DE SEGURANÇA} & & & &
 \end{array}$$

Figura 4-5 Diagrama da Equação do Risco de Segurança da Informação.

Por melhor que estejam protegidos os ativos, novas tecnologias, mudanças organizacionais e novos processos de negócio podem criar vulnerabilidades ou identificar e chamar a atenção para as já existentes. Além disso, novas ameaças podem surgir e aumentar significativamente a possibilidade de impactos no negócio. Sendo assim, medidas corretivas de segurança precisam ser consideradas, pois sempre haverá a possibilidade de um incidente ocorrer, por mais que tenhamos tomado todas as medidas preventivas adequadas.

Risco tendendo a zero

É fundamental que todos tenhamos a consciência de que não existe segurança total e, por isso, devemos estar bem estruturados para suportar mudanças nas variáveis da equação, reagindo com velocidade e ajustando o risco novamente aos padrões pré-especificados como ideal para o negócio.

Diante disso, concluímos que não há um resultado R (risco) igual para todos. Sempre será necessário avaliar o nível de segurança apropriado para cada momento vivido pela empresa, como se tivéssemos de nos pesar em períodos regulares para definir a melhor dose de ingestão calórica (dose de segurança) do período, a fim de buscar aproximação com o peso ideal (nível de risco) para o momento.

4.5 Comitê Corporativo de Segurança da Informação

Representando o núcleo concentrador dos trabalhos, o Comitê Corporativo de Segurança da Informação deve estar, além de adequadamente

posicionado hierarquicamente no organograma, formatado a partir da clara definição de seu objetivo, estrutura, funções, responsabilidades, perfil dos executores, além da formal e oficial identificação de seus membros, que darão representatividade aos departamentos mais críticos e relevantes da empresa.

Reunir gestores com visões do mesmo objeto, mas de pontos distintos, é fundamental para a obtenção da nítida imagem dos problemas, desafios e impactos. Por isso, envolver representantes das áreas Tecnológica, Comunicação, Comercial, Negócios, Jurídico, Patrimonial, Financeira, Auditoria etc., em muito agregará para o processo de gestão, de forma a evitar conflitos, desperdícios, redundâncias e o principal: fomentar a sinergia da empresa intimamente alinhada às suas diretrizes estratégicas de curto, médio e longo prazos.

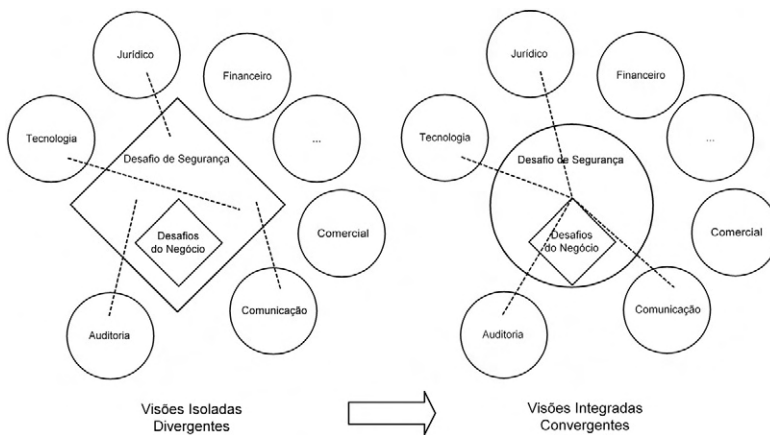


Figura 4-6 Cenários da integração de visões distintas do mesmo objeto (visão do farol).

Objetivos

- Fomentar o Modelo de Gestão Corporativa de Segurança da Informação, através de ações distribuídas, porém integradas, que têm abrangência física, tecnológica e humana, e interferem em todos os Processos de Negócio mantenedores da operação da empresa.
- Analisar, através de equipe multidisciplinar e multidepartamental com representatividade no comitê, os resultados parciais e finais das ações de forma a medir efeitos, compará-los às metas definidas e realizar ajustes no Plano Diretor de Segurança, ade-

quando-o à nova realidade gerada pela mudança de variáveis internas e externas.

- Interagir constantemente com o Comitê Executivo e o Comitê de Auditoria, buscando sinergia dos macro objetivos da empresa, além de trocar informações ligadas aos índices e indicadores de segurança como forma de demonstrar os resultados corporativos do Comitê de Segurança.
- Alinhar e definir ações para os Comitês Interdepartamentais que deverão agir localmente de forma distribuída, coletando, com maior riqueza de detalhes, os fatos relacionados aos aspectos físicos, tecnológicos e humanos inerentes à sua esfera e abrangência.

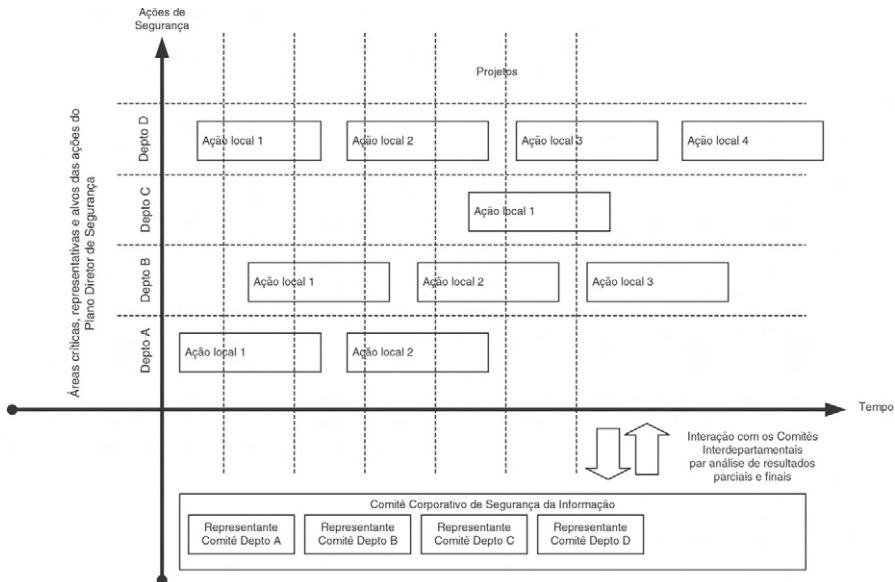


Figura 4-7 Interação do Comitê com as ações corporativas e os Comitês Interdepartamentais.

Coordenador do Comitê Corporativo de Segurança da Informação Security Officer

Estrutura Básica do Comitê

- Coordenação Geral de Segurança
- Coordenação de Segurança

- Controle
- Planejamento e Avaliação
- Execução

Em função da amplitude da atuação do Comitê Corporativo, empresas de grande porte que têm um modelo de gestão distribuído e bem pulverizado, passam a necessitar de “células” de segurança distribuídas pela empresa e localizados em departamentos ou unidades mais representativas e críticas. Estas células recebem o nome de Comitês Interdepartamentais de Segurança da Informação e mantêm, em sua estrutura, as mesmas 4 últimas funções e responsabilidades que se aplicam ao Comitê Corporativo de Segurança. O que os distingue nesta dimensão é a abrangência e a esfera de atuação que correspondem, respectivamente, à gestão tático-operacional e à gestão estratégica.

Desta forma, passam a ter uma relação de dependência e sinergia, em que os comitês interdepartamentais se reportam ao comitê corporativo, que, por sua vez, os mantém alinhados às definições estratégicas de segurança e da empresa como um todo.

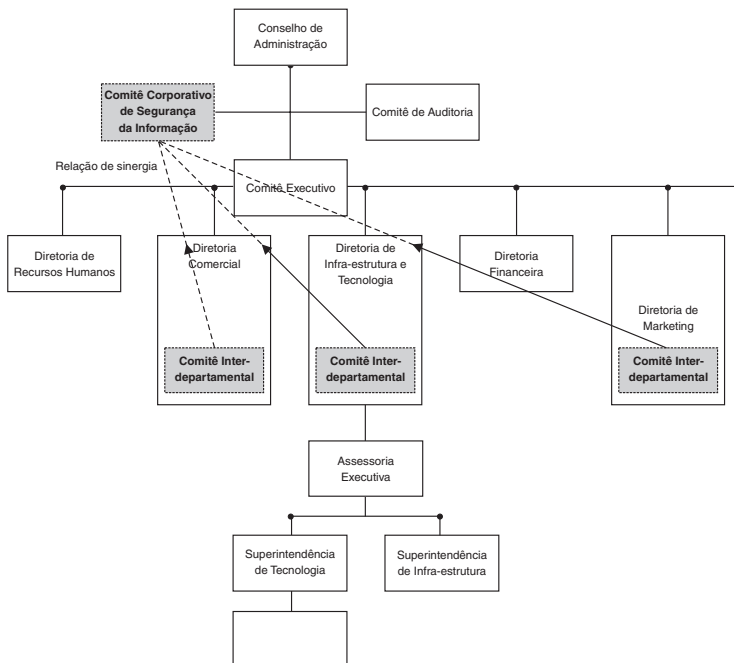


Figura 4-8 Relação de comitês contextualizada a empresas de grande porte e modelo de gestão distribuído.

Estrutura, Funções e Responsabilidades

- **Coordenação Geral de Segurança**
 - Mobilizar corporativamente as áreas associadas
 - Deliberar medidas e contra-medidas corporativas
 - Definir índices, indicadores e metas estratégicas
- **Coordenação de Segurança**
 - Coordenar as subfunções do Coordenador Geral de Segurança
 - Avaliar os resultados alcançados
 - Propor mudanças
 - Propor medidas e contra-medidas
 - Mobilizar os gestores críticos associados
- **Planejamento e Avaliação**
 - Elaborar relatórios gerenciais sobre os resultados alcançados
 - Elaborar propostas de projetos específicos de segurança
 - Promover palestras de conscientização e manutenção do conhecimento
 - Apoiar consultivamente o Coordenador Geral
- **Controle**
 - Conduzir ações de auditoria e monitoramento
 - Analisar métricas dos índices e indicadores
 - Realizar análises de risco
 - Treinar a função de Execução no manuseio dos índices e indicadores
- **Execução**
 - Cumprir e fazer cumprir a Política de Segurança nos ambientes associados
 - Informar à função Controle os resultados dos índices e indicadores

- Responder a questões de auditoria
- Registrar ocorrências de quebra de segurança reportando-as à função Controle
- Executar medidas e contra-medidas de segurança

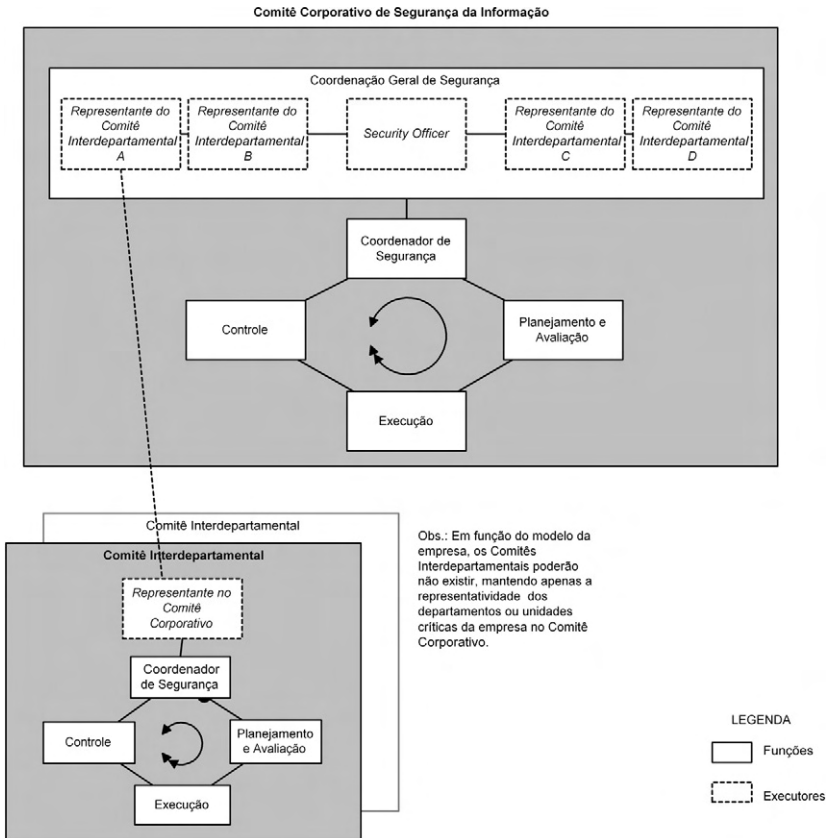


Figura 4-9 Macrodiagrama de estrutura.

Perfil dos Executores

- Coordenação Geral de Segurança
 - Security Officer com apoio de diretores e seus representantes
- Coordenação de Segurança
 - Gestor de Segurança
- Planejamento e Avaliação

- Consultor de Segurança
- Consultor de Contingência
- Analista de Segurança
- Assistente de Segurança
- Controle
 - Auditor de Segurança
 - Gerente de Risco
 - Monitor de Segurança
- Execução
 - Administrador de Rede
 - Gestor de Desenvolvimento
 - Gestor de Produção
 - Gestor de Aplicação

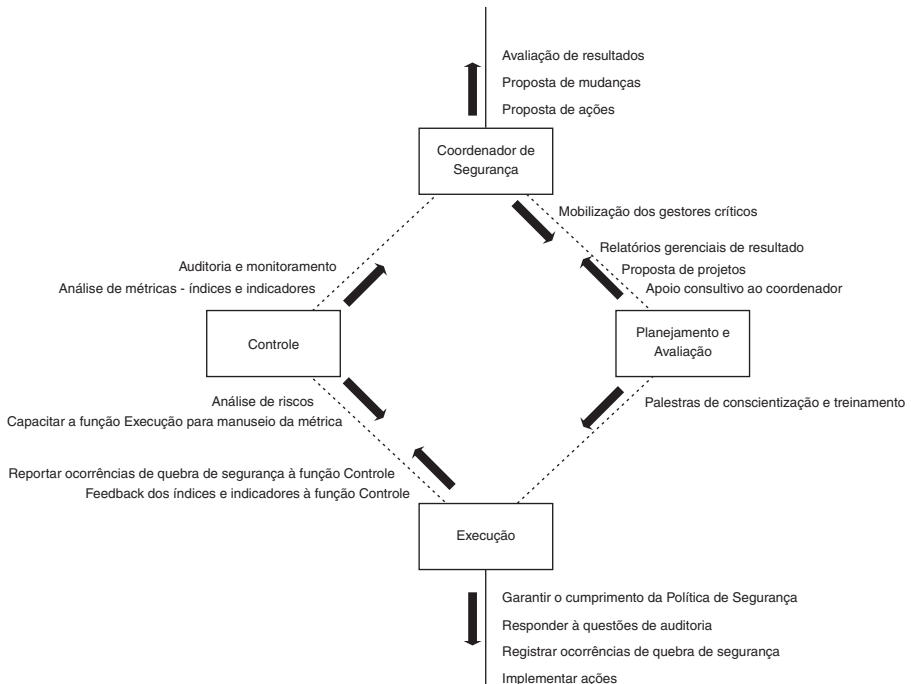


Figura 4-10 Macrodiagrama funcional.

- Gestor de Segurança Física
- Suporte a Tecnologias

4.6 Papel do Security Officer

O *Security Officer*, atuando como eixo central na função de Coordenação Geral do Comitê Corporativo de Segurança da Informação, tem papel substancial para o sucesso do modelo. É quem recebe toda a pressão da empresa diante dos resultados e quem é demandado a adequar o nível de controle, e, portanto, o nível de segurança para suprir as novas demandas do negócio.

Diante do porte de seu desafio, o profissional que ocupar essa posição tem de estar estritamente verticalizado às funções associadas, sem compartilhamento de foco, e, para tal, não basta ter perfil tecnológico extremo. Esse executivo deve ser multiespecialista, deve ter uma visão completa e horizontal da segurança da informação a partir de conceitos sólidos, deve possuir ricos fundamentos de gestão de projetos, coordenação de equipes e liderança. Tem de ser verdadeiramente executivo, em toda a amplitude da palavra, alimentando com sabedoria os relacionamentos interpessoais, sempre em busca da conquista de comprometimento.

Seu fator crítico de sucesso é manter o alinhamento e o foco nas características e necessidades no negócio, conhecendo-o profundamente, e preocupando-se em ajustar constantemente seu plano de ação às premissas e definições estratégicas da empresa.

Como todo executivo, deve estar orientado a resultados, que pode ser entendido nesta dimensão, por fomentar a obtenção do melhor retorno sobre os investimentos, levando a empresa a operar sob risco controlado, além de prepará-la para gerir dinamicamente a segurança, preparando-a para os atuais e futuros desafios.

Fatores importantes para o adequado exercício da atividade de *Security Officer*

- Conhecer o negócio da empresa.
- Conhecer o segmento de mercado.
- Conhecer o *Business Plan* da empresa.

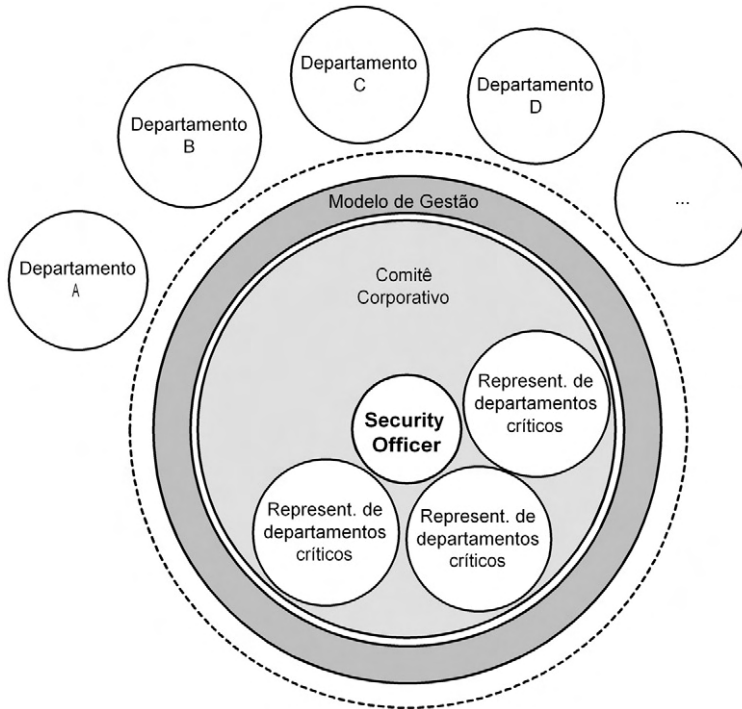


Figura 4-11 *Security Officer como eixo do comitê corporativo e, conseqüentemente, do modelo de gestão de segurança.*

- Conhecer as expectativas do Corpo Executivo em relação à sua atividade.

Macrodesafios do *Security Officer*

- Compreender as fronteiras de autoridade.
- Adequar o Plano de Ação ao *Budget* da Segurança.
- Acompanhar as mudanças culturais da empresa.
- Identificar, no mercado, profissionais preparados.
- Organizar as demandas de segurança do negócio.
- Gerenciar mudanças físicas, tecnológicas e humanas.

4.7 Como conduzir internamente a negociação

Antes de pensar na forma, será preciso definir os assuntos que, efetivamente, sensibilizam o executivo, fazendo-o não só compreender os de-

safios ligados à segurança, mas também sua importância para o desenvolvimento de seu negócio, bem como envolvê-lo de tal forma, que se sinta co-responsável pela superação do desafio e sucesso da iniciativa.

Alinhados os objetivos, é preciso tocar nos pontos que o sensibilizem, nos assuntos que convirjam e estejam em sintonia com suas expectativas e seus maiores interesses. É como se adaptássemos a linguagem, ora técnica, ora gerencial, para outra, contextualizada, que tornasse tangíveis os resultados de curto, médio e longo prazos da solução de segurança. Estou falando de números. Nada melhor do que a linguagem dos números e dos gráficos para se fazer entender na restrita janela de tempo que o executivo nos concederá.

Use a projeção de slides para conduzir a explanação, mas com moderação, sem sobrecarregar em quantidade e evitando poluí-los com informação desnecessária. Procure passar mensagens claras e consistentes. Compare o cenário atual com o cenário projetado, resultante da solução de segurança proposta. Organize seus maiores desafios e os associe com os benefícios diretos e indiretos da segurança. Projete uma análise de ROI – Retorno sobre o Investimento, mesmo que tenha abrangência limitada a ambientes específicos, mas não peque pela inconsistência. Reúna informações reais e representativas que demonstrem o valor agregado pela iniciativa. Identifique – como propõe a lista a seguir – os motivos que levariam o executivo a agir voluntariamente, e o conduza à postura desejada (última da lista).

Principais motivos que levariam os executivos a agirem voluntariamente:

- Modismo (ação pontual motivada pela opinião pública).
- Normativo (ação pontual motivada por regras e regulamentos externos).
- Ameaça da concorrência (ação pontual motivada por espionagem industrial etc).
- Medo (ação pontual motivada pela percepção opaca e parcial dos riscos).
- Desastre (ação pontual reativa motivada por fatos consumados).
- Visão ampla dos desafios e percepção do valor agregado ao negócio (ação integrada motivada pelo entendimento dos benefícios da solução corporativa).

Importante considerar que não estaremos diante de pessoas com comportamentos e perfis padronizados, previsíveis. O ser humano é uma máquina completa, não binária e, por isso, quanto mais informação sobre sua personalidade, sua linha de atuação na empresa e seus valores, maior será a eficiência da abordagem. Contudo, independente de seu perfil, praticamente todos os executivos que estão na diretoria da empresa têm estes assuntos em sua agenda de prioridades e objetivos:

- Valorizar as ações da empresa.
- Viabilizar novos negócios.
- Viabilizar a exploração de novos mercados.
- Bônus e opção de ações.
- Gerar novos produtos e serviços.
- Ser pioneiro.
- Combater a concorrência.
- Aumentar a receita.
- Aumentar a lucratividade.
- Aumentar a produtividade.
- Reduzir o *time-to-market*.
- Reduzir os custos diretos e indiretos.
- Reduzir os riscos.
- Gerir a relação com investidores.
- Dar visibilidade aos resultados.
- Fortalecer a imagem e o posicionamento da empresa no mercado.

Se tivesse a tarefa de sintetizar em uma linha, mesclando todos os tópicos apontados anteriormente como importantes, não hesitaria em afirmar que o grande alvo do executivo é o LLE – Lucro Líquido dos Exercícios. Assim, associe sempre as ações de segurança aos reflexos positivos que poderá causar na última linha do balanço, pois ele tem peso dobrado na tomada de decisão.

Entretanto, apesar de tantos tópicos e pontos de controle, comumente não se obtém muito tempo do executivo para abordar o assun-

to; por isso, tenha em mente os fatores críticos de sucesso: agir com objetividade, definir claramente os impactos proporcionados pela falta de segurança revelando o cenário atual, definir claramente os benefícios da proposta de segurança revelando o cenário projetado e definir os montante de investimentos associado.

Podem parecer tarefas fáceis depois de tudo isso, mas o principal gargalo continua sendo o levantamento de informações reais que mensurem os custos e projetem situações de risco que comprometam a operação e gerem impactos substanciais ao negócio. Em função disso, tem sido constante a execução de um levantamento de segurança superficial de abrangência restrita através de um Teste de Invasão, capaz de capturar uma “fotografia” do ambiente em um determinado período. De posse desses resultados – que comumente são positivos pela concretização da invasão – se ganha poder de persuasão e convencimento, aumentando a eficiência da abordagem e as chances de conquista da atenção e do comprometimento do alto executivo.

Agora é tomar a iniciativa e se preparar para o dia D.

4.8 Sabendo identificar o parceiro externo

Considerando o dinamismo e complexidade dos ambientes, a heterogeneidade de tecnologias e a diversidade de ameaças, vulnerabilidades e riscos, convém repensar sobre o custo x benefício de assumir sozinho a responsabilidade pela gestão da segurança.

O primeiro aspecto a ser analisado está associado ao investimento que se fará necessário para equipar tecnicamente, formar e manter constantemente capacitada uma grande equipe de multiespecialistas capazes de suprir todos os atuais e novos desafios de segurança que surgirem. Além disso, não podemos desprezar o fato desses investimentos não estarem diretamente ligados ao *core business* da empresa, fazendo com que se consuma recursos físicos, humanos e financeiros desassociados à atividade-fim da empresa, o que o torna desinteressante e, muitas vezes, injustificável.

Diante disso, surge um novo e difícil desafio para o *Security Officer* atrelado à busca de empresas capazes de oferecer o apoio externo complementar, atuando como uma verdadeira e onipresente retaguarda de segurança.

Características desejadas na Consultoria externa:

- Posicionamento e perfil de Consultoria e Integradora de Ferramentas.
- Notória especialização em Segurança da Informação.
- Especificidade em Segurança da Informação.
- Equipe técnica multiespecialista.
- Ação local com visão global.
- Estrutura de execução de projetos capaz de viabilizar ações simultâneas em paralelo.
- Metodologia para dimensionamento de solução que considere fundamentalmente as características e desafios de negócio.
- Metodologia específica para execução de projetos de segurança da informação.
- Metodologias em conformidade com as normas internacionais BS7799 e ISO17799.
- Presença geográfica proporcional ou capaz de atender às características da empresa.
- Ponto de presença no exterior, viabilizando a absorção de experiências, inovações e tendências, e facilitação de parcerias e contatos técnicos.
- Comprovada experiência em projetos corporativos complexos.

Tantas virtudes juntas tornam a identificação do parceiro uma árdua tarefa, principalmente por existirem escassas opções no mercado capazes de suportar grandes projetos e, ainda, que tenham em seu curriculum a competência de orientar suas ações ao apurado entendimento do segmento de mercado e das diretrizes estratégicas do negócio de forma integrada, através do comportamento consultivo. O alvo da busca deve ser um parceiro com experiência e em condições de atuar como maestro de uma orquestra, em que os metais – formado por especialistas seniores em cada tipo de instrumento de sopro – pertençam à própria equipe do maestro. Em que os percussionistas – também da equipe do maestro – usem com harmonia os melhores instrumentos disponíveis no merca-

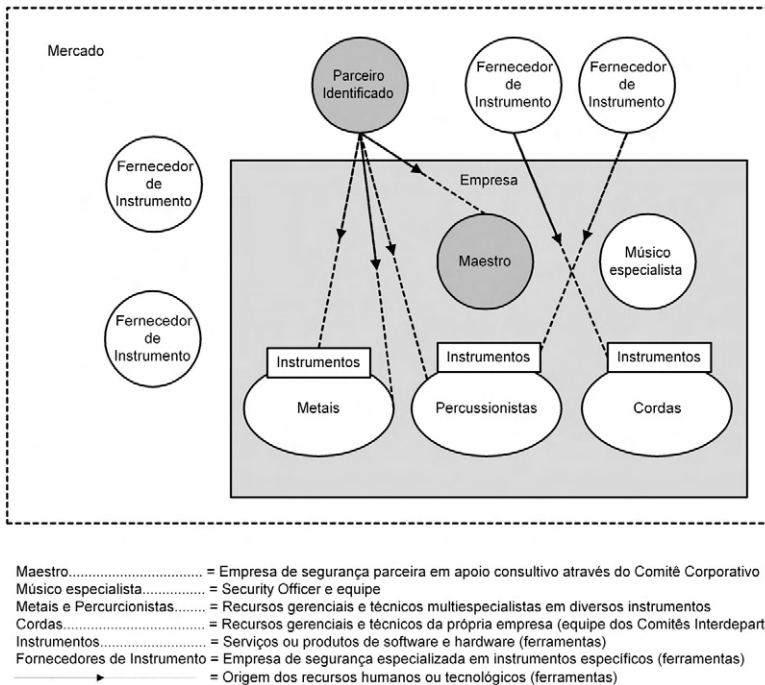


Figura 4-12 Relação de parceria e retaguarda de segurança.

do fornecidos por diversos fabricantes, e, por último, as cordas, executadas pelos instrumentistas da própria empresa, orientados por um músico especialista que receba assessoria do maestro.

É natural e coerente, em determinado momento, avaliar os novos riscos inerentes à terceirização de parte ou de todas as ações de segurança da informação, considerando a acessibilidade de ativos físicos e tecnológicos, informações críticas para a empresa e o conseqüente aumento da exposição. Porém, aprofundando um pouco mais a avaliação, chegaremos logo à conclusão de que se trata de um risco compensador e controlado – se a seleção do parceiro foi apropriadamente criteriosa – capaz de interferir positivamente no resultado da relação custo x benefício.

4.9 Conformidade com Norma específica

Como puderam notar, são muitas as variáveis envolvidas com o desafio corporativo da segurança; e elas tendem a crescer à medida que vão surgindo novas tecnologias, novos modelos de negócio e inovações no relacionamento comercial.

Motivados por isso, a comunidade britânica, liderada pela Inglaterra, criou a Norma BS7799, que reúne as melhores práticas para o gerenciamento de segurança da informação, através do BSI – *British Standard Institution*. À medida que os reflexos da falta de segurança no mundo começaram a ser veiculados e a ganhar visibilidade, diversos países da comunidade britânica, como a Austrália, África do Sul e Nova Zelândia, passaram a adotar a norma.

Considerado o mais completo padrão, esta norma britânica ganhou visibilidade mundial. Como de costume, apesar da reatividade na primeira tentativa de homologação, a ISO – *International Standardization Organization* seguiu seus passos e, sem “reinventar a roda”, buscou analisá-la, a fim de construir a sua versão da norma para tratar do assunto, chamada ISO 17799:2000.

O processo não demorou muito e logo a ABNT – Associação Brasileira de Normas Técnicas, operando em sintonia com a ISO a partir da norma ISO 17799:2000, disponibilizou o projeto na versão brasileira para consulta pública. Neste período, alguns comitês de estudos foram criados no país, com importantes representantes dos setores público e privado, que puderam tecer comentários e sugerir adaptações às necessidades do mercado brasileiro.

Sabe-se, no entanto, que a norma BS7799 parte 1, bem com as normas “filhotes”, não tem as mesmas características de uma típica norma de certificação, mas sugere, através de um modelo menos formal, a preocupação com aspectos importantes e a utilização de controles que orientem as empresas a reduzir seus riscos operacionais que, potencialmente, causariam impactos nos negócios. Reúne, como em um código de conduta, os tópicos que devem ser analisados, as melhores práticas e, didaticamente falando, aponta “O QUE” fazer, sem se preocupar com os detalhes associados ao “COMO” fazer.

Dessa forma, igualmente motivado, nosso país ganha a norma brasileira NBR ISO/IEC17799-1 pelas mãos da ABNT, que, após pequenos ajustes sugeridos pelos comitês em consulta pública, deram vida à primeira norma brasileira do gênero.

Assim como no Brasil, muitos outros países começaram a se preocupar com o tema e iniciaram seus estudos em busca de experiências que pudessem norteá-los na criação de suas próprias normas locais.

O objetivo principal da norma é orientar e, a partir disso, criar uma sinergia entre as empresas que estão diante do desafio do gerenciamento da segurança da informação. Desta forma, será possível buscar

uma “base comum” para desenvolvimento de normas que as fortaleça e as torne compatíveis sob o aspecto de segurança, agregando valor ao processo mercadológico através da redução dos riscos de todos os elementos da cadeia produtiva, provendo confiança nos relacionamentos entre as organizações.

Todas as versões da norma, inclusive a brasileira, que poucas alterações incorporou, tratam de aspectos bem abrangentes, mas girando sempre no eixo dos principais conceitos de segurança: confidencialidade, integridade e disponibilidade.

Abrangente, apesar da superficialidade de suas recomendações, a norma passa a representar um importante instrumento sinalizador da direção para as empresa preocupadas com a operação de seu negócio e a proteção das informações que o sustenta.

Possui 36 grupos de controles que explodem em um total de 127 controles sugeridos e, certamente, poderá – apesar de não ser nativamente uma norma orientada à certificação – ser adotada para indicar a conformidade de empresas e sua preocupação com as informações que subsidiam as relações comerciais entre parceiros, fornecedores e clientes. Deve ser encarada, portanto, como um código de conduta, onde se recomendam posturas sobre a gestão de segurança da informação.

Nota Importante

*BS7799:Parte 1 gerou a ISO/IEC17799:2000 – Código de Conduta
BS7799:Parte 2 em estudo – Requisitos para Information
Security Management System*

“Esta Norma pode ser considerada como o ponto de partida para o desenvolvimento de recomendações específicas para a organização. Nem todas as recomendações e os controles desta Norma podem ou devem ser integralmente aplicados. Além disso, controles adicionais não incluídos nesta Norma podem ser necessários e complementares. Quando isso acontecer pode ser útil manter uma referência cruzada para facilitar a verificação da conformidade por auditores e parceiros de negócio”.

Conforme o texto acima transcrito da norma, pode-se notar a preocupação em desvincular a norma do sentido figurado de um TRILHO, atribuindo à mesma o papel figurado de uma TRILHA, capaz de apontar a direção sem, no entanto, gerar obrigatoriedade e padronização in-

flexível que, certamente, não seria compatível com o dinamismo das empresas, seus ambientes e as mudanças em seus ativos físicos, tecnológicos e humanos.

Tendência

Assim como ocorreu com a norma de qualidade ISO9000, que gradativamente foi ganhando a confiança e a credibilidade das empresas em todos os segmentos e ramos de atividade, teremos seguramente um novo movimento no meio corporativo em busca de sintonia, conformidade e, conseqüentemente, certificação com base na norma de segurança da informação.

À medida que os primeiros e importantes *players* do mercado iniciarem o movimento, logo veremos os demais serem abalroados pela positiva febre de adequação e conformidade. A preocupação com a segurança da informação transcenderá o aspecto tecnológico e os limites físicos e lógicos da empresa, indo buscar – e, posteriormente, cobrar – a mesma sintonia e conformidade com os demais parceiros da cadeia produtiva.

Diante deste exercício de projeção, que poderíamos chamar de exercício premonitório, não deixe que sua empresa seja a última a se mexer. Seja pioneiro e extraia desta – que deverá ser uma das principais reestruturações das empresas neste século – os benefícios atrelados à inovação que poderá representar um importante e poderoso diferencial competitivo para o seu negócio.

4.10 Norma versus Metodologia

O fato de já existirem normas nacionais e internacionais – apesar de estarem em estágio de absorção e amadurecimento – que rezem sobre o código de conduta para o gerenciamento da segurança da informação, não soluciona por completo o desafio que as empresas enfrentam. Isso acontece porque a norma tem o nítido papel de apenas apontar os aspectos que merecem atenção, indicando O QUE fazer para o adequado gerenciamento, sem, no entanto, indicar com precisão metodológica COMO se deve realizar as atividades.

É o mesmo que sermos instruídos a realizar com periodicidade anual um *check-up* de nosso estado de saúde, considerando os sistemas respiratório, circulatório, digestivo etc., sem que soubéssemos exatamente como fazê-lo, senão procurar um especialista. Este, por sua vez,

que detém especificidade, irá aplicar toda a sua base de conhecimento seguindo, com riqueza de detalhes e precisão inerente à atividade, uma metodologia própria. Um grande “manual” que lhes permitirá considerar todos os pontos importantes para análise e lhes apontará as ferramentas mais apropriadas para cada tipo de exame.

É, na verdade, um desdobramento com procedimentos baseados em uma norma maior, como a ISO, que apontará a forma com que os exames, ou melhor, as atividades devem ocorrer, como os instrumentos devem ser manipulados e, ainda, como os resultados devem ser interpretados para uma consistente interpretação do estado de saúde e posterior sugestão de tratamento e medicamento.

Portanto, de nada adiantará estar ciente dos controles e aspectos apontados por uma norma de segurança, se você não dispuser de uma metodologia condizente e consistente, capaz de orientar as atividades, transformando-as em resultados reais ligados à redução dos riscos.

No tempo em que as empresas viviam um grau de exposição baixo (em função da baixa informatização, conectividade e compartilhamento) e a percepção de segurança não transcendia os aspectos físicos, a necessidade de uma metodologia era pouco percebida. Contudo, à medida que os riscos, ameaças e impactos foram se tornando mais presentes e representativos, e houve uma percepção mais apurada e correta de que a segurança não se limita à tecnologia, mas considera, também, os aspectos físicos e humanos, o volume de problemas e as vulnerabilidades cresceram exponencialmente. Os levantamentos e implementações passaram, então, a ser mais profundas, apuradas e, conseqüentemente, o aumento proporcional da massa crítica resultante tornou o processo de análise e gestão ainda mais complexo. Diante disso, adotar uma metodologia passou a ser fator crítico de sucesso para subsidiar o cada vez mais complexo plano de ação, ou melhor, o Plano Diretor de Segurança.

Exemplos de ferramentas metodológicas

- Formulário para mapeamento de vulnerabilidades
- Formulário para mapeamento de processos de negócio críticos
- Formulário para orientação na condução de entrevistas
- Planilha para identificação de ativos físicos, tecnológicos e humanos

- Planilha para estudo de sensibilidades à quebra de segurança
- Instrumento para mapeamento topológico
- Matriz de criticidade para priorização das ações
- Matriz de Tolerância à paralisação

Diferente da norma que se propõe a orientar todos no sentido de construir uma base comum de conduta, não haverá uma única e recomendada metodologia. Surgirão muitas delas simultaneamente pelas mãos de muitas empresas em diversos países, mas todas deverão estar alinhadas às diretrizes da norma sem deixar de serem adaptadas e contextualizadas a cada mercado, considerando a cultura local e as variáveis internas e externas que interferem na empresa.

É tendencioso que, depois de aplicadas sucessivamente, exercitadas e constantemente adaptadas ao longo do tempo, uma delas ganhe maior visibilidade e destaque, podendo, então, ser uma referência – mesmo que local - que inspire as empresas a adotá-la como um padrão.

Knowledge Checkpoint 2

Este ponto de checagem de conhecimento é uma breve e objetiva consolidação dos conceitos abordados em cada seção do livro com o objetivo de reforçar o processo de absorção do conteúdo relevante.

Conceitos de Segurança

CONCEITO: “Conceitos sólidos e seu claro entendimento são a matéria-prima que implicará na qualidade e no resultado dos trabalhos”.

Teoria do Perímetro

CONCEITO: “Saber segmentar os ativos físicos, tecnológicos e humanos de acordo com a similaridade de sua criticidade e importância (valor para o negócio) é a base para a especificação e aplicação dos controles certos que oferecerão o nível de proteção adequado a cada perfil e necessidade”.

Barreiras da Segurança

CONCEITO: “Conhecer as barreiras da proteção e buscar sinergia entre elas não é suficiente sem um diagnóstico capaz de associar ativos e processos de negócio, transcendendo o mapeamento de falhas tecnológicas e identificando os riscos da empresa pela análise do trinômio: pessoas, tecnologia e processos.”

Equação do Risco

CONCEITO: “Cada empresa terá a sua equação de risco personalizada. Um verdadeiro painel de controle que sinalizará situações de risco controlado, situações de risco flutuante e, ainda, situações de risco intolerante”.

Comitê Corporativo de Segurança da Informação

CONCEITO: “Espinha dorsal, o Comitê Corporativo deve ser consistente, dinâmico e flexível para representar oficialmente os interesses da empresa perante os desafios do negócio”.

Papel do Security Officer

CONCEITO: “Explicita as responsabilidades do *Security Officer* para com o resultado; mas municie-o adequadamente para viabilizar sua atividade”.

Como conduzir internamente a negociação

CONCEITO: “Conquistar o comprometimento da diretoria da empresa é condição *sine qua non* para obter o dimensionamento apropriado dos recursos financeiros que irão subsidiar a estrutura mantenedora do Modelo de Gestão Corporativa de Segurança da Informação; por isso, seja convincentemente consistente para fazê-la perceber a segurança como investimento, e não como despesa”.

Sabendo identificar o parceiro externo

CONCEITO: “A escolha do parceiro que cumprirá o papel de retaguarda de segurança irá definir o sucesso ou o insucesso da iniciativa; por isso, reúna informações particulares sobre o candidato que ratifiquem sua notória especialização, sua experiência e, principalmente, seu comprometimento com os resultados corporativos finais e alinhado às diretrizes estratégicas do negócio. Afinal, ninguém procura qualquer médico quando tem de operar o coração”.

Conformidade com Norma específica

CONCEITO: “Ao se estruturar para gerir a segurança da informação a partir de um modelo dinâmico e flexível, é fundamental acompanhar os movimentos do mercado local, de seus parceiros na cadeia produtiva e, também, os movimentos internacionais. Procure estar em siner-

gia com os conceitos e iniciativas de normalização nacionais e internacionais, a fim de lhe proporcionar o melhor retorno sobre o investimento e, ainda, lhe permitir usufruir da posição de destaque ímpar”.

Norma × Metodologia

CONCEITO: “Orientado pela norma de segurança, não inicie as atividades sem que sejam baseadas em uma metodologia condizente, mesmo que – em hipótese – você tenha que desenvolvê-la, ou tenha de identificar no mercado alguma que esteja sendo bem-sucedida, ou tenha de verificar se seu parceiro externo dispõe de uma metodologia consistente com histórico positivo”.

Orientação ao *Security Officer*

Depois de termos depurado, nos capítulos anteriores, os aspectos mais relevantes para conduzir as empresas, ajudando-as a atingir o sucesso e a superar os desafios de gerir a segurança da informação, chega o momento de explodirmos alguns assuntos mais práticos, orientando o executivo responsável por toda a coordenação do processo: o *Security Officer*.

6.1 Solução Corporativa de Segurança da Informação

Talvez ainda haja dúvidas quanto à expressão – e não é para menos – afinal, muitas peças do quebra-cabeça foram identificadas até esta etapa do livro, mas ainda não as reunimos para formar uma imagem única. Chegou a hora de fazê-lo.

Devemos chamar de Solução Corporativa de Segurança da Informação o resultado da criação de uma estrutura corporativa adequadamente posicionada no organograma, chamada Comitê Corporativo de Segurança da Informação, baseado em um modelo de gestão dinâmico, com autonomia e abrangência, coordenado por um executivo em ação focada, intitulado *Security Officer*. Este, apoiado por equipe própria ou terceirizada na esfera tático-operacional, e por representantes de departamentos ou gestores dos processos críticos em esfera executiva, todos orientados por um Plano Diretor de Segurança desenvolvido sob medida e alinhado às diretrizes estratégicas do negócio, que irá organizar as atividades em busca da adoção de controles que conduzam os

riscos ao patamar operacional definido como ideal. Desta forma, estará viabilizando o melhor retorno sobre o investimento, refletindo, conseqüentemente, em maior valor agregado para o negócio, onde se lê: maior lucro líquido do exercício.

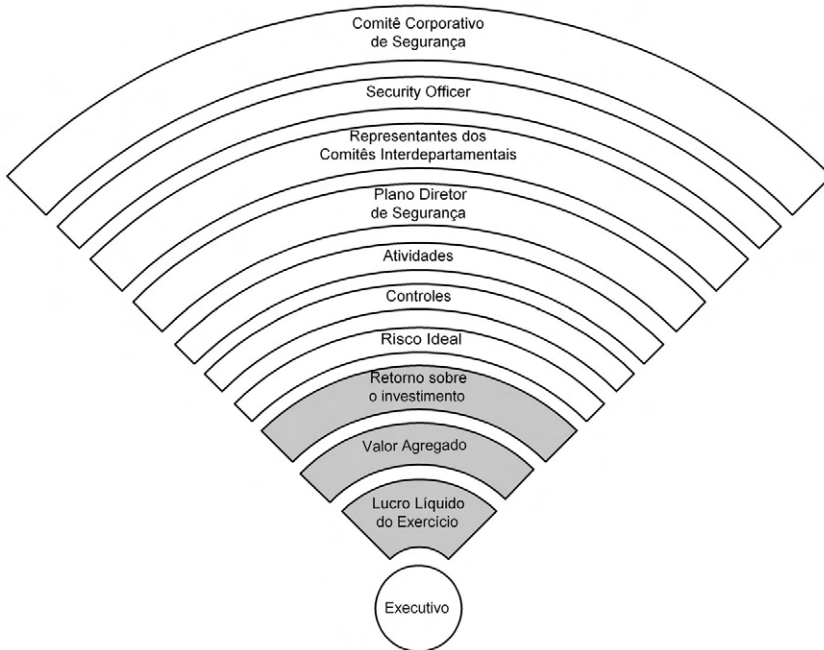


Figura 6-1 *Visão em cascata da Solução Corporativa de Segurança da Informação e seus resultados tangíveis.*

Talvez algumas palavras nos ajudem a compreender tamanha complexidade, e se tivesse de escolher uma para representar o macro-desafio da solução de segurança – capaz de sinalizar todos os aspectos associados – seria: **CONTROLE**.

Pronto. Controle é tudo o que se quer – sob a ótica da aplicação –, efetivamente, para administrar as vulnerabilidades e reduzir os riscos. É com controle que será possível, por exemplo: autorizar ou bloquear pessoas que tentarem entrar em ambientes físicos restritos; registrar as tentativas de acesso ao site Internet; mensurar o prejuízo causado por ocorrências de quebra de segurança; inibir tentativas de ataque ao roteador; evitar o descarte de material crítico impresso sem cuidados adequados; sinalizar a queda de produtividade dos funcionários; apontar as melhores práticas para transportar informações em meio

magnético; impedir tentativas de sabotagem e fraude; realizar e medir a eficiência de treinamentos de conscientização e capacitação de técnicos e usuários da rede corporativa; e reagir com velocidade e eficiência em situações de crise e quebra de segurança previsíveis e, muitas vezes, inevitáveis etc.

Muitos erroneamente teriam escolhido a palavra BLOQUEIO ou PROIBIÇÃO, mas, na verdade, o principal objetivo de uma solução de segurança corporativa está na especificação e aplicação de mecanismos de controle que conduzam os riscos ao patamar predefinido como ideal para a empresa (e este varia de empresa para empresa), a fim de evitar e minimizar impactos no negócio em tempo de manuseio, armazenamento, transporte e descarte de informações.

Outra palavra que poderá nos ajudar, e é igualmente importante para a segurança, é SEGMENTAÇÃO. Considerando as particularidades que diferenciam uma empresa de outra e, ainda, considerando que uma única empresa dispõe de informações com importâncias e valores distintos, fluindo por diversos ambientes e sustentando processos de negócio, chegamos à conclusão de que os perímetros físicos, tecnológicos e humanos desta empresa necessitarão de níveis de segurança diferentes, sempre procurando identificar e aplicar a “dose” ideal. Desta forma, sabendo segmentar inteligentemente a empresa e reunir as peças, digo, as atividades que irão compor a solu-

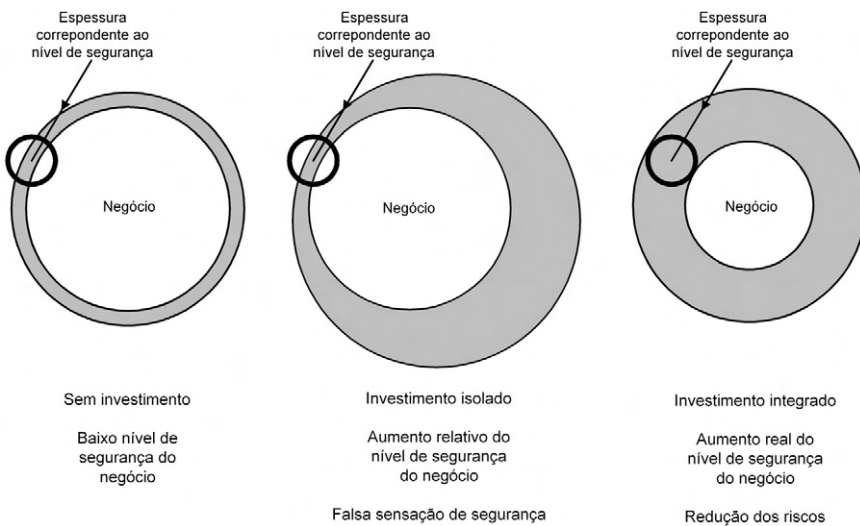


Figura 6-2 Visão figurada dos estágios e do principal objetivo da solução corporativa de segurança da informação.

ção, estaremos viabilizando a efetiva redução de riscos e o real aumento da segurança do negócio, sem depreciar seus processos comerciais, produtivos etc., com burocracia demasiada, perda de agilidade e competitividade. (Consulte a Figura 6-2.)

Objetivo

A solução pode ser muito bem percebida – sob a ótica da aplicação – como um grande jogo de peças de montar que se encaixam suavemente, se bem moldadas e orientadas pelo “gabarito” personalizado do Plano Diretor de Segurança. Reunidas, formarão um mosaico, uma estrutura sólida, porém flexível e dinâmica, que dará sustentação para a empresa construir um modelo de gestão contextualizado para superar os atuais e reagir adequadamente aos futuros desafios associados ao controle do risco de segurança da informação.

As peças são atividades ou projetos com os mais diversificados propósitos e de naturezas distintas. Seguindo o modelo de organização proposto pela Norma BS7799 parte dois, que fora inspirada originalmente no modelo PDCA adotado na ISO 9001, e que tem sinergia com os estudos conceituais da segurança, temos as seguintes fases:

- PLAN (planejamento)
- DO (implementação)
- CHECK (analisar)
- ACT (monitorar)

É importante notar que estas quatro fases são aplicáveis na organização de todas as atividades que fazem parte da solução de segurança, bem como devem orientar as subatividades. (Consulte a Figura 6-3.)

Em um exercício, podemos dizer que é necessário Planejar as ações executivas (Plano Diretor de Segurança) para realizar investimentos adequados e organizar o *Security Office*. Da mesma forma, é preciso Analisar os fatores de risco do negócio que apontarão as características e levantarão informações para apoiar o dimensionamento das ações. Implementar os controles físicos, tecnológicos e humanos é a próxima etapa, seguida da fase Monitoramento, que fará a ligação com a primeira, subsidiando-a com informações de novas falhas, ameaças e riscos. (Consulte a Figura 6-4.)

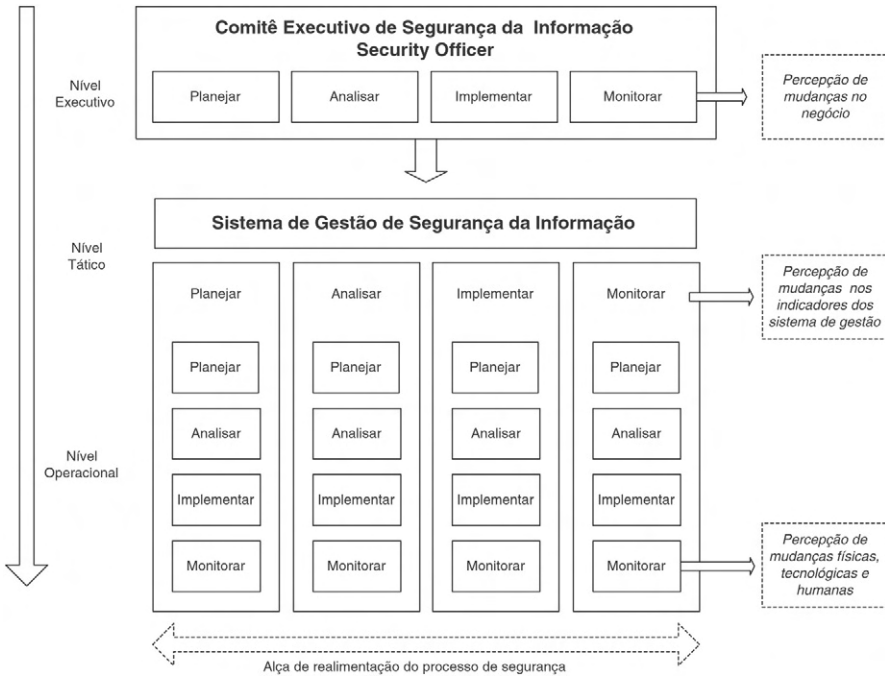


Figura 6-3 Visão da aplicabilidade do modelo PDCA nos diversos níveis.

Descendo mais um nível, o das atividades que compõem cada uma das quatro fases, veremos, mais uma vez, a aplicabilidade do mesmo modelo. Recorrendo novamente ao exercício, podemos Planejar o escopo e as subatividades executadas em uma análise de riscos. Analisar os resultados obtidos durante as entrevistas, análises físicas e análises técnicas. Implementar as medidas emergenciais e, por fim, Monitorar os índices e indicadores que poderão alterar o nível de risco do escopo da análise.

Fases

Planejar (Plan)

Compreende atividades que objetivam definir arquiteturas, ações, atividades, alternativas de continuidade e critérios, abrangendo todo o ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, aplicáveis desde os níveis mais estratégicos aos operacionais, que servirão de orientador.

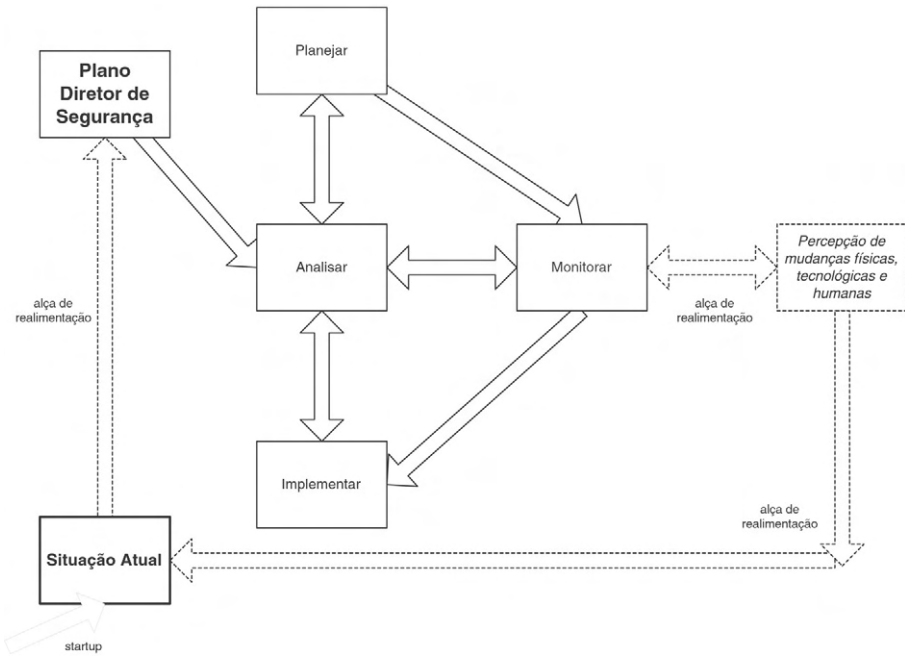


Figura 6-4 Macrofluxo das atividades.

- Plano Diretor de Segurança
- Plano de Continuidade de Negócios
- Política de Segurança da Informação

Analisar (Check)

Compreende atividades que buscam gerar um diagnóstico de segurança, através do mapeamento e da identificação de particularidades físicas, tecnológicas e humanas da empresa como um todo ou de perímetros menores, vulnerabilidades, ameaças, riscos e impactos potenciais que poderão se refletir no negócio.

- Análise de Riscos
- Teste de Invasão

Implementar (Do)

Compreende atividades que aplicam mecanismos de controle nos ativos físicos, tecnológicos e humanos, que possuem vulnerabilidades, buscando eliminá-las – quando possível e viável – ou administrá-las, a fim de aumentar o nível de segurança do negócio. É a fase que materializa as ações tidas como necessárias no diagnóstico e organizadas pelo planejamento.

- Implementação de Controles de Segurança
- Treinamento e Sensibilização em Segurança

Monitorar (Act)

Compreende atividades que visam gerir o nível de segurança, através de dispositivos que monitoram índices e indicadores, canalizando novas percepções de mudança física, tecnológica e humana que provocam oscilação do grau de risco, a fim de adequar as ações de segurança ao contexto. É a fase que representa o elo de ligação com as demais, formando um ciclo contínuo, dando vida ao verdadeiro processo de gestão dinâmica.

- Equipe para Resposta a Incidentes
- Administração e Monitoração de Segurança

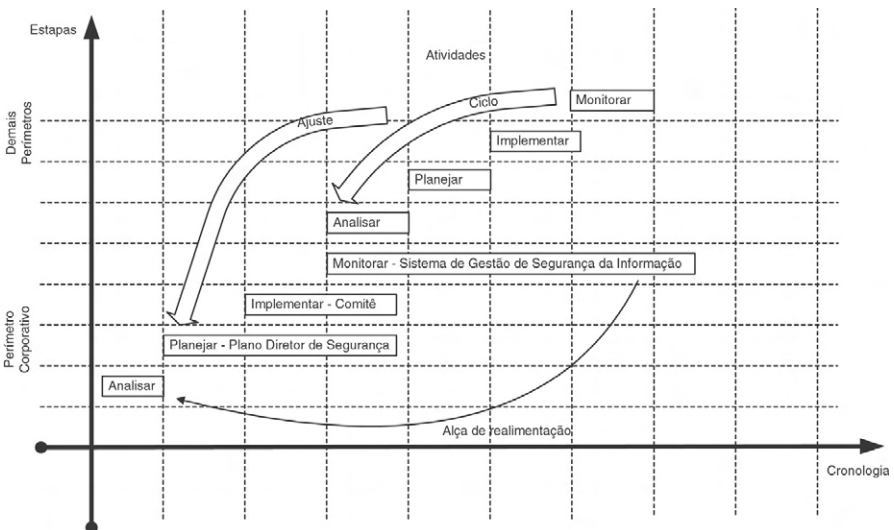


Figura 6-5 Exemplo de encadeamento das atividades.

Por conta da própria natureza das atividades, existe uma seqüência natural de execução fazendo seus produtos finais se integrarem uns aos outros, alimentando a próxima atividade e ligando a última etapa à primeira, de forma a estabelecer um ciclo contínuo de manutenção do risco. Podemos ver no diagrama do exemplo o momento em que as necessidades e as características corporativas foram analisadas, gerando um Plano Diretor de Segurança, que, por sua vez, fora suportado pela implementação de um Comitê de Segurança/*Security Office*. Em seguida, estabeleceu-se um conjunto de critérios, índices, indicadores e métricas para monitoração que fomentaram a criação do Sistema de Gestão de Segurança da Informação.

Pelo papel fundamental exercido pelo Plano Diretor de Segurança, o exploraremos, com riqueza de detalhes, no próximo capítulo.

Em tempo, é importante notar que as atividades de caráter executivo, ou de abrangência corporativa, servirão de norte para todas as demais atividades que irão ocorrer nos outros perímetros da empresa. Esta sinergia permite a integração dos trabalhos, evita redundâncias, desproporcionalidades de investimento e, principalmente, permite que se implemente o conceito de *Building blocs*. Desta forma, a empresa poderá desmembrar as ações de segurança em partes integráveis que, aos poucos, vão construindo um modelo de gestão de abrangência corporativa.

Este movimento está intimamente ligado e em sintonia com o modelo de gestão proposto pela norma internacional BS7799: ISMS – *Information Security Management System*, ou Sistema de Gestão de Segurança da Informação.

6.2 Plano Diretor de Segurança

Planejamento é o fator crítico de sucesso para a iniciativa de gerir a segurança da informação e o Plano Diretor de Segurança é justamente o elemento específico para este fim. Mais do que uma rubrica orçamentária destinada a investimentos tecnológicos, como sugere o já tradicional Plano Diretor de Informática, o PDS tem de ser dinâmico e flexível para suportar as novas necessidades de segurança que surgem em virtude da velocidade como o contexto corporativo muda.

Didaticamente falando, o Plano Diretor de Segurança representa a bússola que irá apontar o caminho e os passos (atividades) que irão formar o mosaico da solução e suprir as necessidades de segurança do

negócio, conduzindo-o a operar sob risco controlado. É importante perceber que esta bússola deve ser especificada sob medida para cada empresa. Não há um modelo de plano que seja capaz de atender a todo tipo de empresa, por mais que sejam empresas do mesmo porte e do mesmo segmento de mercado. Existem particularidades intrínsecas, como ameaças, riscos, sensibilidades, impactos e vulnerabilidades físicas, tecnológicos e humanas que tornam o problema único. Portanto, seguindo a analogia com a medicina, este paciente terá de ser atendido por um receituário medicamentoso único e personalizado, capaz de sanar e estancar a enfermidade também única. Estamos diante, então, do primeiro passo, do primeiro desafio do *Security Officer*: como dimensionar um Plano Diretor de Segurança?

Metodologia

O início da modelagem do PDS está diretamente associado a ações de levantamento de informações do negócio, similar a uma consulta médica, onde, além da anamnese inicial, são realizados exames e testes superficiais para diagnosticar os sintomas, as anormalidades e os riscos potenciais do paciente, ou seja, identificar ameaças, vulnerabilidades, riscos e impactos potenciais ao negócio.

É fundamental entender os desafios do negócio, conhecer os planos de curto, médio e longo prazos, e as demandas que estarão por vir em função do *Business Plan*. Por mais que as ações de segurança não incidam diretamente nos processos do negócio, todas elas terão de ser orientadas por eles; portanto, objetiva-se, nesta fase preliminar do levantamento, montar um mapa de relacionamento e dependência entre Processos de Negócio, Aplicações e Infra-estrutura Física, Tecnológica e Humana. (Consulte a Figura 6-6.)

Trata-se de uma tarefa de natureza complexa, principalmente quando se trata de uma empresa de grande porte, pois dificilmente se encontrará um grupo acessível, pequeno e coeso capaz de ter uma visão corporativa ampla e completa. Além disso, a complexidade dos ambientes, a heterogeneidade de tecnologias, os múltiplos acessos híbridos, a descentralização geográfica e a previsível distribuição de responsabilidades de segurança pelos departamentos tornam-se fatores dificultadores; por isso, considere-os.

Desta forma, a metodologia compreende 6 etapas distintas que se complementam, fomentando uma visão consolidada do negócio que subsidiará a modelagem de um Plano Diretor de Segurança personalizado.

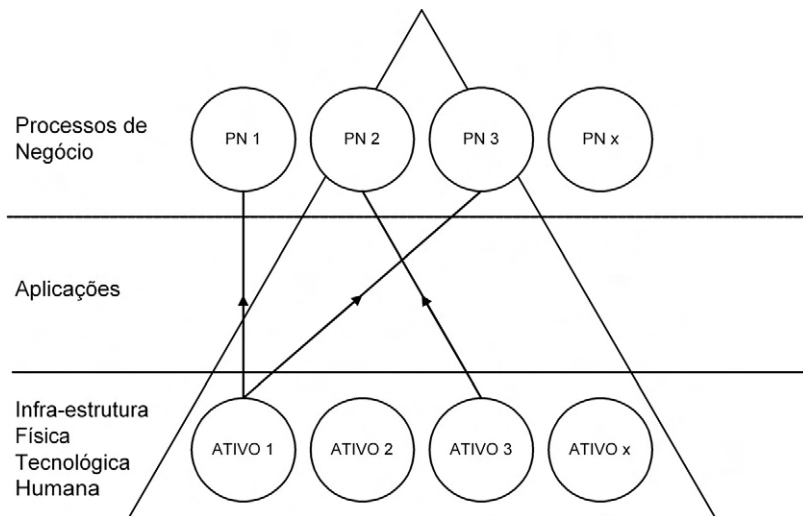


Figura 6-6 Mapa de relacionamento entre processos de negócio e infra-estrutura.

1. Identificação dos Processos de Negócio

Reunindo os principais gestores com representatividade na empresa, previamente identificados comumente na esfera executivo-gerencial, iniciam-se os trabalhos objetivando identificar – através de entrevistas e *brainstorm* – os processos de negócio críticos que serão alvo das atividades que irão compor a solução. Partindo da premissa de que as ações de segurança devem ter o foco no negócio e nas informações que o sustentam, é imprescindível elencar os processos mais sensíveis. É como se perguntássemos ao paciente quais dores está sentindo e a localização delas. Além disso, busca-se identificar as necessidades físicas, tecnológicas, humanas e de conectividade desses processos para o funcionamento de todo o negócio.

Mais uma vez abusando de analogias com objetivo didático, lanço mão da comparação da empresa com um motor de automóvel. Pense em motores distintos, representando empresas distintas. Desta forma, esta etapa preliminar de levantamento ganha o objetivo inicial de identificar as peças mais críticas e representativas para garantir a performance e funcionamento do motor, digo, do negócio.

Lembre-se de que, durante esta etapa, é costumeiro orientar a identificação dos processos críticos com base em seus resultados financeiros e estratégicos resultantes; dessa forma, torna-se importante envolver representantes da empresa que possam compartilhar informações sobre eles, que transcendam os aspectos operacionais.

	Clientes Atendidos	Receita	Margem	Fator Estratégico	Conformidade de Legal
PN 1	N				
PN 2		\$			
PN 3			%		
PN x				Peso	\$ Multa

Figura 6-7 Exemplos de unidades de medida considerados para identificar processos de negócio críticos.

O grande segredo associado a este mapeamento inicial está na percepção da melhor divisão do negócio – que chamamos aqui de processos de negócio – de forma que possam representar perímetros (físicos, tecnológicos e humanos) com características e funções explicitamente específicas, que justifiquem ações sob medida. Seria o mesmo que, sem conhecer a anatomia humana, tivéssemos que identificar os órgãos que estão envolvidos na operacionalização das funções circulatória, respiratória, digestiva etc., para que pudessem ser agrupados a fim de receber um tratamento específico e uniforme.

Resultado esperado desta etapa:

- Mapeamento dos Processos de Negócio críticos para a operação da empresa.
- Identificação dos gestores chaves dos processos mapeados.
- Início da integração e comprometimento dos gestores chaves envolvidos.
- Início do entendimento sobre o funcionamento do negócio.

2. Mapeamento da Relevância

Conhecendo melhor o funcionamento do negócio, depois de tê-lo desmembrado coerentemente a partir da identificação dos processos críticos, chega o momento de mapear a relevância de cada um deles, a

fim de evitar discrepâncias na priorização das atividades que compõem a solução.

Voltando à analogia didática do corpo humano, esta etapa é similar à necessidade de pontuar as funções orgânicas, sinalizando as que merecerão maior atenção, importância e prioridade. Afinal, em uma enfermidade generalizada em que há risco de vida, você como médico, daria prioridade ao tratamento de um ferimento na bexiga ou no coração? Trataria, neste caso, do sistema circulatório ou do digestivo?

Para realizar o adequado mapeamento da relevância de cada processo de negócio crítico (relação de peso entre eles associada à importância para o negócio) é necessário envolver um ou mais gestores que compartilhem uma visão corporativa – conhecendo o funcionamento global do negócio – sem estar diretamente e exclusivamente envolvido com um ou mais processos específicos, ou que possua imparcialidade no momento de ponderar a importância que irá orientar a priorização das ações nas etapas subsequentes.

Crítérios

A metodologia aplica valores dentro da faixa 1 a 5 para indicar o grau de relevância, sendo, este número, diretamente proporcional, aumentando a relevância à medida que a pontuação se aproxima do 5. Além disso, a associação das escalas com palavras e expressões torna o processo de mapeamento mais elucidativo, facilitando os envolvidos a mensurarem a relevância entre os processos. Contudo, deve-se ter cuidado para não gerar uma interpretação errônea das expressões adotadas nas escalas. Elas devem ser encaradas apenas como uma forma de ponderar e mensurar a importância de cada processo de negócio, e não devem ser interpretadas isoladamente. Isso provocaria a inevitável pergunta: “Se o processo XPTO já foi pré-selecionado, como poderá ser agora classificado como NÃO CONSIDERÁVEL?”.

Assim, a melhor forma de conduzir a análise, qualificando-a, é sempre induzir os gestores a refletirem sobre a importância do processo-alvo para a operação do negócio, ajustando (repontuando), ao longo da entrevista, as relações entre todos os processos de negócio.

Aplicando, de forma holística, estes critérios sob os processos de negócio, subsidiaremos as demais etapas com parâmetros de ponderação que auxiliarão na interpretação dos estudos específicos que serão realizados em cada um dos processos isoladamente, contando com a visão segmentada de cada um de seus gestores.

ESCALA	AUXILIO DE INTERPRETAÇÃO
1 NÃO CONSIDERÁVEL	Envolve o atingimento gerenciável do Processo de Negócio podendo provocar Impactos praticamente irrelevantes.
2 RELEVANTE	Envolve o atingimento gerenciável do Processo de Negócio podendo provocar Impactos apenas consideráveis.
3 IMPORTANTE	Envolve o atingimento gerenciável do Processo de Negócio podendo provocar Impactos parcialmente significativos.
4 CRÍTICO	Envolve a paralisação do Processo de Negócio podendo provocar Impactos muito significativos.
5 VITAL	Envolve o comprometimento do Processo de Negócio podendo provocar Impactos incalculáveis na recuperação e na continuidade do negócio.

Figura 6-8 Tabela de escalas para classificação da relevância dos processos do negócio.


Resultado esperado desta etapa:

- Mapeamento da relevância dos Processos de Negócio críticos.
- Envolvimento dos gestores com visão holística do negócio.
- Percepção dos fatores importantes considerados pelos gestores envolvidos.

3. Estudo de Impactos CIDAD

Identificados os processos de negócio críticos na atividade anterior, é hora de realizar estudos que apontarão a sensibilidade de cada um deles diante da possível quebra de segurança, especificamente dos conceitos Confidencialidade, Integridade, Disponibilidade e dos aspectos Autenticidade e Legalidade. O estudo acontece através de entrevistas isoladas com o gestor de cada processo, e os mesmos critérios da escala de classificação utilizados no mapeamento da relevância são novamente aplicados mas, desta vez, sem considerar o negócio como um todo.

Entender melhor como os processos de negócio reagiriam sob a possibilidade de quebra dos três conceitos e dois aspectos de segurança da informação, medindo sua sensibilidade, representa um detalhamento importante para auxiliar no dimensionamento e modelagem do plano diretor de segurança, que ocorrerá na etapa conclusiva.



		CONCEITOS			ASPECTOS	
		CONFIDENCIALIDADE	INTEGRIDADE	DISPONIBILIDADE	AUTENTICIDADE	LEGALIDADE
ESCALA						
1	NÃO CONSIDERÁVEL					
2	RELEVANTE					
3	IMPORTANTE					
4	CRÍTICO					
5	VITAL					

Figura 6-9 Tabela de escalas para classificação de sensibilidade dos processos do negócio.

Resultado esperado desta etapa:

- Classificação da sensibilidade CIDAD de cada Processo de Negócio.
- Envolvimento dos gestores com visão isolada de processos específicos.
- Percepção dos fatores importantes considerados pelos gestores envolvidos.

4. Estudo de Prioridades GUT

Ainda reunidos individualmente com o principal gestor de cada processo de negócio elencado como crítico, inicia-se a etapa de estudo e pontuação de prioridades, aplicando-se, entre eles, a já conhecida por muitos, matriz de GUT: Gravidade, Urgência e Tendência.

A definição da prioridade final é composta pela análise e pelo produto das três dimensões do GUT, seguindo este modelo de condução dos questionamentos:

Dimensão: Gravidade

- Seria muito grave para o processo do negócio em análise se algum fato atingisse qualquer um dos conceitos e aspectos, provocando a quebra da segurança da informação?

Esta linha de análise deve considerar a *severidade* dos impactos associados diretamente, e exclusivamente, ao processo de negócio anali-

sado. Por exemplo: o que seria do processo de aprovação de crédito de uma instituição financeira, se a base de dados dos clientes – matéria-prima principal da atividade – *fosse corrompida*, tendo sua integridade atingida?

Dimensão: Urgência

- Havendo a quebra da segurança da informação, independentemente do conceito ou aspecto atingidos, qual seria a urgência em solucionar os efeitos do ocorrido e em reduzir os riscos no processo de negócio em análise?

Esta linha de análise deve considerar o *tempo de duração* dos impactos associados diretamente, e exclusivamente, ao processo de negócio analisado. Por exemplo: o que seria do processo de aprovação de crédito de uma instituição financeira, se a base de dados dos clientes – matéria-prima principal da atividade – *permanecesse corrompida* 2 dias consecutivos, tendo sua integridade atingida?

Dimensão: Tendência

- Considerando os planos de curto, médio e longo prazos associados à evolução do processo do negócio em análise, qual seria sua tendência dos riscos de segurança se nenhuma atividade preventiva ou corretiva fosse aplicada?

Esta linha de análise deve considerar a *oscilação da importância* dos impactos associados diretamente, e exclusivamente, ao processo de negócio analisado. Por exemplo: o que seria do processo de aprovação de crédito de uma instituição financeira, se a base de dados dos clientes – matéria-prima principal da atividade – *fosse corrompida a curto, médio e longo prazos*, tendo sua integridade atingida?

Critérios

A metodologia aplica valores dentro da faixa 1 a 5 para indicar o grau de prioridade, sendo este número diretamente proporcional, aumentando a priorização à medida que a pontuação de aproxima do 5. Além disso, a associação das escalas com palavras e expressões torna o processo de mapeamento mais elucidativo, facilitando os envolvidos a mensurarem a prioridade entre os processos. Contudo, deve-se ter cuidado para não gerar uma interpretação errônea das expressões adota-

das nas escalas. Elas devem ser encaradas apenas como uma forma de ponderar e mensurar a importância de cada processo de negócio, e não devem ser interpretadas isoladamente.

Gravidade	Urgência	Tendência
1 sem gravidade	1 sem pressa	1 não vai agravar
2 baixa gravidade	2 tolerante à espera	2 vai agravar a longo prazo
3 média gravidade	3 o mais cedo possível	3 vai agravar a médio prazo
4 alta gravidade	4 com alguma urgência	4 vai agravar a curto prazo
5 altíssima gravidade	5 imediatamente	5 vai agravar imediatamente

Figura 6-10 Tabela de escalas para classificação de prioridade dos processos do negócio.

Por se tratar de dimensões que compõem o GUT, apontando a prioridade do processo de negócio em relação aos demais, os valores de classificação são multiplicados gerando o GUT final; dessa forma, a faixa de valor final possível é de 1 a 125.

Objetivando facilitar a identificação rápida dos processos e suas prioridades, o GUT final é posicionado em blocos identificados por cores, onde as faixas de 1 a 42, 43 a 83 e 84 a 125 são sinalizadas, respectivamente, pelas cores VERDE, AMARELA e VERMELHA.

Resultado esperado desta etapa:

- Mapeamento da prioridade de cada Processo de Negócio.
- Percepção das características de cada processo em função das dimensões do GUT.

5. Estudo de Perímetros

Dando continuidade à metodologia do Plano Diretor de Segurança que objetiva montar um mapa de relacionamento e dependência entre Processos de Negócio, Aplicações e Infra-estrutura Física, Tecnológica e Humana, inicia-se a etapa de estudo dos ativos que sustentam cada um dos processos de negócio.

Isso se justifica pelo perfil técnico de muitas atividades que irão compor a solução corporativa de segurança da informação e, portanto, pela necessidade de identificar os alvos de infra-estrutura que têm relação direta e indireta com cada um dos processos de negócio tratados individualmente. (Consulte a Figura 6-11.)

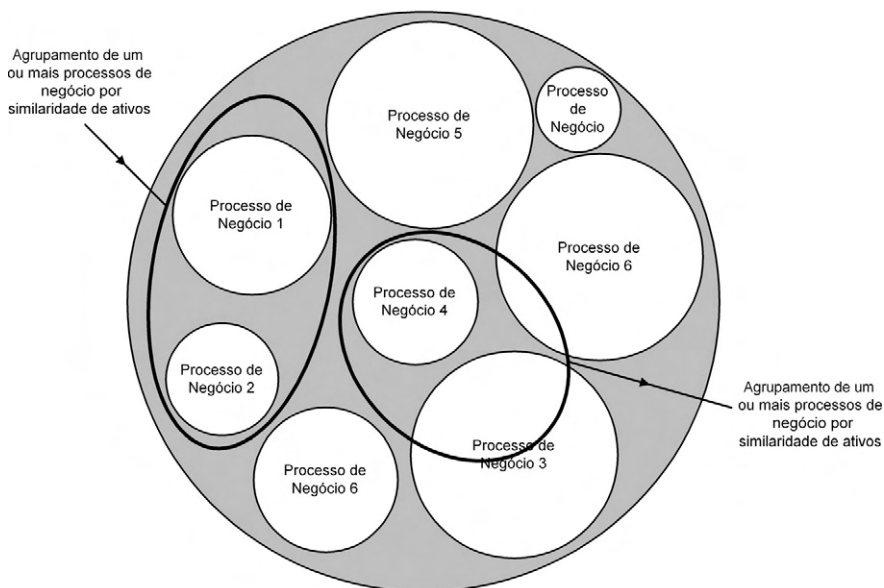


Figura 6-11 Representação hipotética da divisão da empresa em Processos de Negócio e os conseqüentes agrupamentos com base na similaridade dos ativos físicos, tecnológicos e humanos que os sustentam direta ou indiretamente.

De posse do mapeamento de processos, já dispomos dos elementos geradores de dor, sua localização, os possíveis impactos ao corpo, se fossem afetados, e a prioridade em reduzir os riscos de impacto, chega o momento de identificar os ativos – infra-estrutura, tecnologia, aplicações, informações e pessoas – que sustentam e suportam os processos do negócio. De acordo com os aspectos e conceitos de segurança da informação, os ativos possuem vulnerabilidades que deverão ser eliminadas, minimizadas e administradas pelas ações dos controles de segurança. Diferente das atividades anteriores, esta reúne entrevistas com os principais gestores da esfera técnico-tática que irão levantar números e informações topológicas, físicas e tecnológicas, ligadas direta e indiretamente aos processos do negócio. Diante disso, a atividade passa a ser primordial para que os projetos necessários sejam identificados e passem a integrar o Plano Diretor de Segurança.

É comum, nesta etapa, requisitar plantas baixas que revelem os segredos do ambiente físico, mapas topológicos, inventário de equipamentos, sistemas e aplicações nas mais diversas plataformas. Lembre-se de que aqui é o momento de descobrirmos quais ativos estão por trás do funcionamento dos processos de negócio. Tudo o que for im-

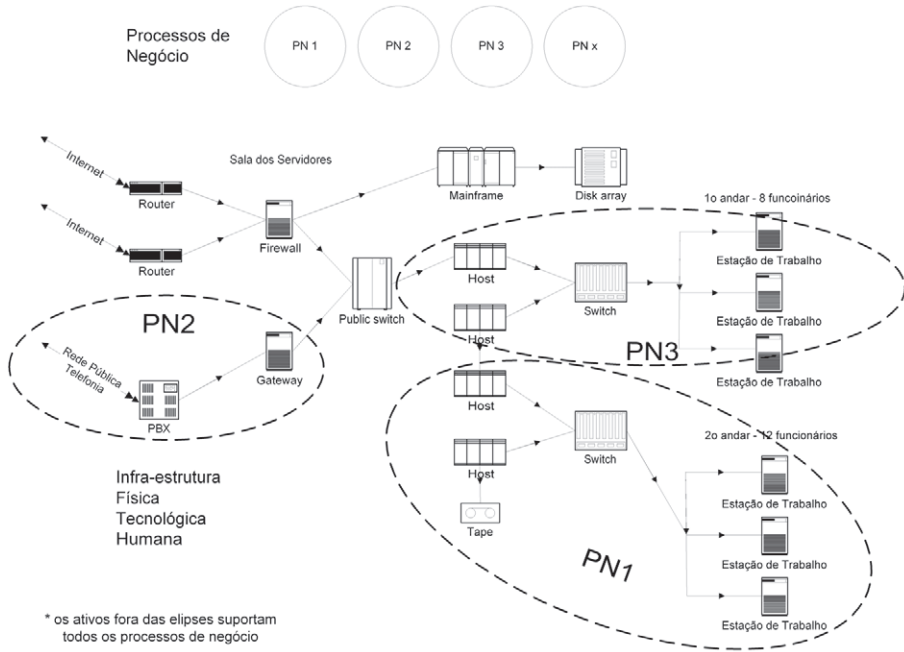


Figura 6-12 Ilustração da relação entre ativos e processos de negócio.

portante para sua operação deve ser relacionado, buscando, inclusive, identificar seu funcionamento, relações de troca de informações e fluxo de dados. (Consulte a Figura 6-12.)

Mais uma vez abusando da analogia com o corpo humano, como se não conhecêssemos sua engenharia de funcionamento, o objetivo desta etapa é descobrir quais órgãos, funções e elementos biológicos são usados por cada um dos sistemas, como respiratório, circulatório, digestivo etc. Somente obtendo um mapeamento preciso, poderemos definir atividades e suas prioridades nas etapas subsequentes.

Resultado esperado desta etapa:

- Mapeamento dos ativos.
- Mapeamento da relação entre ativos e processos de negócio.

6. Estudo de Atividades

É o momento do médico especialista analisar as reclamações de dor, os resultados dos exames, o contexto, o comportamento habitual e as ne-

cessidades do presente e futuro do paciente (de acordo com seus planos) para dimensionar a solução corporativa de segurança, composta por projetos que irão subsidiar a modelagem do PDS. É hora de planejar as ações que ocorrerão em ambientes e perímetros distintos e isolados, mas que estarão sendo coordenadas e, principalmente, estarão em conformidade com as diretrizes de segurança da empresa, proposta pelo modelo de gestão corporativa de segurança da informação.

Esta etapa inicia o processo de elaboração do plano diretor de segurança, indicando as atividades/projetos necessários e distribuindo-os ao longo do tempo e de acordo com a prioridade extraída da percepção de relevância dos processos de negócio.

Conta com inúmeras reuniões de análise e interpretação das informações coletadas, cruzando-as com os planos de negócio, recursos disponíveis e o nível de segurança atual versus o recomendado para a natureza de sua atividade.

Resultado esperado desta etapa:

- Mapeamento dos ativos.
- Mapeamento da relação entre ativos e processos do negócio.

Organização do Comitê Corporativo de Segurança

Paralelamente às atividades de levantamento de informações e diagnóstico, é fator crítico de sucesso iniciar a organização de um grupo, convencionalmente chamado de Comitê Corporativo de Segurança. A primeira atividade é definir as responsabilidades de planejamento, execução, monitoração, seu posicionamento dentro do organograma da empresa, garantindo que tenham acesso a esferas decisivas que possam atuar sobre toda a corporação. Seguido da divulgação interna e oficialização deste grupo formado por representantes de diversas áreas estratégicas da empresa, que reúnem especialidades e visões distintas. Seu principal papel será organizar, concentrar e planejar as ações de segurança que irão interferir em todos os ambientes e processos, tendo a possibilidade de redirecionar os planos de acordo com as mudanças físicas, tecnológicas e humanas que, inevitavelmente, ocorrerão.

Organização do *Security Office*

Esta ocupação deve existir oficialmente na empresa cujas responsabilidades e habilidades estejam diretamente associadas à liderança do Co-

mitê Corporativo de Segurança e à interação com os líderes dos Comitês Interdepartamentais de Segurança. Perfil técnico aprofundado, visão corporativa e destreza para gestão são elementos fundamentais para que haja uma canalização de esforços de forma coerente com os macro-objetivos da segurança e do próprio negócio. A propósito: negócio e segurança devem coexistir em harmonia, onde o primeiro aponta as carências, estratégias e necessidades de novas aplicações, e o segundo se empenha em reduzir os riscos e o potencial de impacto através de controles bem empregados corporativamente. O *Security Officer* tem de ser mediador, orientador, questionador, analisador de ameaças, riscos, impactos e do conseqüente estudo de viabilidade dos próximos passos.

Organização de Comitês Interdepartamentais de Segurança

Com uma esfera de abrangência menor, estes comitês têm importante papel no modelo de gestão de segurança da informação. Apesar de estarem sendo orientados por diretrizes maiores na esfera do Comitê Corporativo de Segurança, deverão medir os resultados dos ambientes específicos, reportar novas necessidades e situações que exponham a informação.

Depois de explicitados anteriormente os fatores críticos de sucesso dentro do modelo de gestão corporativa da segurança da informação, podemos didaticamente sintetizar a estrutura proposta através da expressão: ação local orientada por visão global.

Diante disso, imagino que perceba, a partir de agora, quão necessária é a aplicação desse modelo em seu negócio, o que torna conveniente uma frase de estímulo: “Plano Diretor de Segurança: você também pode!”.

6.3 Plano de Continuidade de Negócios

Garantir a continuidade de processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre. Com este propósito e formado pelas etapas análise de impactos no negócio, estratégias de contingência e três planos de contingência propriamente ditos, o Plano de Continuidade de Negócios deve ser elaborado com o claro objetivo de contingenciar situações e incidentes de segurança que não puderem ser evitados. Deve ser eficaz como o pára-quedas reserva o é em momento de falha do principal, garantindo, apesar do susto, a vida do pára-quedista em queda.

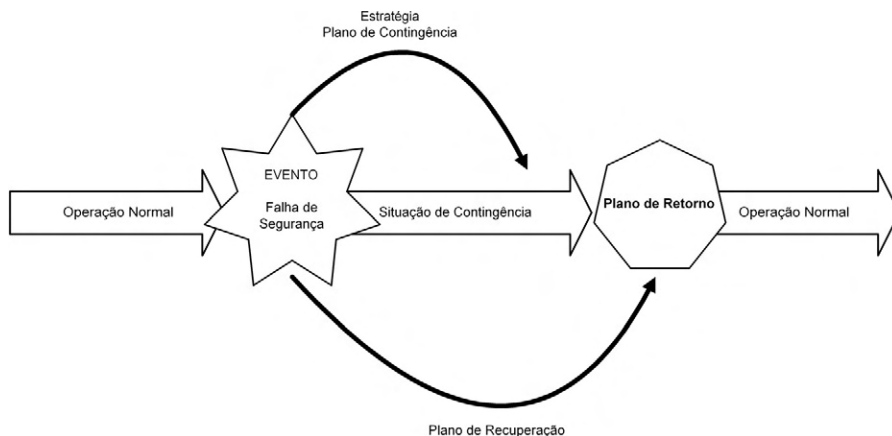


Figura 6-13 Ilustração dos papéis do Plano de Contingência, Plano de Retorno e Plano de Recuperação.

Segundo o DRI – *Disaster Recovery Institute*, de cada cinco empresas que possuem interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos.

Assim, o Plano de Continuidade tem, por sua natureza, um alto nível de complexidade, podendo assumir diversas formas em função do objeto a ser contingenciado e a abrangência de sua atuação. Diferente do que muitos imaginam, uma empresa não possuirá um plano único, mas diversos planos integrados e focados em diferentes perímetros, sejam físicos, tecnológicos ou humanos e, ainda, preocupada com múltiplas ameaças potenciais. Esta segmentação é importante; afinal, uma empresa tem processos cuja tolerância à falha é variável, os impactos idem, assim como o nível de segurança necessário à natureza das informações manipuladas.

Seja qual for o objeto da contingência – uma aplicação, um processo de negócio, um ambiente físico e, até mesmo, uma equipe de funcionários –, a empresa deverá selecionar a estratégia que melhor conduza o objeto a operar sob nível de risco controlado. Apesar de uma base conceitual comum, muitas são as variantes de metodologia para a elaboração de um plano de continuidade; portanto, você pode se deparar com outras nomenclaturas ou novos grupamentos de estratégia. De qualquer forma, as soluções de continuidade vão sendo personalizadas de acordo com o contexto, pelas características de um segmento de mercado ou fato específico, como ocorreu no ano de 1999 por conta dos computadores com dificuldades de gerenciar a representação de data, apelidado de “Bug do Ano 2002”.

Análise de Impactos no Negócio

Conhecido mundialmente pela sigla BIA – *Business Impact Analysis*, esta primeira etapa é fundamental por fornecer informações para o perfeito dimensionamento das demais fases de construção do plano de continuidade. Seu objetivo é levantar o grau de relevância entre os processos ou atividades que fazem parte do escopo da contingência em função da continuidade do negócio. Em seguida, são mapeados os ativos físicos, tecnológicos e humanos que suportam cada um deles, para então apurar os impactos quantitativos que poderiam ser gerados com a sua paralisação total ou parcial.

Processos de Negócio		PN1	PN2	PN3	PN4	PNn
ESCALA						
1	NÃO CONSIDERÁVEL					
2	RELEVANTE	X				
3	IMPORTANTE			X		
4	CRÍTICO				X	
5	VITAL		X			

Figura 6-14 Ilustração da classificação de relevância entre os processos pertencentes ao escopo do plano.

De posse desta análise BIA, torna-se possível definir as prioridades de contingência, os níveis de tolerância à indisponibilidade de cada processo ou atividade pertencente à contingência e, ainda, agrupar os ativos em função de sua natureza e relação de dependência que mantêm com os processos. Tem-se, a partir de então, uma fotografia de funcionalidade dos processos, restando definir as ameaças que se quer contingenciar. A escolha das ameaças a se considerar para cada processo está diretamente ligada à probabilidade e severidade de um incidente.

Perceberemos, adiante, que muitas das tarefas realizadas pelo BIA poderiam ser complementadas pelos resultados de uma análise de riscos, sendo esta, portanto, a atividade primeira e mais importante para orientar todas as ações de segurança da informação. Se esta herança

		Ameaças consideradas					Tolerância
		Incêndio	Greve	Interrupção de Energia	Ataque Denial of Service	Sabotagem	
Processos de Negócio	PN 1	X		X		X	48 horas
	PN 2	X					5 horas
	PN 3	X	X	X	X		24 horas
	PN x				X	X	15 minutos

Figura 6-15 Ilustração da seleção de ameaças a serem consideradas pelo plano e a percepção de tolerância de cada processo do negócio.

ocorresse efetivamente, o BIA se resumiria a quantificar os impactos e a selecionar as ameaças a serem consideradas pelo plano de continuidade do negócio. (Consulte a Figura 6-15.)

Estratégias de Contingência

Hot-site

Recebe este nome por ser uma estratégia “quente” ou pronta para entrar em operação assim que uma situação de risco ocorrer. Mais uma vez, o tempo de operacionalização desta estratégia está diretamente ligada ao tempo de tolerância a falhas do objeto. Se a aplicássemos em um equipamento tecnológico, um servidor de banco de dados, por exemplo, estaríamos falando de milissegundos de tolerância para garantir a disponibilidade do serviço mantido pelo equipamento.

Warm-site

Seguindo a nomenclatura da primeira estratégia, esta se aplica a objetos com maior tolerância à paralisação, podendo se sujeitar à indisponibilidade por mais tempo, até o retorno operacional da atividade. Tomemos, como exemplo, o serviço de e-mail dependente de uma

conexão de comunicação. Vemos que o processo de envio e recebimento de mensagens é mais tolerante que o exemplo usado na primeira estratégia, pois poderia ficar indisponível por minutos, sem, no entanto, comprometer o serviço ou gerar impactos significativos.

Realocação de Operação

Como o próprio nome denuncia, esta estratégia objetiva desviar a atividade atingida pelo evento que provocou a quebra de segurança, para outro ambiente físico, equipamento ou *link*, pertencentes à mesma empresa. Esta estratégia só é possível com a existência de “folgas” de recursos que podem ser alocados em situações de crise. Muito comum, essa estratégia pode ser entendida pelo exemplo em que se redireciona o tráfego de dados de um roteador ou servidor com problemas para outro que possua folga de processamento e suporte o acúmulo de tarefas.

Bureau de Serviços

Esta estratégia considera a possibilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado; portanto, fora dos domínios da empresa. Por sua própria natureza, em que requer um tempo de tolerância maior em função do tempo de reativação operacional da atividade, torna-se restrita a poucas situações. O fato de ter suas informações manuseadas por terceiros e em um ambiente fora de seu controle, requer atenção na adoção de procedimentos, critérios e mecanismos de controle que garantam condições de segurança adequadas à relevância e criticidade da atividade contingenciada.

Acordo de Reciprocidade

Muito conveniente para atividades que demandariam investimentos de contingência inviáveis ou incompatíveis com a importância da mesma, esta estratégia propõe a aproximação e um acordo formal com empresas que mantêm características físicas, tecnológicas ou humanas semelhantes a sua, e que estejam igualmente dispostas a possuir uma alternativa de continuidade operacional. Estabelecem em conjunto as situações de contingência e definem os procedimentos de compartilhamento de recursos para alocar a atividade atingida no ambiente da outra empresa. Desta forma, ambas obtêm redução significativa dos investimentos. Apesar do notório benefício, to-

das as empresas envolvidas precisam adotar procedimentos personalizados e mecanismos que reduzam a exposição das informações que, temporariamente, estarão circulando em ambiente de terceiros. Este risco se agrava quando a reciprocidade ocorre entre empresas pseudoconcorrentes que se unem exclusivamente com o propósito de reduzir investimentos, precisando fazê-lo pela especificidade de suas atividades, como por exemplo, no processo de impressão de jornais.

Cold-site

Dentro do modelo de classificação adotado nas duas primeiras estratégias, esta propõe uma alternativa de contingência a partir de um ambiente com os recursos mínimos de infra-estrutura e telecomunicações, desprovido de recursos de processamento de dados. Portanto, aplicável a situações com tolerância de indisponibilidade ainda maior.

Auto-suficiência

Aparentemente uma estratégia impensada, a auto-suficiência é, muitas vezes, a melhor ou a única estratégia possível para determinada atividade. Isso ocorre quando nenhuma outra estratégia é aplicável, quando os impactos possíveis não são significativos ou quando estas são inviáveis, seja financeiramente, tecnicamente ou estrategicamente. A escolha de qualquer uma das estratégias estudadas até o momento depende diretamente do nível de tolerância que a empresa pode suportar e ainda depende do nível de risco que seu executivo está disposto a correr. Esta decisão pressupõe a orientação obtida por uma análise de riscos e impactos que gere subsídios para a apoiar a escolha mais acertada.

Planos de Contingência

São desenvolvidos para cada ameaça considerada em cada um dos processos do negócio pertencente ao escopo, definindo em detalhes os procedimentos a serem executados em estado de contingência. É acertadamente subdividido em três módulos distintos e complementares que tratam especificamente de cada momento vivido pela empresa.

Plano de Administração de Crise

Este documento tem o propósito de definir passo-a-passo o funcionamento das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados pela mesma equipe no período de retorno à normalidade. O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo plano.

Plano de Continuidade Operacional

Este documento tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio. Orientar as ações diante da queda de uma conexão à Internet, exemplificam os desafios organizados pelo plano.

Plano de Recuperação de Desastres

Este documento tem o propósito de definir um plano de recuperação e restauração das funcionalidades dos ativos afetados que suportam os processos de negócio, a fim de restabelecer o ambiente e as condições originais de operação.

É fator crítico de sucesso estabelecer adequadamente os gatilhos de acionamento para cada plano de contingência. Estes gatilhos são parâmetros de tolerância usados para sinalizar o início da operacionalização da contingência, evitando acionamentos prematuros ou tardios. Dependendo das características do objeto da contingência, os parâmetros podem ser: percentual de recurso afetado, quantidade de recursos afetados, tempo de indisponibilidade, impactos financeiros etc.

A notória complexidade do Plano de Continuidade Operacional, em função da diversidade de objetos, suas características personalizadas, a abrangência das ameaças possíveis consideradas e a necessária integração dos planos de administração de crises, planos de continuidade operacional e dos planos de recuperação de desastres, torna imprescindível a construção de um modelo dinâmico de manutenção dos documentos e de testes.

Por se tratar de uma peça importante na gestão corporativa de segurança da informação, principalmente por ser o último recur-

so depois que todos os demais falharam, os três planos precisam passar por baterias severas de teste e homologação, a fim de garantir sua eficiência e permitir ajustes diante de previsíveis mudanças físicas, tecnológicas e humanas que ocorrem frequentemente no ambiente corporativo.

6.4 Política de Segurança da Informação

Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, a política tem um papel fundamental e, guardadas as devidas proporções, tem importância similar à constituição federal para um país. Desta forma, assume uma grande abrangência e, por conta disso, é subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégica, tática e operacional.

Estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa; portanto, a política deve ser personalizada.

As diretrizes, que por si só, têm papel estratégico, precisam expressar a importância que a empresa dá para a informação, além de comunicar aos funcionários seus valores e seu comprometimento em incrementar a segurança à sua cultura organizacional.

É notória a necessidade do envolvimento da alta direção, refletida pelo caráter oficial com que a política é comunicada e compartilhada junto aos funcionários. Este instrumento deve expressar as preocupações dos executivos e definir as linhas de ação que orientarão as atividades táticas e operacionais.

Responsabilidades dos proprietários e custodiantes das informações, estrutura do *Security Office*, métricas, índices e indicadores do nível de segurança, controles de conformidade legal, requisitos de educação e capacitação de usuários, mecanismos de controle de acesso físico e lógico, responsabilizações, auditoria do uso de recursos, registros de incidentes e gestão da continuidade do negócio são algumas das dimensões a serem tratadas pela política de segurança.

Com caráter tático, as normas são o segundo nível da política, detalhando situações, ambientes, processos específicos e fornecendo orientação para o uso adequado das informações. Baseado em ordem de grandeza, podemos estimar 10 a 20 diretrizes em empresas de qual-

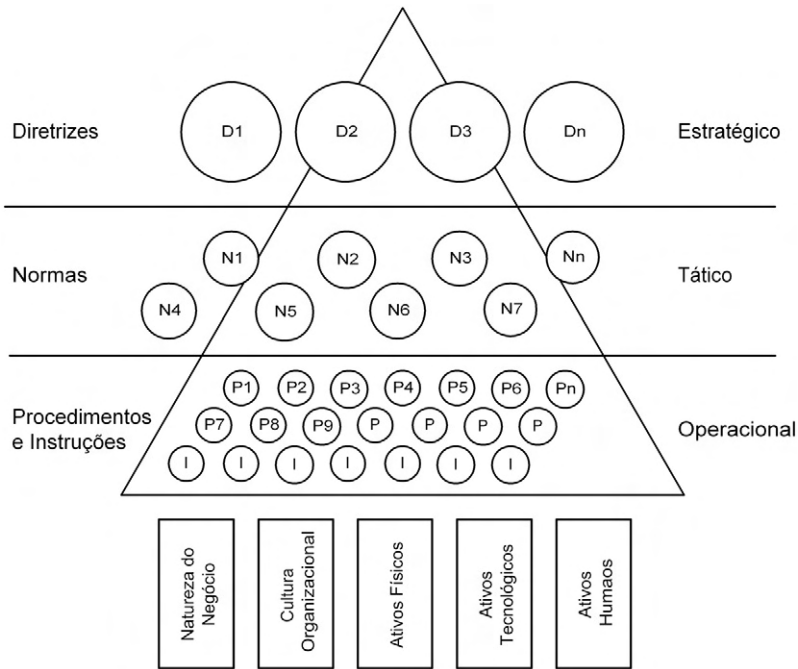


Figura 6-16 Diagrama de conceito dos componentes da política e seus pilares de personalização e sustentação.

quer porte, mas teremos de multiplicar este número por 100 ou mais para estimar o volume de normas aplicáveis. Este volume tende a ser proporcional ao porte da empresa, à heterogeneidade de seus ativos físicos, tecnológicos e humanos, e, ainda, ao grau de detalhamento necessário para levar a empresa a operar sob o nível de risco adequado. (Consulte a Figura 6-16.)

Critérios normatizados para admissão e demissão de funcionários; criação e manutenção de senhas; descarte de informação em mídia magnética; desenvolvimento e manutenção de sistemas; uso da Internet; acesso remoto; uso de *notebook*; contratação de serviços terceirizados; e classificação da informação são bons exemplos de normas de uma típica política de segurança.

Em especial, a norma de classificação da informação é fator crítico de sucesso, pois assume a responsabilidade por descrever os critérios necessários para sinalizar a importância e o valor das informações, premissa importante para a elaboração de praticamente todas as demais normas. Não há regra preconcebida para estabelecer esta classificação; mas é preciso entender o perfil do negócio e as características

Critérios de Classificação da Informação	EXTRA CONFIDENCIAL	CONFIDENCIAL	RESTRITO	INTERNO	PÚBLICO
Ciclo de Vida da Informação					
MANUSEIO					
ARMAZENAMENTO					
TRANSPORTE					
DESCARTE					

critérios para tratamento da informação em cada momento do ciclo de vida de acordo com sua classificação

Figura 6-17 Ilustração da relação entre classificação e tratamento definido na política para o ciclo de vida da informação.

das informações que alimentam os processos e circulam no ambiente corporativo para que os critérios sejam personalizados. (Consulte a Figura 6-17.)

Procedimentos e instruções deverão estar presentes na política em maior quantidade por seu perfil operacional, onde é necessário descrever meticulosamente cada ação e atividade associada a cada situação distinta de uso das informações. Por exemplo: enquanto a diretriz orienta estrategicamente para a necessidade de salvaguardar as informações classificadas como confidenciais, e a norma define que estas deverão ser criptografadas em tempo de envio por e-mail, o procedimento e a instrução específica para esta ação tem de descrever os passos necessários para executar a criptografia e enviar o e-mail. A natureza detalhista deste componente da política pressupõe a necessidade de manutenção ainda mais freqüente.

Diante disso, já é possível perceber o quão complexo é desenvolver e, principalmente, manter atualizada a política de segurança da informação com todos os seus componentes. Esta percepção torna-se ainda mais latente ao considerarmos o dinamismo do parque tecnológico de uma empresa e, ainda, as mudanças previsíveis e imprevisíveis que o ne-

gócio poderá sofrer. Dessa forma, o importante é dar o pontapé inicial e formar um grupo de trabalho com representantes das áreas e departamentos mais representativos, integrando visões, percepções e necessidades múltiplas que tenderão a convergir e gerar os instrumentos da política. Comece elaborando as diretrizes, envolva os executivos e conquiste apoio. Estabeleça os responsáveis e os gestores diretos da manutenção da política. Desenvolva um programa de divulgação das diretrizes, normas, procedimentos e instruções da política como instrumento para disseminação de cultura e conscientização dos funcionários. Lance mão de seminários, cartazes, brindes, comunicações oficiais dos executivos, cursos convencionais ou on-line, protetores de tela e tudo mais que se aplicar ao perfil da empresa e à natureza de sua atividade. O importante é envolver todos os funcionários, fazendo-os se sentir co-responsáveis pela saúde da segurança do negócio e, principalmente, responsáveis pela proteção das informações por eles custodiadas.

A conformidade com requisitos legais, envolvendo obrigações contratuais, direitos de propriedade intelectual, direitos autorais de software e todas as possíveis regulamentações que incidam no negócio da empresa devem ser respeitados e, portanto, deve ser a linha de conduta da construção da política de segurança.

6.5 Análise de Riscos e Vulnerabilidades

Realizar uma análise de segurança já é prioridade para a grande maioria das empresas, o que vem demonstrar a percepção da necessidade de diagnosticar os riscos. Contudo, ainda há um grande “vazio” no entendimento do que é uma análise de riscos de verdade.

Voltando aos pilares de sustentação do negócio, vemos iniciativas de mapeamento de vulnerabilidades concentradas puramente nos ativos tecnológicos, ou seja, instrumentos destinados a analisar e identificar falhas de computadores, redes e sistemas. Evidente que são atividades importantes, mas não suficientes para, isoladamente, diagnosticar com precisão os reais riscos que envolvem a operação da empresa. Muitos outros pilares convivem com os pilares tecnológicos e, dependendo da natureza do negócio, estes podem ser ainda mais relevantes para a sustentação. (Consulte a Figura 6-18.)

Há uma quebra de paradigma ao compreender que os riscos de uma empresa não estão apenas associados ao volume de falhas tecnológicas, à qualificação das ameaças que poderiam explorá-las ou, ain-

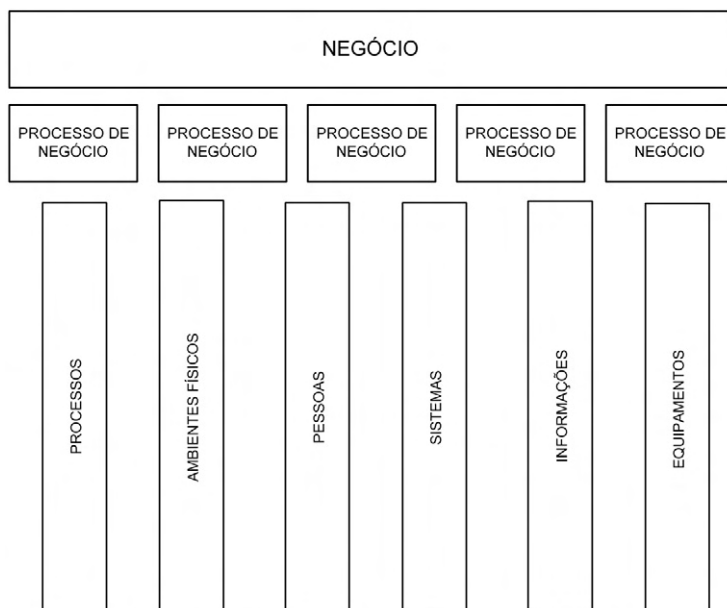


Figura 6-18 Relação de dependência entre ativos, processos de negócio e o próprio negócio.

da, aos impactos potenciais. Diagnosticar o risco envolve a análise de variáveis endógenas que extrapolam os aspectos tecnológicos; portanto, devem considerar, também, os aspectos comportamentais dos recursos humanos, os aspectos físicos, legais e, ainda, um grande leque de variáveis exógenas que interferem direta ou indiretamente na proteção do negócio. Uma mudança estratégica, uma nova *business unit*, a presença de um novo concorrente ou, ainda, um fator representativo da economia podem provocar oscilações no nível de risco do negócio, tirando a empresa de seu ponto de conforto.

Diante disso, a Análise de Riscos tem de ser encarada como um instrumento fundamental para diagnosticar a situação atual de segurança da empresa, através da sinergia entre o entendimento dos desafios do negócio, o mapeamento das funcionalidades dos processos de negócio e o relacionamento deles com a diversidade de ativos físicos, tecnológicos e humanos que hospedam falhas de segurança.

Existem, fundamentalmente, duas linhas metodológicas para orientar uma análise de riscos. A quantitativa é orientada a mensurar os impactos financeiros provocados por uma situação de quebra de segurança a partir da valoração dos próprios ativos. A qualitativa é orientada por critérios que permitem estimar os impactos ao negócio provo-

cados pela exploração de uma vulnerabilidade por parte de uma ameaça. Ambas possuem pontos positivos e negativos; porém, com o grande grau de subjetividade no processo de valoração dos ativos e, ainda, dos impactos em cascata, diretos e indiretos, potencialmente provocados por uma quebra de segurança, a metodologia de análise qualitativa tem demonstrado eficiência superior.

Aplicando a metodologia para mapeamento dos processos de negócio adotada no plano diretor de segurança, ou herdando os resultados dessa atividade, têm-se o mapa de relacionamento e dependência dos ativos. Nesta fase, iniciam-se as atividades de coleta de evidências e identificação de ameaças e vulnerabilidades potencialmente presentes nos ativos. É importante compreender que a vulnerabilidade por si só não causa qualquer dano ao ativo, sendo apenas uma situação de fragilidade. O dano só se efetivará mediante a exploração da vulnerabilidade por parte de uma ameaça.

Aspectos considerados em uma análise de riscos:

- Relação de relevância que um processo de negócio tem para o negócio
- Relação de dependência que um ou mais processos de negócio tem do ativo
- Projeção do impacto resultante da concretização da ação de uma ameaça
- Probabilidade da ameaça explorar uma vulnerabilidade
- Severidade potencial da exploração no ativo
- Qualificação das vulnerabilidades presentes nos ativos
- Qualificação da ameaças potenciais

Vemos, a partir dessa lista, a possibilidade de montar um mapa de relacionamento em que se pode projetar situações de causa e efeito. As ligações múltiplas, a pontuação e a qualificação das ameaças e vulnerabilidades, associadas aos estudos de probabilidade e impactos tornam-se elementos subsidiadores do cálculo do risco.

Por estarmos falando de uma análise que contempla ativos físicos, tecnológicos e humanos, a fase de identificação de ameaças e vulnerabilidades deve ser orientada por entrevistas com gestores e usuários, observação comportamental dos recursos humanos, inspeção física presencial nos ambientes, estudo de documentos e análises

técnicas dos ativos tecnológicos, a fim de coletar evidências da presença de falhas.

Essas atividades são suportadas por metodologias e instrumentos de apoio, comumente baseados em padrões de mercado, normas específicas como as de cabeamento estruturado TIA/EIA 568A e por softwares especializados em plataformas e tecnologias específicas. A justificativa para as ações presenciais, entrevistas, análises físicas e, até mesmo, parte das análises técnicas se dá pela impossibilidade natural de coletar todas as evidências através de dispositivos automatizados ou informatizados. Se pegarmos um sistema operacional de rede como exemplo, veremos que em seu universo de potenciais falhas, parte delas poderia ser identificada por softwares de varredura ou *scanners*, enquanto outra parte representativa necessitaria de intervenção humana, seja para coletar, seja para mensurar a probabilidade e o impacto potencial. Esta percepção nos leva a concluir que uma análise de riscos consistente deve contar com recursos humanos com competências diversificadas, ferramentas automatizadas de apoio e gestão do levantamento e, principalmente, de uma base de conhecimento em segurança constantemente atualizada.

Podemos dizer que este *Knowledge Base* de segurança, ou base de conhecimento de vulnerabilidades, ameaças e novas tecnologias, é o cérebro de uma análise de riscos competente, pois é a responsável por armazenar, gerenciar e suportar as ações de diagnóstico, fornecendo informações atualizadas que irão permitir aos analistas experimentar as técnicas mais eficientes, localizar as mais recentes falhas e, assim, conferir maior precisão na mensuração do nível de risco da empresa.

Relevância dos Processos para o Negócio	Processos de Negócio	Ativos	Vulnerabilidade	Ameaças	Probabilidade 1-5	Severidade 1-5	Impactos	Risco do Ativo
5 VITAL	PN1	Servidor 1	1. Conta Admin com Full Control 2. Sistema Operacional Desatualizado	Ataque DDoS Sabotagem Virus	3	5	Indisponibilidade dos serviços e dos processos de negócio dependentes	3,72
3 IMPORTANTE	PN 2	Data Center		Incêndio Sabotagem ...				
4 CRÍTICO	PN n	Banco de Dados Equipe Call Center						

Figura 6-19 Ilustração das informações coletadas para fins de cálculo de risco.

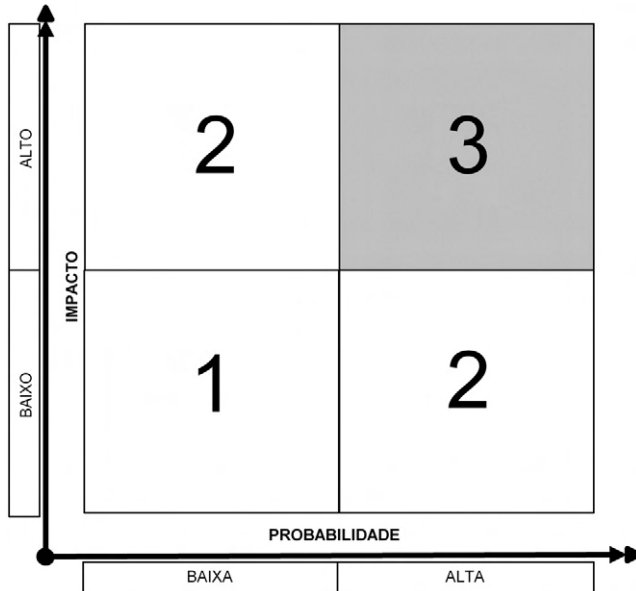


Figura 6-20 Quadrante do Risco medido ilustrativamente pela relação de Probabilidade e Impacto.

Calculada a probabilidade e severidade de uma ameaça explorar cada uma das vulnerabilidades encontradas em cada ativo, obtemos o nível de risco final de cada ativo. De posse desses resultados parciais, podemos projetar o nível de risco de cada processo de negócio, considerando os riscos de cada ativo que o sustenta. A partir desse momento, podemos estimar o risco do negócio como um todo, calculando de forma ponderada os riscos de cada um dos processos de negócio que o suporta. (Consulte a Figura 6-20.)

O resultado obtido nos permite organizar as prioridades e dimensionar um plano de ação de curto, médio e longo prazos, baseando-se na distribuição dos processos de negócio e/ou dos ativos no mapa de quadrantes de risco acima. Desta forma, tem-se a orientação necessária para apoiar as decisões e modelar contramedidas específicas para cada perímetro da empresa, como eliminar o risco, reduzir o risco, transferir o risco ou aceitar o risco. Em qualquer uma dessas situações, limitações orçamentárias, dificuldades técnicas ou fatores externos tendem a impedir a implementação total das contramedidas especificadas, levando qualquer empresa a buscar o nível de risco controlado e de acordo com a natureza de seu negócio (posicionamento consciente).

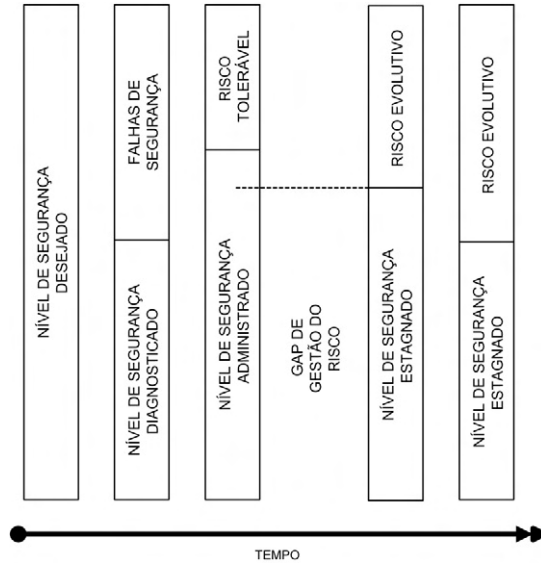


Figura 6-21 Visão geral da aplicabilidade da Análise de Riscos.

Segurança é administrar riscos. Toda empresa possui características próprias, objetivos e planos específicos; por isso, precisa encontrar o nível de risco mais adequado para operar. Dentro desse panorama a análise de riscos é o instrumento perfeito para dimensionar a situação de segurança atual, tornando-a consciente dos riscos e orientando-a a buscar soluções que a conduzam para o patamar de risco aceitável. Contudo, pelo dinamismo das mudanças sofridas pelo ambiente corporativo, devido a fatores ambientais, mercadológicos, estratégicos, econômicos, tecnológicos, estruturais etc., a análise de riscos deve fazer parte de um processo contínuo de gestão, capaz de diagnosticar novas vulnerabilidades e ameaças, garantindo, assim, a manutenção no nível de risco controlado.

Tem-se delineado como tendência, a realização de análises de riscos baseadas na medição de presença e ausência de controles de segurança, e não somente nas vulnerabilidades presentes nos ativos como eixo principal. Este movimento já é um reflexo da credibilidade adquirida pela norma de gestão de segurança da informação ISO17799.

Sua proposta se baseia no interesse e necessidade principal dos gestores de segurança em proteger o ativo, sem, no entanto, ter que se preocupar em eliminar ou administrar cada uma das vulnerabilidades individualmente. Assim, em vez de ter de mapear e buscar soluções in-

dividuais para cada uma das centenas de vulnerabilidades de um sistema operacional, por exemplo, a preocupação se concentra na verificação da presença ou ausência de aplicação do *patch*, ou programa de correção, disponibilizado pelo fabricante. Desta forma, tem-se ganho de performance, eficiência na obtenção dos resultados e, principalmente, aproxima a empresa dos controles recomendados pela ISO.

Enquanto as metodologias de análise de riscos não aderem por completo aos controles de segurança propostos pelas normas internacionais de segurança, como instrumento de medição e recomendação de ações, compete ao *Security Officer* caminhar em direção à sintonia com padrões e melhores práticas. Por conta disso, convém alinhar os resultados da análise e riscos aos controles sugeridos pela norma ISO17799 e identificar o nível de conformidade atingido pela empresa através da medição de aderência a cada um dos 127 controles de segurança.

6.6 Teste de Invasão

Apesar da interpretação distorcida do mercado em geral, julgando ser uma atividade marginal e necessariamente executada por jovens técnicos, o Teste de Invasão tem um papel importante e complementar dentro do mapeamento dos riscos da empresa. Seu objetivo, diferente da análise de riscos, não é mapear todas as ameaças, vulnerabilidades e impactos, mas avaliar o grau de segurança oferecido pelos controles de segurança de determinado perímetro. Para isso, simula tentativas de acesso indevido e invasão a partir de pontos distintos, e adota diferentes métodos e técnicas; contudo, com um objetivo bem definido. É premissa para garantir a qualidade da atividade definir claramente o perímetro que se quer testar, a ação de que tipo de ameaça se quer avaliar a proteção e, ainda, o tempo de validade do teste.

A qualidade de um teste de invasão é medida pelo grau de similaridade reproduzida pela simulação em relação às práticas reais de tentativa de invasão e não à obtenção de resultados positivos ou negativos. Quanto mais real for o teste, sem, no entanto, expor efetivamente as informações e comprometer a operação da empresa, melhor. O que se espera como resultado é a descrição do formato do teste, métodos e técnicas empregadas, evidências das tentativas e possíveis resultados positivos.

São, basicamente, quatro formatos para o teste de invasão que surgem da combinação múltipla de dois dos fatores descritos a seguir:

- Interno

Define o ambiente interno da própria empresa-alvo com o ponto de presença do analista para execução do teste. Este modelo tem se mostrado muito eficiente devido aos altos índices de tentativas de ataque e invasão realizados por funcionários e recursos terceirizados, o que torna o modelo muito próximo da realidade.

- Externo

Define um ambiente externo à própria empresa-alvo com o ponto de presença do analista para execução do teste. Este modelo tem eficiência comprovada para situações que visem simular acessos externos ao ambiente corporativo, como em acessos remotos, responsáveis por fatia representativa dos ataques e invasões.

- Cego

Define a ausência de acesso a informações privilegiadas sobre a estrutura física, tecnológica e humana, a fim de subsidiar o analista na execução do teste. Este modelo não tem demonstrado grande eficiência devido aos baixos índices de tentativas de ataques e invasões sem qualquer informação do alvo. Mesmo que este seja o status inicial de um invasor, na prática o mesmo tende a realizar uma coleta prévia de informações, adotando técnicas de engenharia social, análise de lixo, grampo telefônico, grampo eletrônico etc., a fim de aumentar as chances do ataque.

- Não cego

Define a presença de acesso a informações privilegiadas sobre a estrutura física, tecnológica e humana, a fim de subsidiar o analista na execução do teste. Este modelo demonstra eficiência pela similaridade com situações reais de ataque. E é ainda reforçado pela grande incidência de ataques internos; portanto, executados por pessoas que já dispõem de conhecimento e, muitas vezes, acesso privilegiado a informações e ambientes.

Como vemos, o Teste de Invasão demonstra ser um ótimo recurso para a sensibilização dos executivos e potenciais patrocinadores de ações corporativas, pois simula a exposição da empresa ou de um perí-

metro específico a tentativas de ataque e invasão que simulam a realidade. Por se tratar de uma atividade crítica, pois potencializa a exposição da empresa, de suas informações e processos, deve ser executada por profissionais qualificados e orientados por uma metodologia que garanta o controle das ações, o acompanhamento do *Security Officer* e não represente mais um momento de risco para o negócio.

6.7 Implementação de Controles de Segurança

Implementar é adquirir, configurar e aplicar os mecanismos de controle de segurança a fim de atingir o nível de risco adequado. Comumente esta atividade faz parte de uma orientação obtida pela análise de riscos ou por sugestões de normas específicas de segurança, como a ISO17799, o COBIT, o Technical Report 13335 ou, ainda, normas específicas como a de cabeamento estruturado EIA/TIA586A.

O universo de controles aplicáveis é enorme, pois estamos falando de mecanismos destinados à segurança física, tecnológica e humana. Se pensarmos no *peopleware*, ou seja, no capital humano como um dos elos mais críticos e relevantes para a redução dos riscos, teríamos, por exemplo, os seguintes controles:

- Seminários de sensibilização
- Cursos de capacitação
- Campanhas de divulgação da política de segurança
- Crachás de identificação
- Procedimentos específicos para demissão de admissão de funcionários
- Procedimentos específicos para tratamento de recursos terceirizados
- Termo de responsabilidade
- Termo de confidencialidade
- Softwares de auditoria de acessos
- Softwares de monitoramento e filtragem de conteúdo
- Etc.

Muitos dos controles humanos citados interferem direta ou indiretamente no ambiente físico, mas este deve receber a implementação de um outro conjunto de mecanismos voltados a controlar o acesso e as condições de ambientes físicos, sinalizando, registrando, impedindo e autorizando acessos e estados, dentre os quais podemos citar:

- Roletas de controle de acesso físico
- Climatizadores de ambiente
- Detectores de fumaça
- Acionadores de água para combate a incêndio
- Extintores de incêndio
- Cabeamento estruturado
- Salas-cofre
- Dispositivos de biometria
- *Smartcards*
- Certificados Digitais em Token
- Circuitos internos de televisão
- Alarmes e sirenes
- Dispositivos de proteção física de equipamentos
- *Nobreaks*
- Dispositivo de armazenamento de mídia magnética
- Fragmentadoras de papel
- Etc.

Assim como ocorre com os controles físicos e humanos, a lista dos dispositivos aplicáveis aos ativos tecnológicos é extensa; afinal, além da diversidade e heterogeneidade de tecnologias, ainda temos que considerar a velocidade criativa do setor que nos apresenta uma nova ferramenta ou equipamento praticamente a cada dia. Os instrumentos aplicáveis aos ativos tecnológicos podem ser divididos em três famílias.

Autenticação e autorização

Destinados a suprir os processos de identificação de pessoas, equipamentos, sistemas e agentes em geral, os mecanismos de autenticação mostram-se fundamentais para os atuais padrões de informatização, automação e compartilhamento de informações. Sem identificar a origem de um acesso e seu agente, torna-se praticamente inviável realizar autorizações condizentes com os direitos de acesso, podendo levar a empresa a compartilhar informações valiosas sem controle. Os métodos de autenticação são divididos em três grupos devido ao grau de segurança que oferecem.

O que você sabe

Método largamente adotado e baseado na definição de uma senha, portanto, uma *string* pessoal e intransferível entregue ao agente autorizado a empregá-la, sendo mantida uma cópia de comprovação no instrumento controlador. Nativamente este método já revela fragilidades, pois a segurança depende de fatores internos como a estrutura de construção e manutenção da senha, bem como de fatores externos ao método como o comportamento dos agentes que podem ter desvios de conduta, levando ao comprometimento do mecanismo. Compartilhar a senha, selecionar uma senha fraca, não mantê-la em segredo ou, ainda, manuseá-la sem os critérios adequados, podem por em risco toda a eficiência do método.

Desmistificando a classificação popular de senha fraca ou forte, tome como base os critérios de classificação Acadêmica e Prática. Academicamente falando, uma senha pode ser classificada como forte se possuir mais de seis caracteres, misturar números, letras em maiúsculo, em minúsculo e caracteres especiais como colchete, asterisco etc. E pode ser classificada como fraca se possuir menos de seis caracteres, se for construída apenas por números, letras maiúsculas ou minúsculas e, principalmente, quando, apesar de possuir tamanho maior, representar alguma informação do mundo real, ou seja, nomes próprios, placa de automóveis, datas de nascimento etc.

Em contrapartida, adotando o critério Prático de classificação, uma senha pode assumir o rótulo de forte ou fraca dependendo, fundamentalmente, de três fatores: do valor e importância das informações protegidas por ela, do tempo em que a senha estará cumprindo o papel de proteção, e pelo poderio, interesse e disposição que um suposto interessado despenderia para obter acesso à informação protegida.

O que você tem

Método em adoção crescente baseado na utilização de dispositivos físicos que são apresentados em processos de autenticação de acessos. Há um grande conjunto de dispositivos que se encaixam neste perfil. A escolha do melhor mecanismo está diretamente atrelada ao nível de segurança necessário para as informações e inevitavelmente ao orçamento disponível.

- Cartão com código de barras
- Cartão magnético
- *Smartcard*
- *Tokens*
- Etc.

O que você é

Ainda em fase de popularização e barateamento, este método emprega dispositivos físicos que realizam métricas biométricas para identificar pessoas que exercem o direito de acesso a informações, ambientes etc. Costumeiramente, são equipamentos dispendiosos devido à tecnologia de ponta empregada, pois se baseiam na leitura de informações do corpo humano, que são únicas em cada indivíduo. O nível de segurança oferecido por cada dispositivo depende diretamente da métrica usada e do número de pontos de comparação disponíveis por cada parte do corpo analisado.

- Geometria das mãos
- Geometria da face
- Identificação digital
- Reconhecimento da voz
- Leitura de íris
- Etc.

Diante de tantas opções de autenticação e da oferta de diferentes níveis de segurança proporcionados por cada método, é fator crítico de sucesso para o gestor da segurança analisar em detalhes o perímetro-alvo da autenticação, as reais necessidades de proteção impostas pela criticidade das informações e os impactos relacionados ao de-

sempenho e montante de investimento demandado. Mesmo assim, podem surgir situações em que um único método não atenda aos requisitos mínimos de segurança, tornando necessário combinar um ou mais métodos. Estas soluções híbridas têm sido uma constante em segmentos específicos, como o financeiro, onde o cliente, além de possuir um cartão magnético, tem de inserir uma senha fixa e, ainda, informações pessoais de comprovação de identidade.

Combate a ataques e invasões

Destinados a suprir a infra-estrutura tecnológica com dispositivos de software e hardware de proteção, controle de acesso e conseqüente combate a ataques e invasões, esta família de mecanismos tem papel importante no modelo de gestão de segurança, à medida que as conexões eletrônicas e tentativas de acesso indevido crescem exponencialmente. Nesta categoria, existem dispositivos destinados ao monitoramento, filtragem e registro de acessos lógicos, bem como dispositivos voltados para a segmentação de perímetros, identificação e tratamento de tentativas de ataque.

Firewall

Velho conhecido dos ambientes de rede, este dispositivo, que pode assumir a forma de um software e também incorporar um hardware especializado, tem o papel de realizar análises do fluxo de pacotes de dados, filtragens e registros dentro de uma estrutura de rede. Como o próprio nome diz, ele representa uma parede de fogo que executa comandos de filtragem previamente especificados com base nas necessidades de compartilhamento, acesso e proteção requeridos pela rede e pelas informações disponíveis através dela.

Buscando um modelo didático, podemos compará-lo ao tradicional filtro de água doméstico que, a princípio, é formado por um compartimento vazio por onde passa a água supostamente poluída, e por um elemento ou vela contendo camadas de filtragem formadas por diversos materiais. Ao passar por este compartimento, já com o elemento de filtragem, as impurezas da água são retidas pelas diversas camadas do elemento. Desta forma, o filtro poderá ser considerado eficiente se conseguir reter todas as impurezas e permitir a passagem de todos os demais componentes benéficos à saúde, como sais minerais etc. O *firewall* se assemelha ao filtro por também necessitar da es-

pecificação de camadas de filtragem específicas para cada empresa e situação, com o propósito de impedir acessos indevidos que ocorram de dentro ou de fora da rede, registrando essas ocorrências e, principalmente, permitindo o tráfego normal de pacotes de dados legítimos. Por ser baseado na análise binária de parâmetros definidos no filtro, o *firewall* age sempre da mesma maneira e sem considerar variáveis externas que possam modificar as situações; portanto, a eficiência de proteção desse dispositivo está ligada diretamente à adequada especificação e manutenção das regras de filtragem.

É importante lembrar que surgiu uma categoria de *firewall* destinada ao usuário final, chamada *personal firewall*, com o propósito de estender a segurança e complementar à proteção. Obviamente são recursos de software com baixa performance, mas adequadamente proporcionais, na maioria das situações, ao volume de dados trafegados em uma conexão desse gênero.

Detector de Intrusos

Normalmente chamado pela sigla em inglês IDS, o detector de intrusos é um dispositivo complementar ao *firewall* que agrega maior inteligência ao processo de combate a ataques e invasões. Diferente do *firewall*, o IDS é orientado por uma base de dados dinâmica contendo informações sobre comportamentos suspeitos de pacotes de dados e assinaturas de ataques. É uma verdadeira enciclopédia de ameaças consultada a todo o momento para que o dispositivo possa transcender a análise binária de situações e avaliar a probabilidade de um acesso ser um conhecido tipo de ataque ou uma nova técnica de invasão. Ainda não estamos falando de inteligência artificial; afinal, a ferramenta não aprende com as próprias experiências e não gera conclusões de forma autônoma, mas o dispositivo demonstra seu potencial como sinalizador de situações que fujam à normalidade. É importante ressaltar que, por possuir um grau de inferência sobre possíveis situações de risco, o detector de intrusos é responsável por muitos falso-positivos, ou seja, por sinalizar situações aparentemente estranhas, mas que são legítimas. Por conta disso, dependendo do ambiente protegido e do grau de tolerância à indisponibilidade de acesso, não é conveniente deixar que o IDS aja sozinho, mas que atue como um instrumento de sinalização para que os técnicos possam avaliar a situação e, então, decidir pelo bloqueio ou pela permissão.

Existem dispositivos que, apesar de terem sido desenvolvidos originalmente para outros fins, incorporaram, com o passar do tempo, recursos que auxiliam e, muitas vezes, reforçam atividades de bloqueio e combate a ataques. O roteador com filtro, por exemplo, incorpora parte das funcionalidades de um *firewall*, e o *switch*, naturalmente destinado à melhoria de performance e gerenciamento das redes, tem grande aplicabilidade na segmentação lógica da mesma, reduzindo a eficiência de tentativas de ataque que monitoram o meio, grampeando-o, a fim de capturar informações relevantes. Da mesma forma, o *proxy*, software com o propósito de aumentar a performance do acesso ao serviço Web da Internet através da gerência de conteúdo como se fosse uma memória *cache*, tem o potencial de filtrar e registrar acessos proibidos que sinalizam o descumprimento das normas da política de segurança.

Privacidade das comunicações

É inevitável falar de criptografia quando o assunto é privacidade das comunicações. A criptografia é uma ciência que estuda os princípios, meios e métodos para proteger a confidencialidade das informações através da codificação ou processo de cifração e que permite a restauração da informação original através do processo de decifração. Largamente aplicada na comunicação de dados, esta ciência se utiliza de algoritmos matemáticos e da criptoanálise, para conferir maior ou menor proteção de acordo com sua complexidade e estrutura de desenvolvimento. Quando vemos softwares de criptografia de mensagem ou por exemplo, aplicações que adotam criptografia, estamos diante de situações em que a ciência foi empregada e materializada em forma de programas de computador. Existem duas técnicas principais de criptografia.

Simétrica ou de chave privada

Técnica criptográfica que utiliza uma única senha, ou chave, para cifrar informações na origem e decifrá-las no destino. Apesar de sua excelente performance, entre outras coisas pela existência de uma única chave que confere velocidade aos processos matemáticos de cálculo, este método tem uma vulnerabilidade nativa presente no processo de envio ou compartilhamento da chave simétrica com o destinatário. Usando um exemplo hipotético em que se quer enviar uma mensagem criptografada do usuário A para o

usuário B, o primeiro passo seria criar uma chave simétrica e enviar uma cópia da mesma ao destinatário para que ele pudesse decriptografar a mensagem após recebê-la. O risco ocorre justamente no momento do envio da cópia da chave ao destinatário por não ter sido adotado nenhum processo de proteção. Se, exatamente neste momento frágil, apesar da pequena janela de tempo da operação, a confidencialidade da chave for quebrada, todo o processo de criptografia fica comprometido; afinal, qualquer um que conheça a chave simétrica poderá decriptografar a mensagem interceptada.

Um dos algoritmos de chave simétrica mais utilizados no mundo é o DES – *Data Encryption Standard*, criado em 1977, com chave criptográfica de 56 bits, além do 3DES, RC2, RC4 e *Blowfish*. O tamanho da chave criptográfica está diretamente ligada ao nível de segurança do algoritmo devido ao aumento exponencial de possibilidades e tentativas necessárias para “quebrar”, ou seja, para descobrir a chave certa que decifre a proteção.

Assimétrica ou de chave pública

Técnica criptográfica que utiliza um par de chaves para cada um dos interlocutores, mais especificamente uma chave privada e outra pública para o remetente, e o destinatário. Desta forma, com a criptografia assimétrica criada em 1976 por Diffie e Hellman, os interlocutores não precisam mais compartilhar uma chave única e secreta. Baseado no conceito de que para decifrar a criptografia é necessário possuir as duas chaves matematicamente relacionadas, pública e privada, o remetente só precisa da chave pública do destinatário para garantir a confidencialidade da mensagem e para permitir que o destinatário consiga decifrar a mensagem.

Como o próprio nome diz, a chave privada pertence exclusivamente ao seu proprietário e deve ser mantida em segredo. A pública, por sua vez, pode e deve ser compartilhada e estar disponível a qualquer interessado em enviar uma mensagem a você de forma criptografada. Este técnica ainda reserva recursos complementares, como a assinatura digital, obtida pela utilização da chave privada para fazer uma “marca binária” na mensagem, sinalizando ter sido escrita e enviada pelo proprietário da própria. O certificado digital é um instrumento eletrônico que atesta a veracidade da chave pública do usuário, conferindo autenticidade ao documento assinado digitalmente.

Não podemos nos esquecer, também, da função HASH, que confere a possibilidade de verificar a integridade de uma mensagem a partir da comparação, no destino, do resultado obtido pela aplicação da função. Quando os resultados obtidos pela função na origem não coincidem com os resultados obtidos no destino, tem-se a indicação de que a mensagem sofreu qualquer tipo de alteração, mesmo que muito pequena.

Aparentemente esta técnica se mostra perfeita, se não fosse pelo fato de possuir baixa performance, chegando a consumir centenas ou milhares de vezes mais tempo para ser processada se compararmos com a técnica simétrica.

Devido aos problemas presentes em ambas as técnicas, foi encontrada uma solução híbrida a partir da união de técnicas que permitiu usufruir da performance da simétrica e da segurança e funções satélites de assinatura digital e validação de integridade proporcionadas pela técnica assimétrica. De posse do par de chaves pública e privada, o remetente gera a chave simétrica e insere uma cópia em uma nova mensagem, método este que se convencionou chamar de encapsulamento, criptografando-a com a chave pública do destinatário. Este por sua vez, ao receber a mensagem confidencial, lança mão de sua chave privada para decifrá-la, obtendo acesso à cópia da chave simétrica. A partir deste momento, em que ambos estão de posse da chave simétrica enviada e recebida em segurança, o processo de comunicação criptografada pode ser reiniciado adotando esta mesma chave simétrica que irá conferir a velocidade necessária para viabilizar a troca de informações.

Virtual Private Network

Esta solução, comumente chamada pelo acrônimo VPN, é fruto da aplicação de criptografia entre dois pontos distintos através de uma rede pública ou de propriedade de terceiros. O resultado da adoção de criptografia é a criação de um túnel seguro que garante a confidencialidade das informações sem, no entanto, absorver os riscos nativos de uma rede que transcende seus limites de controle. Desta forma, a empresa passa a ter uma rede virtual privada, ou seja, a tecnologia viabiliza o uso de uma rede nativamente insegura como se parte dela fosse privada pela segurança agregada pelo tunelamento. Para cumprir o papel de extensão de sua rede corpora-

tiva, a VPN precisa garantir o mínimo de performance a fim de viabilizar conexões com filiais e parceiros, usufruindo, assim, dos benefícios de capilaridade e redundância que a Internet, por exemplo, oferece. Assim, são implementadas por software e hardware especializados e capazes de processar a codificação e a decodificação dos pacotes de dados com extrema velocidade e competência.

É importante lembrar que surgiu uma categoria de *virtual private network* destinada ao usuário final, chamada *personal VPN*, com o propósito de permitir conexões remotas seguras. Obviamente são recursos de software com baixa performance, mas adequadamente proporcionais, na maioria das situações, ao volume de dados trafegados em uma conexão desse gênero.

Public Key Infrastructure

É possível notar a grande aplicabilidade do certificado digital em processos de autenticação e criptografia, seja na publicação de informações, acessos a ambientes físicos, aplicações e equipamentos, envio de mensagens eletrônicas, redes virtuais privadas, ou na troca eletrônica de informações em geral. Sua versatilidade e potencial de crescimento trazem à tona um potencial problema: o gerenciamento do processo de emissão, revogação, guarda e distribuição; afinal, para que os documentos e processos possam assumir a credibilidade do agente ou usuário do dispositivo, a mesma dever ter sido herdada do processo de gerenciamento do dispositivo. Por conta dessa necessidade, a tecnologia PKI, ou Infra-estrutura de Chaves Públicas em português, reúne recursos de software e serviços para suportar a montagem de um processo de gestão de certificados. Buscando um exemplo que privilegie a didática, podemos fazer uma analogia com os cartórios tradicionais. Para que a compra de um bem seja concretizada, muitos documentos precisam ser autenticados por uma estrutura que tenha fé pública ou, no mínimo, confiança das partes envolvidas na transação. Este processo requer a presença física para identificação das partes através de documentos, comprovação visual da autenticidade dos documentos originais para, então, estender a originalidade às cópias.

De forma similar, o processo de certificação digital implementado com a infra-estrutura de PKI requer a identificação prévia das partes para, só então, emitir o instrumento digital. Além disso, essa mesma estrutura tem de estar orientada por uma política específica

e ser capaz de reemitir, revogar, distribuir e, principalmente, manter sob altos critérios de confidencialidade, integridade e disponibilidade o segredo do processo: a chave privada e seus critérios de concepção.

A percepção da importância técnica do assunto e, principalmente, dos fatores legais que envolvem a responsabilização de pessoas e empresas pela relação eletrônica de informações reconhecidas como legítimas, já chegou ao setor público. O interesse do governo é orientar e subsidiar uma base comum de construção de infra-estruturas de chaves pública para, no primeiro momento, garantir o reconhecimento mútuo das empresas e a administração pública federal dentro do país e, em um segundo momento, viabilizar o reconhecimento por outras estruturas internacionais integradas, que fomentarão o comércio eletrônico, as relações governamentais e empresariais. O reflexo desse movimento se materializou em agosto de 2001, através da medida provisória MP2002-2, que institui uma infra-estrutura de chaves públicas do Brasil, ou ICP-Brasil.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 62 da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz – AC Raiz, pelas Autoridades Certificadoras – AC e pelas Autoridades de Registro – AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I – Ministério da Justiça;

II – Ministério da Fazenda;

- III – Ministério do Desenvolvimento, Indústria e Comércio Exterior;
- IV – Ministério do Planejamento, Orçamento e Gestão;
- V – Ministério da Ciência e Tecnologia;
- VI – Casa Civil da Presidência da República; e
- VII – Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I – adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II – estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III – estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV – homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V – estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI – aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII – identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII – atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subsequente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10º Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei nº 3.071, de 1º de janeiro de 1916 – Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos

em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11^º A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 – Código Tributário Nacional”.

Figura 6-22 Trecho da MP2200-2 publicada no Diário Oficial de 27/08/2001

Esteganografia

Existem outras técnicas voltadas à privacidade no envio de informações. Esta, em especial, ganhou o conhecimento público através dos filmes de agentes secretos e do triste atentado terrorista de setembro de 2001. A técnica propõe o uso de métodos de camuflagem de informações sigilosas em mensagens e arquivos aparentemente inofensivos que só poderiam ser extraídas pelo destinatário, que detém o conhecimento do mapa de camuflagem. Esses métodos podem ser aplicados a arquivos binários, voz analógica, imagens eletrônicas e até mesmo a vídeo, em que os gestos aparentemente comuns podem esconder mensagens ocultas. Esse método mostra um ponto positivo, devido ao fato de não sinalizar a potenciais atacantes que uma determinada mensagem carrega informações notoriamente sigilosas, diferente da criptografia que, por estar cifrada, já denuncia sua condição e classificação.

6.8 Treinamento e Sensibilização em Segurança

Os recursos humanos são considerados o elo mais frágil da corrente, pois são responsáveis por uma ou mais fases de processo de segurança da informação. Esta situação é ratificada pelo fato de o *peopleware* não ter um comportamento binário e previsível em que se possa eliminar todas as vulnerabilidades presentes. O ser humano é uma máquina complexa, dotada de iniciativa, criatividade e que sofre interferência de fatores externos, provocando comportamentos nunca antes experimentados. O fator surpresa é um dos pontos nevrálgicos dos processos de segurança que dependem das pessoas. Se especificarmos normas de criação, manuseio, armazenamento, transporte e descarte de senhas, implementamos recursos tecnológicos de auditoria e autenticação de acesso para tornar um ambiente mais seguro, podemos ter a eficiência

dessas iniciativas postas em dúvida à medida que um recurso humano descumpra as instruções da política de segurança e compartilhe sua senha supostamente pessoal e intransferível.

Esses riscos precisam ser tratados de forma gradativa, objetivando formar uma cultura de segurança que se integre às atividades dos funcionários e passe a ser vista como um instrumento de autoproteção. As ações devem ter a estratégia de compartilhar a responsabilidade com cada indivíduo, transformando-o em co-autor do nível de segurança alcançado. Somente desta forma as empresas terão, em seus funcionários, aliados na batalha de redução e administração dos riscos.

Muitas são as formas de iniciar a construção da cultura de segurança. Algumas delas se aplicam a públicos com perfis diferentes; outras se aplicam a todos os perfis, mas em momentos distintos.

Seminários

O trabalho deve começar com seminários abertos voltados a compartilhar a percepção dos riscos associados às atividades da empresa, os impactos potenciais no negócio e, principalmente, o comprometimento dos processos críticos se alguma ameaça se concretizar. Desta forma, cada funcionário passa a se enxergar como uma engrenagem da máquina e co-responsável por seu bom funcionamento, podendo gerar impactos diretos ao seu processo e indiretos a processos adjacentes.

Campanha de Divulgação

É importante que a empresa disponha de uma política de segurança atualizada e alinhada às necessidades e estratégias do negócio, mas é fundamental que ela seja reconhecida pelos funcionários como o manual de segurança da empresa. Suas diretrizes devem ser conhecidas por todos, e suas normas, procedimentos e instruções específicas devem ser apresentados a cada grupo com perfil de atividade semelhante. Desta forma, cada membro percebe suas responsabilidades dentro de um modelo de segurança único, motivando-o a colaborar. Mas não é suficiente. Lembre-se de que os resultados efetivos de comprometimento ocorrem lentamente e, muitas vezes, requerem ações complementares.

Por conta disso, a campanha deverá lançar mão de diversos artifícios para comunicar os padrões, critérios e instruções operacionais, como cartazes, jogos, peças promocionais, protetores de tela, e-mails

informativos, e-mails de alerta, comunicados internos, páginas especializadas na Intranet etc.

Carta do Presidente

Como instrumento de oficialização dos interesses da empresa em adequar o nível de segurança de suas informações a partir do envolvimento de todos os níveis hierárquicos é conveniente que o presidente, CEO ou CIO externar esta vontade oficialmente. A Carta do Presidente tem esse papel e é disponibilizada, quando não, encaminhada a cada funcionário, dando um caráter formal ao movimento. Por vezes, este documento aparentemente simples, é responsável por muitos apoios espontâneos e o natural fortalecimento do plano estratégico de segurança da informação.

Termo de Responsabilidade e Confidencialidade

Considerado mais um importante instrumento de sensibilização e formação de cultura, o Termo de Responsabilidade e Confidencialidade tem o propósito de formalizar o compromisso e o entendimento do funcionário diante de suas novas responsabilidades relacionadas à proteção das informações que manipula. Além disso, este termo se encarrega de divulgar as punições cabíveis por desvios de conduta e, ainda, esclarecer que a empresa é o legítimo proprietário dos ativos, incluindo as informações, que fluem pelos processos de negócio e ora são temporariamente custodiadas pelas pessoas.

Cursos de Capacitação e Certificação

Dentro do quadro de funcionários, existem perfis profissionais que necessitam de maior domínio dos conceitos, métodos e técnicas de segurança, podendo inclusive, variar sua área de interesse e profundidade. Os administradores de rede, por exemplo, precisam estar preparados para reagir às tentativas de ataque e invasão, ou para contingenciar situações de risco. O *Security Officer*, por sua vez, deve ter condições de definir, medir e avaliar os índices e indicadores de segurança para subsidiar seus planos de gestão e seu planejamento de trabalho, a fim de garantir a total integração das ações e, principalmente, alcançar os objetivos. Para todos esses casos, não bastam os seminários, campanhas de conscientização ou a carta do presidente. Eles

precisam de capacitação formal através de cursos especializados, que propõem uma certificação como instrumento de reconhecimento da competência. Pela heterogeneidade de perfis, surgem demandas de cursos verticalmente técnicos, voltados a capacitar recursos em uma determinada tecnologia de segurança, bem como demandas para orientação e preparação de *Security Officers*. Entretanto, é relevante destacar a necessidade de processos contínuos de sensibilização e capacitação das pessoas, sob pena de ter a equipe estagnada e, brevemente, despreparada para a administração das novas situações de risco.

6.9 Equipe para Resposta a Incidentes

A velocidade com que uma empresa responde a situações de risco, como o aparecimento de uma nova vulnerabilidade, a indisponibilidade de ativos, ataques e invasões e tentativas de sabotagem, determina o tempo em que a empresa estará exposta e sujeita aos impactos associados.

Por conta da complexidade dos parques tecnológicos, da velocidade com que surgem novas falhas de segurança, vírus de computador e, principalmente, por causa da exigência crescente de integração, conectividade e compartilhamento, ter e manter uma equipe de segurança faz a diferença.

Como já foi comentado anteriormente, essa complexidade pode demandar um volume de recursos tão grande que pode deixar de ser interessante mantê-los. Investir de maneira desproporcional em equipes de segurança quando o *core business* de sua empresa está distante desse fim, não é uma das coisas mais inteligentes a fazer, salvo exceções em que vale a pena esse investimento devido à natureza dos produtos e serviços da empresa.

Em ambos os casos, seja com recurso próprio ou terceirizado, a empresa precisa construir um modelo de contratação e acionamento de equipes, de tal forma integradas e sintonizadas, que consigam oferecer eficiência e imprimir grande velocidade na resposta a incidentes. Parte dos resultados positivos desse modelo estão ligados à figura do coordenador, mais especificamente o *Security Officer*, que irá, a partir do conhecimento do negócio e da visão corporativa, definir as diretrizes de trabalho das equipes.

De qualquer forma, vemos a dependência de profissionais especializados em múltiplas tecnologias e constantemente atualizados, para que se mantenham aptos a reagir antes que seja tarde.

6.10 Administração e Monitoração de Segurança

É comum julgar que esta atividade possa significar o fim do trabalho, mas na verdade representa o recomeço. É uma alça de realimentação do processo de gestão de segurança, com o propósito binário de medir os resultados alcançados pelas atividades predecessoras e de gerar novos indicadores de mudança. Através do acompanhamento de índices e indicadores de segurança definidos pelo *Security Officer*, torna-se possível perceber desvios de conduta, sobrecarga de infra-estruturas, tentativas de ataque e invasão, ineficiência dos controles implementados e, principalmente, presença de mudanças físicas, tecnológicas ou humanas que venham a provocar a oscilação do nível de segurança.

A auditoria faz parte desse universo e pode ser realizada com instrumentos automatizados e manuais. São dispositivos capazes de registrar acessos, sinalizar a transposição de perímetros, bloquear comportamentos em ambiente físico e eletrônico, bem como métodos que requerem presença física em busca de evidências materiais que denotem inadequação de ambientes, o descumprimento da política e comportamentos de risco tomados por recursos humanos. De forma complementar, ainda existem dispositivos classificados como *Policy Enforcement*, ou seja, instrumentos físicos e tecnológicos que visam forçar o cumprimento às regras definidas pela empresa, obrigando de forma impositiva que as mesmas sejam seguidas. Se há qualquer proibição de acesso a um determinado site Internet, por exemplo, e um funcionário ignora a restrição e tenta estabelecer a conexão, um software pode cumprir o papel de controlador, bloquear o acesso e, ainda, registrar a ocorrência. A propósito, o mecanismo de registro de ocorrências é ferramenta fundamental para garantir o sucesso da administração e monitoração de segurança. São ótimas fontes de informação para medir o grau de aderência dos funcionários, o índice de eficiência dos controles e, ainda, para perceber falhas de segurança que permaneceram mesmo depois dos controles implementados.

É imprescindível que o *Security Officer* identifique os controles adequados que irão gerar índices para o monitoramento, de acordo com as necessidades específicas da empresa. É bem verdade que muitos deles se aplicam a todas as empresas, mas há sempre o personalizar para atender, principalmente, às expectativas de acompanhamento dos executivos patrocinadores. Muitas vezes, dependendo do grau de maturidade do corpo diretor, esses monitoramentos geram um *Security Index* que chega a se integrar ao conjunto de índices corporativos do *Balance Score Card*.

Vale relembrar a tendência das análises de risco em orientar-se por controles de segurança, como os sugeridos pela ISO17799. Estes mesmos controles, somados aos critérios, padrões e regras definidas pela política de segurança da própria empresa, são uma ótima referência para suportar as ações de auditoria, servindo de parâmetro de conformidade. O que estaremos vendo, em breve, é a sinergia dos conceitos já empregados pela ISO9000 e seu processo de certificação de qualidade, como a norma de segurança ISO17799, também baseada em controles que irão subsidiar o Manual da Segurança, similar ao renomado Manual da Qualidade.

Knowledge Checkpoint 3

Orientação ao *Security Officer*

Solução Corporativa de Segurança da Informação

CONCEITO: “Segurança é a gestão inteligente da informação em todos os ambientes, independentemente de sua forma. Controle e Segmentação são as melhores palavras para representar este desafio”.

Plano Diretor de Segurança

CONCEITO: “A metodologia aplicada na confecção do Plano Diretor de Segurança já adota atividades de diagnóstico, porém em caráter mais estratégico e orientado às necessidades do negócio como um todo; portanto, não há conflito com a Análise de Riscos. Um PDS bem estruturado é fundamental para a coerência e a integração das atividades subsequentes do ciclo PDCA”.

Plano de Continuidade de Negócios

CONCEITO: “Para garantir a eficiência do Plano de Continuidade de Negócios é preciso construir um processo dinâmico de manutenção e gestão de todos os documentos, garantindo a integração e a eficácia em situações de desastre. Desenvolver o plano a partir de uma Análise de Riscos prévia é a melhor forma de aumentar a eficácia e o retorno sobre os investimentos”.

Política de Segurança da Informação

CONCEITO: “Forme um grupo multidisciplinar, integrando necessidades e visões distintas e enriquecedoras. Defina um processo de criação, manutenção e divulgação da política. Envolver a alta direção e inicie os trabalhos com a elaboração das diretrizes e principais normas. Comece pequeno, mas pense grande. A maturidade de segurança de uma empresa está ligada diretamente à abrangência de sua política de segurança e à disseminação de cultura por seus ativos humanos”.

Análise de Riscos e Vulnerabilidades

CONCEITO: “Para extrair todo o potencial de uma análise de riscos, é preciso considerar em seu escopo todo o espectro de ativos presentes no ambiente corporativo que, de forma direta ou indireta, suportam seus processos de negócio. Além disso, é fator crítico de sucesso mapear os relacionamentos dos processos com os ativos, pois só assim será possível gerar um diagnóstico efetivamente orientador e alinhado com os interesses da empresa”.

Teste de Invasão

CONCEITO: “O Teste de Invasão não se propõe a mapear todas as falhas de segurança, mas a experimentar a exploração de qualquer controle de segurança em busca de um ponto vulnerável, a fim de demonstrar a fragilidade da empresa. Sua qualidade está diretamente ligada à sua eficiência em reproduzir situações próximas à realidade”.

Implementação de Controles de Segurança

CONCEITO: “O sucesso da atividade de implementação de controles de segurança está diretamente ligado à etapa preliminar de dimensionamento das necessidades, projeção de impactos e, principalmente, da segmentação de perímetros físicos, tecnológicos e humanos que permitirá empregar os controles certos que ofereçam o nível de segurança mais adequado para cada situação”.

Treinamento e Sensibilização em Segurança

CONCEITO: “O nível de segurança de uma corrente é equivalente à resistência oferecida pelo elo mais fraco. O *peopleware* representa justamente esse elo; por isso, deve ser alvo de um programa contínuo e dinâmico, capaz de manter os recursos humanos motivados a contribuir,

conscientes de suas responsabilidade e preparados para agir diante de antigas e novas situações de risco”.

Equipe para Resposta a Incidentes

CONCEITO: “A segurança do negócio depende do tempo em que a empresa mantém seus ativos vulneráveis e à mercê de ameaças que podem explorá-las. Pela complexidade dos ambientes e a velocidade com que as mudanças surgem, é preciso manter ou acionar uma equipe multiespecializada capaz de agir de forma integrada e com velocidade para reduzir o tempo de exposição, minimizando os impactos”.

Administração e Monitoração de Segurança

CONCEITO: “O nível de segurança de uma organização tende a oscilar sempre que ocorrer uma mudança endógena ou exógena; por conta disso, é condição de sucesso montar um modelo de administração e monitoração de controles de segurança, formado por índices e indicadores importantes para o negócio, a fim de retroalimentar o processo de gestão coordenado pelo *Security Officer*. Esses insumos é que irão provocar mudanças de direcionamento, priorização e otimização do retorno sobre o investimento”.

Conformidade com a norma ISO17799

Para que serve uma norma ISO? Muitos de nós nunca fizemos esta pergunta, apesar de estarmos cotidianamente em contato com produtos certificados, empresas que possuem o reconhecimento de organismos certificadores e, em alguns casos, relações comerciais *business to business* que só ocorrem pela presença mútua de conformidade com determinada norma. Sendo didático, podemos dizer que uma norma tem o propósito de definir regras, padrões e instrumentos de controle que dêem uniformidade a um processo, produto ou serviço.

Mas por que é que tantas empresas buscam adesão a essas normas? Em uma economia tradicional e saudável, as empresas representam engrenagens de um sistema complexo onde há trocas constantes de bens e serviços, através da utilização da moeda, para concretizar as relações financeiras. Diante disso, é saudável que todas as empresas procurem uma base comum que facilite a interação e a confiança entre elas e, oportunamente, busquem elementos que as projetem mais, conquistando diferenciais competitivos. Essa é a lei de mercado.

As normas surgiram para sugerir bases comuns, cada qual com a sua especificidade, como vemos na ISO9001 – Qualidade e a ISO14000 – Meio Ambiente. São exemplos de critérios, padrões e instrumentos de controle, aplicáveis parcialmente ou totalmente em função da natureza de cada negócio, que acabaram formando cultura e recebendo o reconhecimento mundial de segmentos específicos.

O mercado atingiu um nível de automação, de compartilhamento de informações e de dependência tal, que motivou a elaboração e compilação de uma norma específica para orientar a padronização de uma base comum voltada para a gestão de segurança da informação. A ela dá-se o nome de BS7799: parte 1, que possui uma versão brasileira – a NBR /ISO17799:1.

A primeira parte da Norma Britânica BS7799 deu origem à versão ISO17799:1 após avaliação e proposição de pequenos ajustes. Em seguida, foi traduzida e disponibilizada pela ABNT – Associação Brasileira de Normas Técnicas. Tem o objetivo de definir na parte 1 um Código de Prática para a Gestão de Segurança da Informação. São, ao todo, 10 domínios, reunidos em 36 grupos que se desdobram em um total de 127 controles. Por se tratar de um código de prática, esta parte da norma não é objeto de certificação, mas recomenda um amplo conjunto de controles que subsidiam os responsáveis pela gestão corporativa de segurança da informação.

Domínios:

- Política de Segurança
- Segurança Organizacional
- Classificação e Controle dos Ativos de Informação
- Segurança de Pessoas
- Segurança Física e do Ambiente
- Gerenciamento das Operações e Comunicações
- Controle de acesso
- Desenvolvimento e Manutenção de Sistemas
- Gestão da Continuidade do Negócio
- Conformidade

Por ora, a parte 2 da BS7799, que especifica um *framework* de segurança chamado SGSI – Sistema de Gestão de Segurança da Informação, está em consulta pública, a fim de gerar a versão ISO correspondente, e será, quando concluída, a base para a certificação das empresas. Enquanto isso não ocorre, a alternativa é buscar a conformidade e a certificação da BS7799, que já poderia representar uma pré-certificação para a ISO17799.

É notório que uma norma não ganha respeito e adesão automática pelo simples fato de existir. O processo é lento, mas pode se tornar rápido, sobretudo quando temos em mente que, a exemplo do que aconteceu com a ISO 9001, aderir pode significar um importante diferencial competitivo para as organizações.

8.1 Framework e os controles de segurança

O *framework* de segurança definido pela parte 2 da norma britânica BS7799 estabelece um SGSI – Sistema de Gestão de Segurança da Informação que, somado ao conjunto de controles sugeridos pela primeira parte da norma, serve de objeto para a certificação. Desta forma, as empresas podem conduzir as ações de segurança sob a orientação de uma base comum proposta pela norma, além de se prepararem indiretamente para o reconhecimento de conformidade aferido por órgãos credenciados. A certificação de segurança, similar aos reflexos obtidos pela conquista da certificação de qualidade ISO9000, promove melhorias nas relações *business-to-business* e *business-to-consumer*, além de adicionar valor à empresa por representar um diferencial competitivo e uma demonstração pública do compromisso com a segurança das informações de seus clientes. Este diferencial se potencializa por estar restrito a pouco mais de 150 empresas em todo o mundo até o momento, o que demonstra a posição de destaque, inovação e maturidade da empresa certificada.

Contudo, o caminho que conduz ao reconhecimento da conformidade é longo, pouco pavimentado e requer esforços dedicados ao planejamento, seleção de controles aplicáveis e a coordenação das atividades que irão preparar o objeto da certificação. Como ocorre na prática, o objeto da certificação não precisa necessariamente ser toda a empresa, devendo começar por um escopo restrito, normalmente um processo representativo para a natureza da atividade da empresa. Assim, os trabalhos se iniciam e desdobram em seis fases principais:

- Definição das diretrizes da política de segurança
- Definição do SGSI – Sistema de Gestão de Segurança da Informação
- Execução de uma análise de riscos
- Definição de uma estrutura para gerenciamento de risco
- Seleção dos objetos de controle e os controles aplicáveis
- Preparação da Declaração de Aplicabilidade dos Controles

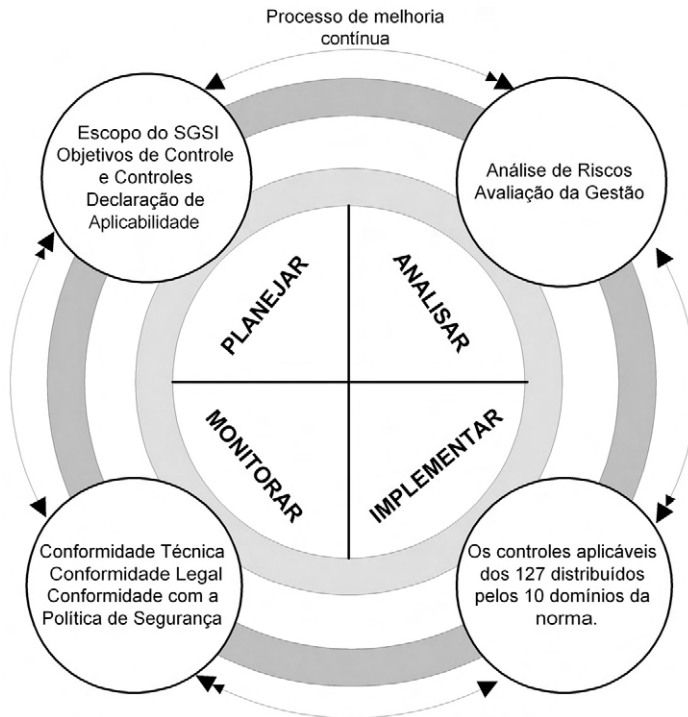


Figura 8-1 Modelo de framework SGSI – Sistema de Gestão de Segurança da Informação.

A norma representa uma trilha que orienta as empresas dispostas a se estruturar para gerir os riscos de segurança da informação; por isso, se limita a indicar o que deve ser feito sem, no entanto, dizer como deve ser feito. Pelo envolvimento de múltiplas especialidades e competências gerenciais e técnicas, recomenda-se que as empresas que se submetam à preparação para a certificação, contem com o apoio externo a fim de agregar experiências, *know-how* acumulados pela execução de outros projetos e, principalmente, pela visão isenta de vícios que adicionam qualidade ao trabalho.

Fator relevante aos responsáveis foi o direcionamento que a parte 2 da norma tomou, buscando sintonia com os padrões adotados pela norma de qualidade ISO9000. Este elemento agregou facilidade por permitir o aproveitamento das experiências vividas pelo processo de preparação, que requer o registro de controles e a construção do manual da qualidade, viabilizando a convergência das duas certificações. Diante de tantos benefícios diretos e indiretos proporcionados por esta nova certificação de segurança, e a oportunidade de fazer parte de

um grupo ainda seletivo de empresas, identifique seu nível de conformidade realizando o teste sugerido a seguir, e tome coragem para iniciar os trabalhos. Boa sorte.

8.2 Teste de conformidade

Este instrumento irá auxiliá-lo a perceber o grau de aderência de sua empresa em relação às recomendações de Segurança da Informação da norma internacional BS7799 ou de sua versão brasileira, a NBR ISO/IEC 17799. Pela superficialidade natural deste tipo de teste, poderíamos apelidá-lo de *ISO17799 Gap Analysis Light*; ou seja, um diagnóstico simples e rápido, baseado em perguntas objetivas com pontuação associada que irá revelar seu índice de conformidade.

Objetivo do Teste

Permitir a sua percepção quanto ao grau de conformidade que a organização tem em relação aos controles sugeridos pelo código de conduta de gestão de segurança da informação definidos pela norma ISO/IEC 17799.

Instruções

Escolha apenas uma resposta para cada pergunta e contabilize os pontos ao final.

Sua empresa possui:

1. POLÍTICA DE SEGURANÇA

Política de segurança?

- Sim
- Sim, porém desatualizada
- Não

Algum responsável pela gestão da política de segurança?

- Sim
- Sim, porém não está desempenhando esta função
- Não

2. SEGURANÇA ORGANIZACIONAL

Infra-estrutura de segurança da informação para gerenciar as ações corporativas?

- Sim
- Sim, porém desatualizada
- Não

Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?

- Sim
- Sim, mas não está sendo utilizado atualmente.
- Não

Definição clara das atribuições de responsabilidade associadas à segurança da informação?

- Sim
- Sim, porém desatualizada
- Não

Identificação dos riscos no acesso de prestadores de serviço?

- Sim
- Sim, porém desatualizada
- Não

Controle de acesso específico para os prestadores de serviço?

- Sim
- Sim, porém desatualizado
- Não

Requisitos de segurança dos contratos de terceirização?

- Sim
- Sim, porém desatualizados
- Não

3. CLASSIFICAÇÃO E CONTROLE DOS ATIVOS DE INFORMAÇÃO

Inventário dos ativos físicos, tecnológicos e humanos?

- Sim
- Sim, porém desatualizado
- Não

Critérios de classificação da informação?

- Sim
- Sim, porém desatualizados
- Não

4. SEGURANÇA EM PESSOAS

Critérios de seleção e política de pessoal?

- Sim
- Sim, porém desatualizados
- Não

Acordo de confidencialidade, termos e condições de trabalho?

- Sim
- Sim, porém desatualizados
- Não

Processos para capacitação e treinamento de usuários?

- Sim
- Sim, porém desatualizados
- Não

Estrutura para notificar e responder aos incidentes e falhas de segurança?

- Sim
- Sim, porém desatualizada
- Não

5. SEGURANÇA FÍSICA E DE AMBIENTE

Definição de perímetros e controles de acesso físico aos ambientes?

- Sim
- Sim, porém desatualizada
- Não

Recursos para segurança e manutenção dos equipamentos?

- Sim
- Sim, porém desatualizados
- Não

Estrutura para fornecimento adequado de energia?

- Sim
- Sim, porém desatualizada
- Não

Segurança do cabeamento?

- Sim
- Sim, porém desatualizada
- Não

6. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

Procedimentos e responsabilidades operacionais?

- Sim
- Sim, porém desatualizados
- Não

Controle de mudanças operacionais?

- Sim
- Sim, porém desatualizado
- Não

Segregação de funções e ambientes?

- Sim
- Sim, porém desatualizada
- Não

Planejamento e aceitação de sistemas?

- Sim
- Sim, porém desatualizados
- Não

Procedimentos para cópias de segurança?

- Sim
- Sim, porém desatualizados
- Não

Controles e gerenciamento de Rede?

- Sim
- Sim, porém desatualizados
- Não

Mecanismos de segurança e tratamento de mídias?

- Sim
- Sim, porém desatualizados
- Não

Procedimentos para documentação de sistemas?

- Sim
- Sim, porém desatualizados
- Não

Mecanismos de segurança do correio eletrônico?

- Sim
- Sim, porém desatualizados
- Não

7. CONTROLE DE ACESSO

Requisitos do negócio para controle de acesso?

- Sim
- Sim, porém desatualizados
- Não

Gerenciamento de acessos do usuário?

- Sim
- Sim, porém desatualizado
- Não

Controle de acesso à rede?

- Sim
- Sim, porém desatualizado
- Não

Controle de acesso ao sistema operacional?

- Sim
- Sim, porém desatualizado
- Não

Controle de acesso às aplicações?

- Sim
- Sim, porém desatualizado
- Não

Monitoração do uso e acesso ao sistema?

- Sim

- Sim, porém desatualizado
- Não

Critérios para computação móvel e trabalho remoto?

- Sim
- Sim, porém desatualizados
- Não

8. DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Requisitos de segurança de sistemas?

- Sim
- Sim, porém desatualizados
- Não

Controles de criptografia?

- Sim
- Sim, porém desatualizados
- Não

Mecanismos de segurança nos processo de desenvolvimento e suporte?

- Sim
- Sim, porém desatualizados
- Não

9. GESTÃO DA CONTINUIDADE DO NEGÓCIO

Processo de gestão da continuidade do negócio?

- Sim
- Sim, porém desatualizado
- Não

10. CONFORMIDADE

Gestão de conformidades técnicas e legais?

- Sim
- Sim, porém desatualizada
- Não

Recursos e critérios para auditoria de sistemas?

- Sim
- Sim, porém desatualizados
- Não

Tabela de pontuação

Some os pontos correspondentes às respostas de acordo com a tabela a seguir:

Resposta A: some 2 pontos Resposta B: some 1 ponto Resposta C: não some, nem subtraia pontos
--

Índices de Conformidade com a norma ISO 17799

Depois de preencher as 40 questões do teste, você deve ter notado a amplitude dos assuntos abordados pela norma e, obviamente, a complexidade em planejar, implementar e gerir todos os controle de segurança, a fim de proteger a confidencialidade, integridade e disponibilidade das informações. Fazê-lo conhecer todos os aspectos envolvidos, orientando-o a dimensionar a grandeza dos desafios são os primeiros objetivos deste exercício.

Seria ingênuo prometer com esse teste o mesmo resultado de uma análise de riscos, mas, através dos índices obtidos com a pontuação final, será possível ver o quão distante sua empresa está do que vem sendo considerado referência nacional e internacional de gestão de segurança da informação.

É bem provável que sua empresa se saia bem em um ou mais domínios. Esta situação está presente na maioria das organizações e acontece co-

mumente pela ausência de um diagnóstico abrangente e capaz de integrar o levantamento de ameaças, impactos, vulnerabilidades físicas, tecnológicas e humanas, associando-as às reais necessidades do negócio. Sem uma análise de riscos desse tipo, as ações tornam-se desorientadas, mal priorizadas, redundantes muitas vezes, e, assim, não pecam por não oferecer o retorno esperado e medido pelo nível de segurança da empresa.

Veja agora a que distância sua empresa está da conformidade com a norma.

Resultado entre 80-54

Parabéns! Sua empresa é uma exceção e deve estar em destaque em seu segmento de mercado por conta da abrangência dos controles que aplica no negócio. Apesar de não podermos ver a uniformidade das ações, distribuídas pelos 10 domínios, podemos dizer que sua empresa está conscientizada da importância da segurança para a saúde dos negócios. A situação estará ainda melhor se todas as ações e controles aplicados tiverem sido decididos com base em uma análise de riscos integrada e, ainda, sob a gestão de um *Security Officer*.

Resultado entre 53-27

Atenção! Este resultado pode ter sido alcançado de diversas formas. Sua empresa pode ter adotado quase que a totalidade dos controles, mas a maioria dos quesitos pode estar defasada, desatualizada ou inativa, o que demonstra um bom nível de consciência, mas também deficiência na estrutura de gestão ou a falta de fôlego financeiro para subsidiar os recursos de administração. Poderia, ainda, ter uma parcela representativa dos controles em ordem, deixando os demais inoperantes, ou mesmo inexistentes. Diante disso, é conveniente alertarmos para a grande possibilidade de evolução, bem como a possibilidade de estagnação e de redução tendenciosa do nível de segurança por falta de orientação. Mais uma vez, a ausência de uma análise de riscos pode ser a causa para a desorientação dos investimentos e a dificuldade de priorização das atividades.

Resultado entre 26-0

Cuidado! A situação não é confortável para a empresa. A segurança da informação não está sendo tratada como prioridade e a pontuação in-

dica a ausência ou ineficácia de muitos dos controles recomendados pela norma. As causas podem ser o desconhecimento dos riscos e a falta de sensibilização dos executivos e da alta administração. Arrisco dizer que seu segmento de mercado não vive um momento muito competitivo, ou que a segurança não seja vista por seus clientes como um fator crítico de sucesso por conta da natureza de sua atividade. Outra hipótese é que devem estar ocorrendo ações isoladas – de um departamento ou de outro – que, apesar de louváveis, não distribuem uniformemente a segurança e acabam por minimizar o aumento do nível de segurança do negócio. Apesar de tudo, não é hora de desanimar. Sempre há tempo de reverter a situação. Comece com uma análise de riscos e boa sorte.

NOTA: é importante considerar, ao obter os resultados, que os mesmos espelham um momento de mercado, um estágio evolutivo de segurança da informação; portanto, estes diagnósticos perpetuados no livro tendem a oscilar com o tempo, podendo perder sua eficácia.



Conclusões Finais

Diante deste apanhado de percepções e visões compartilhadas ao redor dos aspectos de segurança, não devemos nos enganar por achar que o tema é ingrediente novo na receita. A segurança é estudada, planejada e aplicada há décadas nas mais diversas atividades e com os mais diversos propósitos. Se fizermos um breve retorno na história, veremos épocas distintas em que os ativos, que detinham a atenção e, portanto, eram valorizados pelas empresas em seus negócios, mudavam dinamicamente.

Sem muito esforço, lembramo-nos da importância das máquinas que representavam todo o diferencial competitivo quando aplicadas na automação das linhas de produção, dos grandes armários de ferro que armazenam documentos e mais documentos, mais especificamente fichas, com todo o segredo do negócio, e agora vemos todo o valor e diferencial acumulado em arquivos eletrônicos, circulando em redes de computador cada vez mais conectadas, capilarizadas e distribuídas.

Os ativos mudaram, os valores mudaram, os pilares que sustentam os processos produtivos e operacionalizam os negócios mudaram, a forma de representar, manusear, armazenar, transportar e descartar o patrimônio da empresa também mudou e continuará mudando dinamicamente e em uma velocidade cada vez maior.

Diante disso, temos que extrair a essência valiosa de todas essas experiências, inclusive a que está sendo vivida exatamente neste mo-

mento, buscando acumulá-las para darmos continuidade ao processo – que me parece infinito, até que provem o contrário – de planejar a proteção e a administração dos riscos ligados à informação.

Independentemente das futuras transformações relacionadas aos processos, à forma e à tecnologia adotadas para promover o fluxo de dados na empresa, estes estarão sempre suportando informações que não poderão sair da nossa alça de mira.



Bibliografia recomendada

1. NBR/ISO/IEC 17799. Tecnologia da Informação: Código de prática para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas ABNT, 2002. 56 pp
2. KRAUSE TIPON, *Handbook of Information Security Management* 1999, Editora Auerback,1999.
3. HUTT, Arthur E. et al. *Computer Security Handbook*. 3rd Edition. Nova York: John Wiley & Sons, Inc., 1995.
4. RUSSEL, Deborah e GANGEMI, G.T. *Computer Security Basics*. California: O'Reilly & Associates, Inc., 1991. 441 pp.
5. VALLABHANENI, S.Rao. *CISSP Examination Texbooks. Volume 1: Theory*. Illinois: SRV Professional Publications, 1ª ed., 2000. 519 pp.
6. PARKER, Donn. *Fighting Computer Crime: a new framework for protecting information*. Nova York: Willey Computer Publishing, 1998. 512 pp.
7. GIL, Antonio de Loureiro. *Segurança em Informática*. São Paulo: Atlas, 2ª ed., 1998. 193 pp.
8. ISO/IEC JTC 1/SC 27. *Glossary of IT Security Terminology. Information technology - security techniques*. 1998.

9. SCHNEIER, Bruce. *Segurança.com: Segredos e Mentiras sobre a Proteção na Vida Digital*. Rio de Janeiro: Campus, 2001.
10. SECINF. *Glossary of Terms: Messaging and Network Security*. <http://secinf.net/info/misc/glossary.html>
11. WEBOPEDIA. *Security*. <http://webopedia.internet.com/Networks/Security/>
12. Coluna eletrônica de Gestão de Segurança da Informação da IDGNow assinada pelo autor: www.idgnow.com.br/idgnow/colunas/firewall/firewall.htm
13. Portal de Segurança da Informação da Módulo Security Solutions, a primeira empresa da América Latina certificada BS7799. www.modulo.com.br