Coletânea ABSEG de Segurança Empresarial

Volume I

Antonio Esdras de Góes Almeida
Carlos Alberto de Souza
Dagoberto Lorenzetti
Edison Fontes
Fernando Só e Silva
HUGO TISAKA
Isaac de Oliveira e Souza
José Luiz Cardoso Zamith
Mauro de Lucca
Nino Ricardo de Menezes Meireles
Tácito Leite
Vinicius Domingues Cavalcante

CRÉDITOS:

Realização: ABSEG – Associação Brasileira de Profissionais de Segurança

Projeto Gráfico e Capa: Ferracini Assessoria de Comunicação Ltda.

Organização: CN Editorial e Serviços Ltda.

Impressão e Montagem: Copbem Editora e Gráfica Ltda.

Maio/2009

APRESENTAÇÃO

A ABSEG - Associação Brasileira de Profissionais de Segurança foi constituída em 2005 com o objetivo de promover o reconhecimento, a capacitação, o aperfeiçoamento e o desenvolvimento profissional de todos os que atuam no segmento de segurança e proteção, em suas mais diversas modalidades.

Por intermédio de um permanente programa de eventos e cursos, busca promover o intercâmbio entre profissionais, associações, instituições de ensino, além de entidades nacionais e internacionais de segurança, propiciando vasto conhecimento sobre esse importante segmento da nossa sociedade e contribuindo para a sua evolução.

Esse intercâmbio permite, ainda, a informação, em tempo real, aos associados, sobre tudo o que está ocorrendo no mercado e, o mais importante, tendo na própria rede de contatos da associação, a solução de dúvidas e o apoio aos mais diversos problemas encontrados no dia a dia do profissional de segurança.

A geração de conhecimento na área de segurança em nosso país é intensa, em todos os aspectos, da segurança física à segurança digital, passando pela pública, do trabalho, pessoal, de informações e outras, e é preciso tornar esse conhecimento disponível para os profissionais que atuam na área, independentemente de sua localização geográfica ou área de atuação.

Por todos estes motivos, a ABSEG lança o primeiro volume da "Coletânea ABSEG de Segurança Empresarial".

Constituída de textos elaborados por renomados profissionais de segurança de nosso país, a Coletânea ABSEG de Segurança Empresarial, além de levar conhecimento a nosso mercado, é uma forma de prestigiar os profissionais que tanto contribuem para nosso segmento, dando-lhes a oportunidade de ter seus ensinamentos, estudos e experiências publicadas em um livro.

Todo profissional de segurança atualizado sabe da importância de seu trabalho para a manutenção e para a continuidade dos negócios das empresas a que, direta ou indiretamente, presta serviços. Quanto mais preparadas estiverem as equipes e mais integrados todos os sistemas de segurança, menores serão as perdas dessas empresas, em suas diversas áreas, melhorando consideravelmente seu potencial competitivo.

É fundamental que o profissional de segurança esteja preparado para enfrentar o desafio de "vender" bem seu trabalho, convencendo os empresários - alguns ainda céticos - da importância da gestão de segurança nas corporações, e atuando com ética e competência para garantir seu espaço e consolidar sua profissão.

A ABSEG espera estar contribuindo para que isso aconteça!

Tatiana Diniz
Presidente da ABSEG

SUMÁRIO

Controle de Acesso e Segurança

Antonio Esdras de Góes Almeida

É incontestável que o controle de acesso é uma das mais importantes ferramentas de apoio à segurança de instalações, pessoas e patrimônio. Ele pode ser obtido através de:

- design do ambiente,
- barreiras de canalização do fluxo para pontos controlados,
- mecanismos de identificação (credenciais com foto ou com código de barras e leitoras integradas a algum sistema),
- sinalização e avisos,
- equipamentos de ação mecânica (portões, portas, fechaduras...),
- dispositivos eletrônicos (com ou sem bloqueio físico),
- fiscalização humana, que também precisa estar combinada com todas as outras opções.

Na maioria dos casos em que as instalações requerem um nível elevado de segurança, a solução mais indicada é a combinação de várias das opções citadas acima. Quanto maior o fluxo de pessoas e /ou veículos, maior será a necessidade de controle de acesso eletrônico para garantir restrições automáticas, monitoramento e controle.

Neste artigo, focaremos os aspectos relacionados ao controle de acesso eletrônico, que é o mais indicado quando prevalecem as demandas de segurança, quando é grande o número de pessoas a serem controladas ou quando existem possibilidades de burla dos mecanismos de controle convencionais. Procuraremos evitar uso de terminologia técnica e expor as questões usando uma linguagem que facilite a compreensão de usuários.

O controle de acesso eletrônico é obtido através de "placas eletrônicas" (semelhantes às CPU de microcomputadores) que são programadas via software para controlar e monitorar diferentes tipos de bloqueio físico (catracas, torniquetes, portas com fechaduras eletrônicas, cancelas etc.), restringindo o acesso de pessoas previamente cadastradas e negando acesso a pessoas não cadastradas ou não autorizadas.

Particularmente, eu defendo a teoria de que não existe uma referência única ou uma "receita de bolo" que se aplique a todos os tipos de instalações, pois variam muito as necessidades de segurança, os fluxos nos horários de pico, os tempos de resposta dos equipamentos e tecnologias de comunicação e leitura / validação utilizadas.

Procure usar a tecnologia a seu favor para:

- aumentar a eficiência da segurança;
- gerar informações;
- automatizar ações;
- gerar dados para investigações;
- permitir gestão remota;
- prevenir e inibir ocorrência de sinistros.

"Catracas Virtuais"

Existem equipamentos que fazem o controle de acesso sem o bloqueio físico, que normalmente usam sensores infravermelhos ativos para detectar e sinalizam, através de dispositivos visuais e sonoros, a passagem de pessoas não autorizadas ou que passaram sem apresentar a sua credencial na leitora. A desvantagem no uso deste tipo de equipamento, é que a sinalização do acesso não autorizado ocorre durante ou após a passagem pelo equipamento, sendo necessário contar com o recuo espontâneo do intruso ou com uma ação humana, para retirar a pessoa não autorizada da referida área. Assim sendo, esse tipo de equipamento não impede os acessos não autorizados, ele apenas intimida e inibe a tentativa de intrusões.

CFTV

Normalmente as catracas e portas convencionais com fechadura eletrônica não impedem a passagem do "carona", ou no

caso das catracas convencionais, a burla, passando por cima ou por baixo da haste de bloqueio.

Outro tipo de burla que ocorre no controle de acesso eletrônico é a utilização de crachás de terceiros para liberação do bloqueio. Dessa forma, para reduzirmos esses tipos de vulnerabilidades e inibir efetivamente as burlas, faz-se necessário combinar os dispositivos de controle de acesso com a fiscalização humana e a instalação de fiscalização eletrônica com Circuito Fechado de Televisão. Atualmente já existem sistemas de CFTV que fazem o reconhecimento de face e de placas e que podem até realizar ações, ao reconhecerem um registro existente na base de dados, como liberar a abertura de uma cancela, catraca ou fechadura eletrônica. Trata-se de uma tecnologia relativamente nova e que requer o atendimento de alguns requisitos, como o correto posicionamento das câmeras. Ainda neste artigo trataremos das tecnologias de identificação / validação biométrica e passaremos informação sobre o seu desempenho.

Tendência Futura de Automação do Processo de Identificação

Pelo que podemos perceber neste momento, é bem provável que, no futuro, as nossas informações pessoais e complementares (como foto e impressão digital), sejam armazenadas em um único smart card. Assim sendo, terminais de auto-atendimento em portarias poderiam extrair alguns dados básicos e validar que se trata de uma identificação oficial e que o visitante da instalação realmente é o dono do referido documento. Através desse mesmo terminal de auto-atendimento poder-se-á contatar o visitado que, ao autorizar a visita por um telefone ou micro, estará registrando no sistema de controle de acesso e / ou no próprio smart card a permissão temporária de acesso para aquela visita, indicando por quais bloqueios físicos com controle eletrônico o visitante poderá passar e até que horário.

Ação Humana

Por mais tecnologia que seja empregada no controle de acesso, a ação humana na interação com os sistemas, seja para carregar dados, fazer autorizações, monitorar tentativas de burla ou extrair informações, é indispensável.

A presença física da segurança também é essencial para fiscalizar, orientar o público e inibir burlas no controle de acesso.

Equilíbrio entre necessidades de Segurança e de Operação

Para garantir o sucesso da implantação do controle de acesso eletrônico faz-se necessário considerar, também, as demandas da operação, para que a organização tenha o incremento desejado de segurança, sem causar sérios transtornos à operação.

Convém lembrar, ainda, de não bloquear tanto os acessos e saídas de emergência, de modo que impeçam a desocupação rápida das edificações em casos de incêndio e emergências.

Outro aspecto relevante que deve ser considerado no projeto de controle de acesso são os acessos para deficientes físicos, que devem ser projetados (principalmente nas portarias de prédios), considerando a utilização de portas auxiliares, que servirão também para outras finalidades, como passagem de carga e apoio à evasão do prédio, no caso de necessidade de evasões em função de emergências.

Normas e Procedimentos

Para comunicar adequadamente aos membros da organização e evitar questionamentos ou conflitos durante a operação, convém avaliar previamente todo o processo e documentar normas e procedimentos de controle de acesso, que devem ser validadas e aprovadas pela alta gestão, para garantir a aceitação por todos os níveis hierárquicos da organização.

Dependendo do porte da organização e complexidade do procedimento e restrições pode ser indicada a criação de um comitê de segurança, para deliberar sobre as ocorrências do período e propor melhorias nas normas e procedimentos.

Tecnologias de Comunicação

Atualmente, no controle de acesso, a comunicação entre os equipamentos e a unidade centralizadora se faz através de protocolo de comunicação TCP/IP (padrão de redes ethernet – de microcomputadores) ou RS 485 que usa pares de fios e

protocolo proprietário do fabricante.

A comunicação TCP/IP tem a vantagem de poder operar em grandes distâncias, em redes sem fio e até em redes remotas conectadas por links de dados, mas fica mais vulnerável a interferências e problemas de performance, por causa da concorrência e tráfego de outras informações na mesma rede.

Leitoras e Crachás de Identificação

Entre as tecnologias de crachás e de leitoras disponíveis no mercado, vêm prevalecendo o uso de código de barras em função do menor investimento, bem como as tecnologias de leitura sem contato (proximidade, smart card, RFID), por serem mais seguras e funcionais (principalmente no caso de identificação de motoristas embarcados, ao se identificarem para ter acesso através de cancelas).

Por ter a possibilidade de incorporar outras aplicações (convênios, benefícios...), pela segurança que pode oferecer contra cópias e pela possibilidade de gravar informações adicionais no cartão, como permissão de acesso, validade do cartão, etc., as leitoras e crachás smart card, sem contato, vêm aumentando significativamente a sua participação no mercado nos últimos anos e sendo a preferida pelos profissionais que lidam com tecnologia.

Uso de Biometria

O uso de dispositivos de identificação biométrica, associada a equipamentos de controle de acesso eletrônico, está cada vez mais frequente, até em locais onde o seu uso não é indispensável.

O que se deve considerar na opção pelo uso da biometria é que ela é um eficiente recurso de identificação ou de validação do usuário do crachá, recomendado para áreas de acesso restrito, onde os requisitos de segurança são elevados.

Para evitar transtornos para a operação, o uso de leitoras biométricas deve ser evitado em catracas de visitantes localizadas em portarias com grande fluxo de pedestres, ou em controladores de cancelas, principalmente se o fluxo de veículos for intenso, pois o processo de identificação e de cadastro é mais lento, em função dos requisitos de segurança exigidos.

Outras recomendações básicas são: fazer um piloto para testes de desempenho dos equipamentos e sistema (normalmente com um grupo reduzido de pessoas; pode ser a equipe de TI), adotar o tipo de biometria adequado para o uso proposto, criar condições adequadas para a identificação (iluminação, ruído, apoio...), definir procedimentos para tratar falhas no processo de identificação (bloqueio indevido), treinar e acompanhar a operação dos usuários.

Quadro comparativo do desempenho das diferentes tecnologias de identificação biométrica usadas no controle de acesso eletrônico:

	Digital	Mão	Face	Íris	Retina	Voz
Pode Mudar?	***	**	**	***	**	*
É Único?	***	**	*	***	***	*
Não Intrusiva?	***	***	***	**	*	***
Dificuldade de Copiar	**	**	**	***	***	*
É Precisa?	**	**	*	***	***	*
É Aceito?	***	***	**	*	*	***
Interferência do Ambiente	**	***	**	**	**	*

**** Baixo Desempenho*** ***** Médio Desempenho*** ****** Alto Desempenho***

Neste quadro, não incluímos o item de comparação "valor do investimento", em função das variações existentes de qualidade, tecnologia de leitura, fabricante, garantia, etc. De qualquer modo, a relação entre desempenho e investimento das leitoras de impressão digital é que tem garantido a sua preferência no uso em sistemas de controle de acesso eletrônico.

Benefícios

São benefícios esperados com a implantação de um bom sistema de controle de acesso eletrônico:

• maior disponibilidade das informações;

• maior segurança na identificação dos usuários;

• identificação da burla em tempo real (monitoramento);

• criação de imagem diferenciada da organização no tratamento da segurança;

• maior poder de intimidação do possível infrator;

• maior segurança (redundância do controle e fiscalização – humano e eletrônico);

• processos automáticos e eliminação de retrabalhos.

Planejamento

Devemos considerar em nosso planejamento de implantação de um sistema de controle de acesso:

• viabilidade econômica da solução em relação ao orçamento de segurança;

• adequação e proporção - adotar tecnologia adequada à aplicação desejada e na medida certa, que atenda aos fluxos e requisitos de segurança;

• possibilidade técnica – de se atingir os objetivos almejados com a solução escolhida;

• transtornos para a operação – o sistema não deve impedir ou criar grandes transtornos para operação;

• aplicação política – as restrições definidas pelo procedimento para a solução de controle de acesso devem considerar e evitar problemas no bloqueio de autoridades ou tratamento diferenciado, que possa caracterizar discriminação;

• princípios do Planejamento de Segurança (Dispositivo, Segredo, Informação);

• importância da Prevenção – procurar inibir a intrusão para reduzir a demanda de reação;

• Análise dos Riscos – através dela poderemos priorizar os recursos em função da vulnerabilidade, probabilidade e perda possível;

• revisão do layout e adequação da estrutura das portarias de pedestre e de veículos, para suportar uma operação adequada, otimizar o desempenho dos equipamentos e evitar desconfortos, filas exageradas ou retenções indesejadas;

• suporte local à tecnologia escolhida – evitar pioneirismos e buscar garantias de que a assistência técnica local tem estrutura adequada e agilidade para o atendimento de problemas técnicos.

As principais dificuldades na contratação de uma solução de controle de acesso eletrônico normalmente são:

1. Falta de conhecimento do mercado, dos fornecedores e dos produtos pelo contratante, uma vez que os equipamentos têm vida útil relativamente longa e as aquisições de equipamentos não acontecem com muita frequência;

2. É relativamente grande o número de fornecedores no mercado, com belos discursos técnicos, destacando as vantagens de suas tecnologias;

3. Nem sempre a assistência técnica local dispõe de recursos adequados para atendimento ágil, em campo ou laboratório próprio;

4. Pouco compromisso de longo prazo de alguns fornecedores - muitas vezes o proponente se foca na venda dos equipamentos e não nas necessidades atuais e futuras do cliente;

5. Nem todos os sistemas oferecem facilidade de integração com outras aplicações ou cadastro (gerando algum retrabalho na sua operação);

6. Muitas vezes, aspectos relevantes na escolha da solução são omitidos pelo proponente;

7. Os investimentos e os riscos de insucesso são relativamente altos.

Ações para viabilizar o Sucesso na Implantação:

1. Fazer o planejamento interno e contratar um projeto de um especialista;

2. Definir uma equipe interna de projeto e de operação e alocar a sua disponibilidade, para garantir a implantação e uso adequado do sistema;

3. Definir os recursos a serem utilizados (pessoal, equipamentos, sistemas...);

4. Avaliar criteriosamente os fornecedores e clientes já atendidos pelos proponentes;

5. Definir e divulgar os procedimentos a serem implementados junto com o sistema;

6. Fazer o endomarketing, divulgando os benefícios e resultados esperados com a implantação;

7. Desenvolver sinalização de apoio adequada (ordenar o fluxo, indicar áreas de acesso restrito, indicar procedimentos para os visitantes...);

8. Preparar uma boa infraestrutura de hardware, software, comunicação e alimentação elétrica;

9. Implementar o projeto que foi elaborado;

10. Gerenciar o processo de mudança;

11. Evitar pioneirismos na tecnologia a ser utilizada;

12. Atentar para a qualidade da assistência técnica local;

13. Assegurar a manutenção e o uso da solução;

14. Revisar e atualizar o sistema e os procedimentos.

Como pudemos observar, são muitas as variáveis, os riscos e os fatores críticos de sucesso envolvidos; por isso, faz-se necessário um planejamento adequado e considerar as recomendações descritas neste artigo.

Não chegamos a tratar do assunto proposto em sua plenitude e nem entramos em maiores detalhes técnicos, porque acabaríamos estendendo demais o conteúdo, mas esperamos que a nossa abordagem resumida tenha sido esclarecedora e proveitosa para os interessados no assunto.

Antonio Esdras de Góes Almeida, CPP

Administrador de Empresa, com diversos cursos de extensão, Especialista em Dirección y Gestión de Seguridad en Empresas pela Universidad Pontifícia Comillas de Madrid e curso avançado de Desenvolvimento de Dirigentes pela Fundação Dom Cabral.

CPP – Certified Protection Professional pela American Society for Industrial Security(ASIS) desde 2003. Oficial R/2 – 1° Ten – Comandante de Pelotões e de Companhia, possui vasta experiência como Consultor, Coord. Projetos, Diretor Comercial, Diretor Técnico, Diretor Operações em áreas de segurança. Habilidades Especialista em Sistemas de Controle de Acesso e Segurança Eletrônica, Sistemas Administrativos e de Gestão Empresarial.

Palestrante de diversos temas relacionados à Segurança e Gestão.

A Contra-Inteligência no Cotidiano Empresarial

Carlos Alberto de Souza

Certo dia um amigo me contou uma história muito interessante a respeito de uma consultoria de segurança por ele realizada em uma importante empresa de Campinas/SP. Ao ser questionado pelo Diretor de T.I., responsável pela Segurança da Informação do grupo e avesso à consultorias externas, sobre o histórico de resultados obtidos pelo consultor, meu amigo respondeu que não estava autorizado a divulgar tais dados, por questões óbvias (preservar as empresas auditadas). Entretanto, meu amigo lançou um desafio ao diretor contrariado:

"Em dois dias de trabalho lhe apresentarei um relatório, no qual transcorrerei sobre as oportunidades de melhorias de sua empresa. Com base nos dados fornecidos, o senhor decidirá a respeito da contratação dos meus préstimos."

O Diretor concordou e o consultor partiu para a ação. Conversou com alguns funcionários e logo ficou sabendo que seria realizada uma confraternização em um clube da cidade para comemorar as metas atingidas pela empresa. Por ter conhecimento de algumas técnicas operacionais de Inteligência, meu amigo acessou com certa facilidade o evento, no qual identificou as pessoas influentes da empresa, seus familiares, veículos, endereços, telefones, dentre outros dados sensíveis, que não recebiam a devida proteção por parte de seus detentores. Além disso, com as informações obtidas na festa, levantou os itinerários e locais da escola das crianças, fotografou a rotina das famílias e gravou algumas conversas interessantes de funcionários das residências dos empresários.

Após 48 horas de trabalhos intensos, retornou à empresa e apresentou o material ao Diretor de T.I., que ficou estupefato...

Tal relato nos leva a refletir sobre o nível de segurança que desejamos estabelecer em nossas empresas, para que possamos avaliar os investimentos necessários e as áreas a serem protegidas, em ordem de prioridade, conforme o grau de criticidade obtido a partir de uma detalhada análise de riscos.

A Contra-Inteligência insere-se neste contexto no que tange à análise dos dados levantados pela Inteligência Operacional. Ela é uma ciência que mensura e reage às ameaças, vulnerabilidades, riscos, impactos e medidas necessárias a mitigar e até eliminar o efeito dos perigos que possam afetar os processos de determinada organização. O investimento necessário será estabelecido na fase do Planejamento Estratégico, a partir da elaboração dos Planos de Ação que detalharão o COMO FAZER.

A Segurança Estratégica de uma organização, que a Contra-Inteligência preconiza como Segurança Orgânica, deve abranger todos os processos organizacionais que são operacionalizados, a partir dos Procedimentos Operacionais Padrão (POP).

Fica bastante evidente a necessidade da participação e o comprometimento de todas as pessoas que participam, direta ou indiretamente, dos processos organizacionais que garantem a continuidade do negócio.

O Empresário proativo consegue antever a necessidade de implementar medidas de Contra-Inteligência capazes de, com oportunidade, alertar os responsáveis pela Segurança Operacional quanto a iminência de riscos de qualquer natureza, que possam afetar e até mesmo inviabilizar os negócios do empreendimento.

A análise de situação de Contra-Inteligência deve ser parte integrante do Planejamento Estratégico, pois ela orientará, por exemplo, quanto ao melhor posicionamento de câmeras de vigilância, que tipo de equipamento de controle de acesso condiz com a realidade da empresa, aos dados referentes a intempéries, ao melhor posicionamento geográfico de instalações etc, tudo com o objetivo de otimizar os investimentos relativos à Segurança Orgânica do empreendimento.

Uma área extremamente sensível e que merece destaque é a Segurança da Informação dos Meios de Tecnologia da Informação. A análise de Contra-Inteligência abrange, neste caso, até mesmo a seleção das pessoas da empresa que terão acesso às informações sensíveis, que possam, em caso de vazamento, impactar na produtividade e nos lucros do grupo.

Uma demonstração em um seminário promovido pela Comunidade de Inteligência Policial e Análise Evidencial (CIPAE) em 2008 gerou polêmica entre os presentes:

"Com apenas um celular nas mãos, o presidente da Companhia SecurStar, Wilfried Hafner, foi capaz de grampear conversas telefônicas, acessar dados de outros aparelhos e usar os celulares grampeados como microfones para escutas ambientais."

Usando um vírus enviado por meio de mensagem de texto, Hafner pode grampear qualquer telefone celular – basta possuir

o número do aparelho. O programa espião chamado RexSpy foi desenvolvido por sua empresa para mostrar a vulnerabilidade do sistema de telefonia celular. De acordo com ele, versões similares do vírus circulam pela internet em comunidades de hackers, principalmente na China e Coréia do Sul.

Sua empresa, que trabalha no ramo de segurança de dados e produz software para criptografar ligações, tornando-as seguras, identificou ataques de vírus similares ao RexSpy no Brasil. A primeira incidência se deu em agosto de 2008.

Ao receber o vírus, o telefone infectado sequer alerta para a chegada da mensagem. A partir de então, o "espião" passa a ter acesso a todos os dados do aparelho, como a agenda telefônica, mensagens de texto, fotos e vídeos. Além disso, o telefone que enviou o vírus recebe uma mensagem cada vez que o aparelho grampeado é usado, permitindo ouvir ou gravar as conversas realizadas.

Também sem deixar pistas, é possível que o "espião" use o celular infectado como microfone, ouvindo conversas de reuniões privadas, bastando que o aparelho infectado esteja no recinto. Todas as modalidades de grampo foram apresentadas durante o evento.

"Temos identificado o uso de vírus semelhantes ao RexSpy para espionagem industrial. A primeira vez que descobrimos uma tentativa de invasão foi em abril de 2008, na França. No Brasil, percebemos a tentativa em agosto de 2008", disse.

A Contra-Inteligência precisa ser entendida como uma ferramenta eficaz de assessoria, pois ela funciona como verdadeira guardiã de todo e qualquer sistema. No exemplo acima, o papel da Contra-Inteligência inicia com a prevenção, alertando os usuários dos sistemas sobre os riscos inerentes a cada processo desenvolvido, e termina com a análise conclusiva sobre os meios disponíveis para a completa extinção dos perigos.

TC EB Carlos Alberto de Souza

- ***BACHAREL EM CIÊNCIAS MILITARES PELA ACADEMIA MILITAR DAS AGULHAS NEGRAS***
- ***MESTRE EM APLICAÇÕES MILITARES PELO EXÉRCITO BRASILEIRO***
- ***ESPECIALISTA EM INTELIGÊNCIA MILITAR PELA ESCOLA DE INTELIGÊNCIA DO EXÉRCITO***
- ***ESPECIALISTA EM ATUALIZAÇÃO PEDAGÓGICA PELA UFRJ***
- ***MBS EM SEGURANÇA EMPRESARIAL PELO BRASILIANO E FECAP***
- ***PROFESSOR DO CURSO DE PÓS-GRADUAÇÃO EM INTELIGÊNCIA E CONTRA-INTELIGÊNCIA DO PITÁGORAS DE BELO HORIZONTE/MG***
- ***PROFESSOR DO CURSO DE GESTÃO EM SEGURANÇA EMPRESARIAL DA UNICID***

Engenharia de Processos e Gestão da Segurança Empresarial

Dagoberto Lorenzetti e Fernando Só e Silva

Embora estejam alardeando que o mercado de segurança patrimonial está se beneficiando com a insegurança crescente no Brasil, muito provavelmente por consequência do modelo econômico vigente no país, as grandes oportunidades neste mercado estão concentradas em poucas empresas. Para a maioria das empresas do setor, a situação de competição é análoga ao que se pode definir como maturidade de mercado, aliada ao fato de praticamente não existirem barreiras para novos "entrantes" (novas empresas), o que acirra ainda mais a competição. Para esse grupo de empresas prestadoras de serviços de segurança patrimonial, dificilmente criam-se grandes oportunidades; o mercado já esta posto, com as boas oportunidades que aparecem para a captura de novos clientes sendo advindas do processo competitivo acirrado. Algumas vezes, pela saída de um concorrente, por má administração de seus serviços e/ou por insatisfação do cliente com o serviço ofertado. Outras vezes, podendo ser resultado da bancarrota de um concorrente, como se vê de tempos em tempos, ou pela oferta de um concorrente com os preços um pouco mais baratos, etc.

Na situação de pouco crescimento, com o mercado na fase análoga à "maturidade", as participações de mercado chegam a uma certa rigidez e a concorrência chega a uma situação de impasse. Os preços são basicamente os mesmos, os benefícios prometidos são parecidos, sendo as expectativas e ideias dos clientes, a respeito dos serviços, de certa forma, também enrijecidas, não conseguindo esses enxergarem onde a grande quantidade de empresas que lhes oferta propostas de serviços se diferencia. Neste ponto, o ambiente está propício para o desarranjo da competição, com os chamados "mergulhos" (reduções drásticas de preços), praticados por empresas desestruturadas gerencialmente, com objetivos somente de "fazer caixa" com a captura de algum cliente e quebra da inércia vigente. Esta estratégia poderá se constituir num fato extremamente negativo para o setor e/ou para um grupo de empresas, pois representa, na maioria das vezes, a oferta de serviços que não cobrem os custos. Por outro lado, tais ações poderão também acelerar o fenômeno conhecido por "destruição criativa" (expressão cunhada pelo economista clássico Schumpeter, para fases econômicas em que parte do setor sucumbe, para dar surgimento a outro mais vigoroso). Tal situação nos parece estar sendo também vivenciada por parte do setor de segurança patrimonial, como já foi, e talvez ainda seja realidade, em vários outros setores da economia brasileira, consequências da exaustão do modelo econômico vigente, globalização, da abertura de mercado e mais recentemente, fruto da valorização do Real frente ao Dólar.

Desta forma, sempre que nos são dadas oportunidades de expressar nossas ideias sobre gestão, destacamos a necessidade de se trazer mais engenharia para o setor de segurança patrimonial, não no sentido do profissional engenheiro, mas no sentido das atividades de engenharia. O "engenheirar", no sentido da ciência aplicada, no aprender a aprender sobre os sistemas operacionais vigentes, sobre os fundamentos da qualidade em serviços, na inovação, na melhoria contínua, no como medir o desempenho, no como competir, etc. No caso deste artigo, mais uma vez trazemos o tema "engenharia de processos", pelo qual a organização pode ter o mapeamento de suas atividades produtivas (seus processos) e a determinação precisa de seus resultados. Este método permite o monitoramento da operação da organização, através de um sistema de indicadores de desempenho, "engenheirando", assim, as partes fundamentais de uma estratégia inovadora, indicada para o ambiente de competição acirrada.

Na estrutura funcional usada nos modelos de gestão conservadores, como é o caso do setor de segurança patrimonial, é delimitada, a priori, a função de cada colaborador, por meio das descrições dos cargos, fazendo com que esses se encaixem nos cargos, e as pessoas que pensam e controlam fiquem separadas das que fazem. Na gestão por processos, diferentemente da estrutura funcional, o que importa é o colaborador ter a compreensão dos processos e estar apto para exercer, em suas atividades, a "transformação" dos recursos que são fornecidos, em recursos "processados" (a entrega do serviço). No caso do departamento operacional de uma empresa de serviços de segurança patrimonial, um bom exemplo de "transformação" de recursos, tem-se o caso do recebimento de um pedido de implantação de posto vindo do comercial, para o qual serão especificados os recursos materiais e humanos e os meios administrativos. Como resultado da "transformação" dos recursos, tem-se a implantação, de acordo com as especificações do que foi vendido e as expectativas do cliente.

Outro ponto importante no setor é o emprego da tecnologia da informação (inclusa na segurança eletrônica), que ocupa espaço cada vez mais relevante. Sistemas de proteção, com o emprego da TI e outras tecnologias, além de complementarem a segurança com recursos humanos, podem representar reduções consideráveis de custos, de forma que, hoje em dia, é impensável não aplicá-los. Nos países desenvolvidos, o emprego da tecnologia na proteção patrimonial pode variar entre 30% e 100%

do total aplicado. Para a obtenção de resultados efetivos com o uso da TI, em geral, e como instrumento de aperfeiçoamento da ação humana, segundo os especialistas, são necessários os "meios organizacionais", outra denominação para os processos, que permitirão a integração entre a tecnologia e os recursos humanos aplicados. O homem de segurança, operando um sistema de segurança eletrônica, deve saber o que fazer ao receber, por exemplo, o disparo de um botão de pânico, vindo por uma conexão GPRS, trafegando via Web, num protocolo TCP/IP, instalado num de seus clientes. Da mesma forma, deve ser instruído sobre suas atividades, quando recebe a determinação de fazer ronda em seu turno, utilizando o sistema de controle eletrônico de rondas (bastão de ronda).

Sob o ponto de vista do cliente que contrata os serviços de segurança empresarial, as perspectivas são alvissareiras. A abordagem atual contempla o mapeamento minucioso dos processos de transformação do cliente (seus meios e formas de produção) e posterior auditoria, sob a ótica dos riscos e vulnerabilidades. Fica, então, facultada à alta gestão da empresa contratante, decidir a que níveis de riscos e com quais vulnerabilidades estará disposta a operar. Os sistemas de proteção e as especificações dos serviços de segurança patrimonial ofertados por empresas prestadoras desses serviços serão, cada vez mais, balizados sob essa perspectiva.

Assim é importante, tanto para os profissionais das empresas contratantes, quanto das provedoras de serviços de segurança empresarial, desenvolver familiaridade com alguns conceitos e abordagens da área de engenharia de processos aqui apresentados. Os métodos utilizados buscam garantir a qualidade dos serviços prestados (seu desempenho) e permitem identificar, quantificar e determinar os custos dos recursos a empregar. Trazem contribuição significativa, tanto por propiciar uma disciplina de trabalho, quanto por viabilizar o mapeamento de toda a organização. Os conhecimentos em segurança complementarão, então, a metodologia de processos, com sua abordagem de riscos, sistemas de proteção e vulnerabilidades.

Qualidade

No mundo da economia globalizada, qualidade é essencial. Na área de segurança empresarial, particularmente após o episódio de 11 de setembro de 2001 (atentado terrorista ao WTC) em Nova York, a importância da qualidade nos serviços de segurança tornou-se um fator ainda mais evidente e importante. Da qualidade dos serviços prestados, amiúde, dependem vidas humanas. Infelizmente, no caso brasileiro, a qualidade na maioria dos serviços de segurança empresarial deixa a desejar. Muitas vezes até por falta da compreensão, por parte dos gestores, do seu significado. Resta lembrar que, no Brasil, esta é uma indústria incipiente, de certa forma carente em métodos de gestão e, principalmente, não está, ainda, submetida à concorrência de empresas globais. O mercado brasileiro de segurança é vedado à atuação de empresas estrangeiras. Obviamente, há diversas empresas brasileiras de serviços de segurança patrimonial bem estruturadas, com padrões de excelência, com serviços de altíssima qualidade e que não se encaixam nessa classificação. Mas a exceção parece confirmar a regra.

Um perfeito entrosamento entre as áreas afetadas diretamente pela segurança empresarial e os demais departamentos e áreas das organizações pode ser obtido com uma competente aplicação dos conceitos da gestão da qualidade. Qualidade começa e termina no cliente. Começa e termina com o aprendizado. Por exemplo, a disponibilidade é um item de qualidade em serviços (JURAN, Gryna; Controle de Qualidade – Conceitos, Políticas e Filosofia da Qualidade – Makron Books Ed., São Paulo – 1991) da mais alta importância. Disponibilidade pode ser entendida como um conceito da área de confiabilidade, com viés técnico, ou como "estar à disposição". Produtos que não chegam aos clientes por falhas na segurança impactam diretamente as relações cliente-fornecedor, a imagem da empresa, as receitas e os lucros.

Ainda que possa parecer um conceito suficientemente difundido no meio empresarial, o uso da palavra "qualidade", frequentemente, contribui para complicar a comunicação. Provedores e clientes podem ter percepções peculiares. Se a pergunta "O que é qualidade?" for feita para n diferentes pessoas, serão dadas, quase certamente, n respostas diferentes. As pessoas conversam sobre qualidade como se estivessem falando da mesma coisa. Na verdade, cada uma está pensando num conceito diferente. É comum que até mesmo gerentes e pesquisadores tenham dificuldade para utilizar o conceito. Um profissional pode estar usando o termo no sentido lato e outro pode estar entendendo o vocábulo "qualidade" num sentido bastante restrito do termo.

Além da "excelência inerente", indefinível, mas apreensível, "qualidade" deve ser entendida como "conformidade com especificações", "adequação aos usos previstos para o produto/serviços" e até "valor ao cliente". Pode ainda significar "valor para todas as partes interessadas", ou, conforme definição da de Norma ISO, baseada na definição de Armand Valin Feigenbaun, criador da sigla TQC (Controle de Qualidade Total), "a totalidade dos aspectos e características de um produto ou serviço, relacionado à sua capacidade de satisfazer as necessidades declaradas ou implícitas de seus consumidores".

Analisando-se o arrazoado de definições acima, podemos identificar diversos conceitos, entre os quais salientamos: adequação ao uso ou ao objetivo; relação custo-benefício; confiabilidade; satisfação do cliente; conformidade aos requisitos etc.

Podemos ir ainda mais longe nas questões da qualidade e afirmar que o desenvolvimento de programas de garantia de qualidade para os serviços de segurança é uma necessidade em termos de eficácia (fazer o que o cliente quer) e eficiência (fazer certo o que o cliente quer) e, de certa forma, uma obrigação em termos éticos e morais, principalmente quando se trata de segurança contra os riscos que ameaçam a vida humana e o meio ambiente. Ensina-nos Maslow, em sua conhecida escala de necessidades dos seres humanos, que segurança é a segunda necessidade básica, e está logo acima das necessidades fisiológicas.

A qualidade total, ou seja, o foco no cliente, a adoção da filosofia de aperfeiçoamento constante das operações (dos produtos e serviços) e o respeito às partes interessadas, é um caminho que poderá diferenciar empresas de serviços de segurança, tanto em nosso mercado que, de certa forma, encontra-se em estágio primevo de maturidade, quanto em países do primeiro mundo. Nas condições vigentes, em muito mercados atuais, os preços pouco diferem, os pacotes de serviços ofertados são praticamente os mesmos. A qualidade dos serviços prestados é, geralmente, o fator de diferenciação entre as organizações. Buscar a excelência pode e deve tornar-se parte essencial da filosofia da organização e parte de sua estratégia competitiva, sendo a aplicação dos conhecimentos da gestão por processos um grande facilitador para a implementação de um programa de qualidade competente.

Processos

Processos estão relacionados com a maneira de agir, um conjunto de atos pelos quais se realiza uma operação. É qualquer atividade que recebe uma entrada (input), agrega-lhe valor e gera uma saída (output), para um cliente interno ou externo. Conhecer o processo de produção é, em última análise, definir o que é feito para transformar entradas em saídas, e que a partir do uso de recursos da própria empresa serão gerados os resultados (VARVAKIS, Gregório; Gerenciamento de Processos, Grupo de Análise de Valor – UFSC – 1999).

FIGURA 1 - REPRESENTAÇÃO DE UM FLUXO DE PROCESSO

Ainda, segundo o Prof. Varvakis (1999), uma boa definição para processos, que é adequada ao emprego no setor de serviços de segurança patrimonial, pode ser "o conjunto de recursos e atividades empregados sob determinadas condições e que são submetidos a transformações, gerando um determinado efeito final, com consequências desejadas". Exemplos de processos, na operação de serviços de segurança, podem ser: a implantação de um posto, a análise de riscos empreendida num cliente, as atividades de supervisão nos postos, a ronda noturna empreendida pelo vigilante, o controle eletrônico da ronda (bastão de ronda), as atividades de controle de acesso no posto, as atividades de monitoramento de imagens na sala de segurança, etc.

As organizações, geralmente, apresentam estruturas organizacionais do tipo funcional, onde são agrupadas, numa mesma unidade administrativa, aquelas atividades pertencentes a uma mesma área técnica e/ou de conhecimento (financeiro, operacional, comercial, RH etc.). Esta forma de estrutura organizacional acaba criando "ilhas" de especialidades dentro da organização, que não se comunicam suficientemente entre si, causando distorções na forma como é visto o fluxo de trabalho, suas consequências e as interrelações envolvidas. Isto acaba trazendo sérios prejuízos a qualquer atividade de gerenciamento, uma vez que se perde a noção do todo.

A segurança empresarial também é estruturada dessa forma e sofre suas consequências, dificultando a sua atuação em permear várias outras áreas e sua interrelação com as mesmas precisa ser conhecida, para uma possível identificação, avaliação e controle dos riscos.

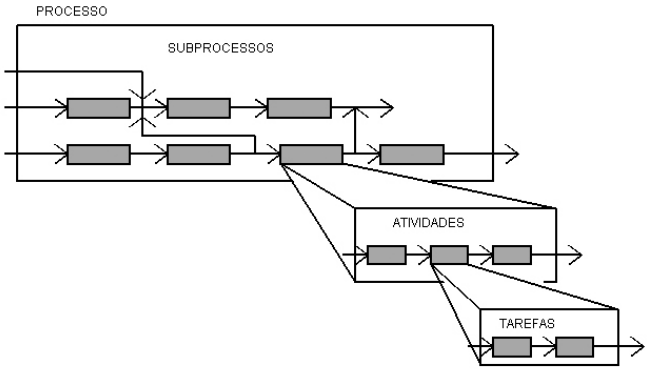
Uma forma simples e ampla de abordagem é a visão processual da organização, representando-a como um conjunto de processos, passando assim a compreendê-la melhor. Ao se orientar pelos processos, a organização estará trabalhando com todas as dimensões complexas de seu negócio.

A visão processual da organização permite o entendimento de como o trabalho é executado, através de processos que se interrelacionam além das fronteiras funcionais. Dessa forma, o conceito de processo, quando assimilado pelos profissionais de segurança, deverá fazer parte de qualquer estrutura de "análise de riscos", "valorização de sistemas" e "programas de qualidade" conduzidos por esses profissionais, em suas atividades de planejamento.

De acordo com a metodologia, hierarquicamente, os processos sofrem divisões que vão desde os macro-processos passan-

do pelos processos propriamente ditos, subprocessos, atividades, até o nível das tarefas. Os macro-processos são aqueles processos que envolvem mais de uma função dentro da organização, cuja operação tem impacto nas demais funções. Os processos propriamente são as atividades que recebem uma entrada, realizam transformações, agregam-lhes valor, gerando uma saída. Os subprocessos são divisões do macro-processo quando os mesmos possuem objetivos específicos, organizados seguindo linhas funcionais, ou seja, os subprocessos recebem entradas e geram suas saídas em um único departamento. Na sequência, os subprocessos podem ser divididos nas diversas atividades que os compõem e, em um nível mais detalhado, em tarefas.

FIGURA 2 - HIERARQUIA DO PROCESSO: PROCESSO, SUBPROCESSO, ATIVIDADES, TAREFAS.



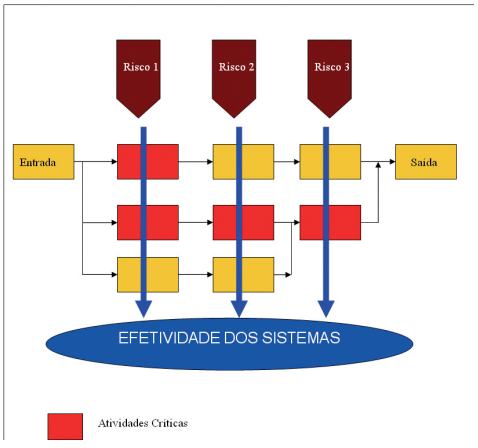
A principal dificuldade na visão processual é o problema de identificar a estrutura hierárquica dos processos, dado que eles estão fragmentados pela organização. É difícil determinar o início e o fim do macro processo.

Uma das práticas correntes, em organizações "competentes", é a análise dos seus processos de trabalho, a qual sendo realizada de forma criteriosa, tem demonstrado poder aumentar a produtividade, através da definição e compreensão dos aspectos relativos a problemas e sua consequente solução. De uma forma geral, pode-se iniciar a análise a partir de uma visão macro das atividades e seus problemas; em seguida, particularizar detalhes específicos de interesse ao processo produtivo. De qualquer forma que nasça o estudo, sempre existirá uma sequência fixa de passos predeterminados, que devem ser seguidos, ao se empreender uma análise de processos.

Uma das ferramentas de apoio para o melhor entendimento dos processos produtivos, através de uma representação clara e precisa, é a representação através do fluxo de processo. Onde são mostradas as atividades do processo, bem como a sequência e a forma como as mesmas são realizadas. A elaboração do fluxograma do processo de trabalho tem como principal objetivo a visualização do funcionamento de todos os componentes do processo, de forma simples e objetiva, permitindo assim que seus custos ou valores sejam medidos.

Define-se um fluxograma como um método para descrever graficamente um processo existente, ou um novo processo proposto, usando símbolos simples, linhas e palavras, de forma a apresentar graficamente as atividades e a sequência no processo. Do ponto de vista do gerenciamento de riscos, o fluxograma poderá ser utilizado como base estratégica para o reconhecimento de ameaças, a presença de riscos e os pontos críticos.

FIGURA 3 - REPRESENTAÇÃO GRÁFICA DE UM PROCESSO COM SUAS ATIVIDADES CRÍTICAS



Fonte: ACIA

Nos fluxogramas de processos têm-se a representação dos fluxos de atividades e informações de um determinado processo, normalmente apresentados na forma de diagramas de blocos. No diagrama de blocos, as etapas de um processo são mostradas de forma gráfica. Cada bloco representa a divisão do que se quer analisar. No diagrama de um processo, cada bloco representa um subprocesso, e num diagrama de subprocesso cada bloco representa uma atividade e assim por diante. Na confecção do diagrama deverão ser envolvidos os atores dos diferentes níveis hierárquicos da organização, e que sejam conhecedores da realidade de como os eventos ocorrem, possibilitando uma análise mais realista da situação a partir de vários pontos de vista.

Compõem as etapas básicas de um diagrama de blocos:

a) Definição do nível de detalhamento pretendido;

b) Definição do que se deseja analisar (processo, subprocesso, atividade, tarefa);

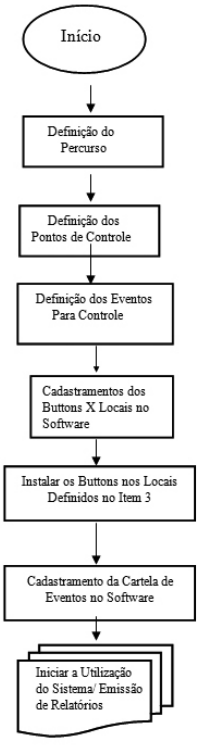
c) Definição de quantos, e quais os blocos para a sequência de eventos; e,

d) Montar o diagrama respeitando a sequência dos acontecimentos dos eventos.

e) Determinar os recursos empregados em cada atividade e atribuir valor a este

A elaboração de fluxogramas é uma ferramenta inestimável para se entender o funcionamento interno e os relacionamentos entre os processos empresariais. Durante a elaboração de um fluxograma de processo tornam-se transparentes e óbvias determinadas interrelações entre diferentes setores de trabalho. Isto pode contribuir para consolidar uma visão sistêmica e por processos nos profissionais e setores envolvidos. Quando esta visão de conjunto não for pertinente ou implicar em riscos indesejáveis, fórmulas que mantenham o necessário sigilo podem ser concebidas pela equipe de projeto.

No fluxograma a seguir, temos o exemplo do mapeamento dos processos de implantação do sistema de controle eletrônico de rondas (Bastão de Ronda), cedido pela empresa Deggy ®.



1 - Início – Decisão de implantação da Ronda e do Controle Eletrônico;

2 - Definir o percurso ou itinerário a ser realizada pelos Vigilantes rondantes;

3 - Definir quais os pontos serão os de controle – Locais onde serão instalados os buttons;

4 - Definir quais eventos serão controlados, considerados nos processos de segurança, nos percursos de ronda e nos pontos de controle

5 - Cadastrar os buttons no software de gerenciamento do sistema, associando cada button a um local;

6 - Instalar buttons nos locais de controle, de acordo com item 3;

7 - Cadastrar no software os eventos definidos no item 4;

8 - Início da utilização do sistema.

MAPEAMENTO DOS PROCESSOS

Segundo Harrigton (HARRIGTON, James; Aperfeiçoando Processos Empresariais, Makron Books Editora, São Paulo – 1993), quanto mais se entender os processos, mais capazes seremos de aperfeiçoá-los, trazendo a dimensão da qualidade mais uma vez para o foco. Recomenda, ainda, três etapas básicas para a melhor organização dos processos:

• A eliminação das perdas (ações corretivas);

• A eliminação das causas das perdas (ações preventivas);

• A otimização dos processos (consolidação dos resultados).

Características Básicas dos Processos

Os processos possuem características básicas que suportam a implantação de seu gerenciamento:

1. Fluxo de Valor: transformação de entradas em saídas, com a utilização de recursos da empresa, com a esperada agregação de valor;

2. Eficácia: grau com que as expectativas do cliente são atendidas. Ser eficaz é fazer o que o cliente quer.

3. Eficiência: grau de aproveitamento dos recursos para gerar uma saída. Ser eficiente é fazer o que o cliente quer da melhor forma para a empresa (otimizando o processo).

4. Tempo de ciclo: tempo necessário para transformar uma entrada numa saída. Deseja-se que o tempo de ciclo seja o menor possível.

5. Custos: recursos despendidos no processo.

O conhecimento dessas características é importante para:

• Identificar as áreas com oportunidades de melhoria;

• Fornecer o conjunto de dados para a tomada de decisão;

• Fornecer a base para definir metas de aperfeiçoamento e avaliar resultados.

No caso da segurança empresarial, sob o ponto de vista dos processos do cliente, teríamos que introduzir a dimensão da análise de riscos, que no mínimo responderá as seguintes questões:

• A quais riscos o processo está submetido?

• Quais as causas da existência dos riscos?

• Qual a probabilidade desses riscos se concretizarem?

• Qual o impacto econômico que causará na organização, caso o risco se concretize?

• Qual a situação dos nossos sistemas de proteção?

• Qual o nível de segurança que estamos operando?

Técnica de Gerenciamento de Processos (GP)

De acordo com a metodologia de Varvakis (1999), o gerenciamento de processos é uma metodologia que se destina à implementação da melhoria contínua em organizações. Empregada para definir, analisar e gerenciar as melhorias no desempenho dos processos em empresas, com a finalidade de atingir condições ótimas para os clientes. Resumidamente, o gerenciamento de processos é uma técnica de resolução de problemas. Falta de segurança é a causa de uma boa parte de problemas na sociedade brasileira atual, com reflexos diretos nas organizações.

Ainda segundo Varvakis (1999), as consequências advindas da implantação do GP estão intimamente relacionadas ao aumento global da qualidade e da produtividade, uma vez que os mesmos concentram seus esforços na melhoria contínua das atividades que efetivamente agregam valor aos produtos e serviços. Normalmente, o GP tem a orientação dos processos e subprocessos, voltados aos requisitos dos clientes, tanto externo quanto interno. Os processos propriamente ditos são orientados pelos clientes externos e os subprocessos pelos clientes internos, ou seja, aquele que recebe a saída desse subprocesso. Portanto, o conhecimento necessário e suficiente dos processos envolvidos e das suas interrelações é essencial para o entendimento do GP.

As etapas básicas da metodologia para o GP e os resultados esperados na sua aplicação estão divididas em quatro pontos de ação:

Etapa 1 - Base para o GP

Informar sobre a metodologia de GP. Identificar e elaborar: missão, produtos/serviços finais, processos na visão macro, clientes e fornecedores externos.

Etapa 2 - Definição do Processo

Identificar e descrever clientes internos, saídas, entradas e objetivos dos subprocessos. Mapear o fluxo de atividades e informações, definir indicadores e identificar os recursos utilizados nos diferentes subprocessos.

Etapa 3 - Identificação de Oportunidades de Melhoria

Priorizar oportunidades de melhorias. Gerar e avaliar impacto das ideias. Selecionar ideias.

Etapa 4 - Garantia da Melhoria do Processo

Concretizar as oportunidades de melhoria (desenvolver planos de ação, envolver as pessoas). Acompanhar implantação do plano realizando sua manutenção periódica, assegurando a continuidade do Gerenciamento de processo.

Etapa 5 – Análise de riscos (introduzida na técnica)

Analisar os processos sob a ótica dos riscos a que estão submetidos e sugerir ações que minimizem ou neutralizem tais possibilidades. Avaliar os sistemas de proteção existentes e definir o nível de segurança.

Conclusões

Como já nos posicionamos em outras ocasiões, continuamos a ter, para uma boa parte das organizações empresariais, a atividade de segurança patrimonial como um verdadeiro enigma que fica no subsolo das instalações, responsável pelos "homens de preto" que circulam pelos prédios, com seus rádios HT na mão. Sua forma de atuação, na maioria dos casos, tem conotações militaristas e/ou policialescas, porque trazem a cultura das forças públicas, utilizando seus manuais, mais voltados para a ação de polícia, atuando nas consequências e calcada no homem em ação, muitas vezes intimidador (o "Vigão"). Um recurso humano com pouca instrução requerida pelo cargo, com dificuldades de entender a visão sistêmica dos possíveis processos envolvidos em suas tarefas de segurança e muitas vezes sem condições de oferecer soluções para os problemas detectados. O mais grave nesta situação é que, na prestação de serviços de segurança, com emprego da vigilância humana, quem vai entregar o serviço é justamente o "Vigão", e vai estar o tempo todo em contato com o cliente, sendo o principal responsável pela qualidade(da segurança) do serviço que está sendo entregue.

Outra deficiência do setor, que continuamos a apontar sem grandes mudanças nos últmos anos, está relacionada ao enfoque fatalista que encontramos muitas vezes. A preocupação com o todo só é motivada por uma ocorrência grave, tida como fora de cogitação na organização, implicando, nestes termos, os efeitos sendo mais importantes do que as causas. O enfoque preventivo muitas vezes é subestimado, sendo o enfoque corretivo o centro das atenções. Evidentemente que, também para esta situação, não podemos deixar de abrir parêntesis para a citação e elogios às inúmeras exceções ao exposto acima, em que as ações dos "practionários" da segurança empresarial seguem as mais modernas técnicas de gestão.

O fato é que muito se fala em segurança empresarial, os esforços têm sido grandes em fazer algo, os gastos têm sido expressivos, mas os resultados parcos, quando se examinam as estatísticas, consequência da falta de preparo de seus atores e da falta de ciência aplicada. A segurança empresarial carece de métodos que atuem sobre problemas específicos, que proporcionem melhorias sistemáticas, mas que estejam também sintonizados com a participação efetiva dos outros setores da empresa. Como visto anteriormente, a metodologia de gerenciamento de processos (GP) é uma técnica que promove desdobramentos nos processos, atingindo atividades e tarefas, quando necessário. O GP permite, entre outras coisas, uma observação profunda desses processos, facilitando o reconhecimento de atividades críticas, que devem ser aproveitadas como agentes de melhoria contínua e da difusão da qualidade. É uma metodologia aceita e reconhecida por seus efeitos benéficos em organizações de renome que a utilizam.

Dessa forma, ações e soluções conjuntas, em que a nomenclatura e o simbolismo empregados sejam reconhecidos pelos mais diversos setores empresarias da organização, se fazem necessárias. Portanto, a aplicação de metodologia já testada e aceita pelas áreas produtivas e da qualidade, pode vir ao encontro dos anseios de mudanças nas relações entre o setor de segurança e demais áreas das organizações.

Partindo do pressuposto que gerenciamento de risco é a arte, a função que visa à proteção dos recursos humanos, materiais e financeiros de uma empresa, quer através da eliminação ou redução de seus riscos, quer através do financiamento dos riscos remanescentes, conforme seja o mais economicamente viável (BRASILIANO, A.; Manual de Planejamento e Gestão de

Riscos Corporativos, São Paulo; Ed. Sicurezza, 2003), tê-la explicitada nos processos produtivos das organizações certamente aumentará a competitividade de quem a adota e seria assim estabelecido o vínculo entre as atividades de gestão operacional das organizações e suas atividades de segurança.

Dessa forma, unir os conceitos de gerenciamento de riscos de Brasiliano (2003) à metodologia de gerenciamento de processos de Varvakis (1999) poderá ser o início de um conhecimento, no qual a segurança empresarial deverá ser vista como algo inerente a qualquer processo de produção.

Quanto à aplicação desta técnica na operação das empresas prestadoras de serviços de segurança, de acodo com os argumentos apresentados ao longo do texto, certamente os benefícios serão muitos, podendo ser o caminho que empresas "competentes" achem, para diferenciar seus serviços, consolidar métodos para a garantia da qualidade de seus serviços, aumentar seus clientes, seus faturamentos e seus lucros.

Outra conclusão importante está relacionada às dificuldades das atividades de segurança patrimonial em comprovar resultados, via relatórios utilizados pela alta gestão, tais quais as análises econômico-financeiras, aplicando ferramentas como o valor presente líquido, payback, retorno dos investimentos, etc. A gestão por processos, por meio de suas ferramentas, que decompõem a organização em processos/atividades/tarefas, permite facilmente a atribuição de valores para esses, podendo, desse modo, realizar todo o tipo de análise econômico-financeira, suprindo, assim, a lacuna apontada.

E, como último argumento para o convencimento dos mais céticos, que ainda não se renderam à necessidade do entendimento dos processos e dos sistemas da qualidade que envolvem as atividades operacionais dos serviços de segurança, destacamos o fato de ser toda organização uma "coleção de processos", um "conjunto de tarefas", antes de ser "um conjunto de funções". Para melhor administrá-la, temos que entendê-los na sua essência.

Dagoberto Helio Lorenzetti

Engenheiro pelo ITA; Pós-Graduado em Engenharia Nuclear pela Escola Politécnica da USP; Pós-Graduado em Análise de Sistemas pela FAAP; Mestre em Análise e Gerenciamento de Riscos pela The Johns Hopkins University; Doutor em Administração pela FEA/USP. Especialidades: Gestão Sustentável, Gerenciamento de Perdas e Riscos e Gestão de Operações (Qualidade e Produtividade em Operações de Manufatura e Serviços, Logística e Sistemas Integrados). Exerceu funções executivas em empresas nacionais e multinacionais. Consultor e palestrante em organizações públicas e em empresas nacionais e multinacionais – Professor da Fundação Getúlio Vargas/SP

Fernando Só e Silva, MSc

Engenheiro mecânico pela PUCRS, especialista em engenharia de produção pela UFSC (Universidade Federal de Santa Catarina), MBA em Administração pela FEA/USP, especialista em Gestão de Segurança pela FECAP/SP, Mestre em Engenharia de Processos pelo Instituto de Pesquisas Tecnológicas de São Paulo/IPT , treinamentos nos USA e Alemanha. Oficial R2 do Exército Brasileiro, com experiência de mais de 10 anos em projetos de gerenciamento de riscos, segurança e engenharia de processos. Autor de livro e de diversos artigos publicados por revistas especializadas, membro de grupo especializado em gestão e análise de riscos patrimoniais e TRC. Associado a ABSEG desde 2006. Participação em projetos internacionais. Diretor comercial da empresa Deggy® do Brasil.

Segurança da informação

Edison Fontes, CISM, CISA

1. INTRODUÇÃO

O processo de segurança da informação em uma organização possui várias dimensões ou aspectos. Normalmente somos levados a nos concentrar no (admirável) mundo da tecnologia. Principalmente os profissionais que têm formação nessa área, têm uma tentação mais forte em estudar profundamente questões de proteção da rede dos computadores, invasão cibernética e constantes atualizações em termos de produtos de proteção. Tudo isso é importantíssimo e necessário, porém não é suficiente.

A proteção da informação somente vai acontecer de uma maneira efetiva (eficiente e eficaz ao longo do tempo) se realizarmos uma abordagem completa para a informação. Evidentemente a maior quantidade de informação de uma organização está no seu ambiente computacional, mas, não apenas lá. No momento em que pessoas acessam esse ambiente computacional elas guardam a informação na sua mente, imprimem (e deixam) na impressora, entregam relatório a outras pessoas, não destroem esse relatório quando ele é jogado no lixo e, finalmente, falam com outras pessoas sobre essas informações. Neste último ponto, falam porque realmente precisam comunicar aquela informação ou falam (para mostrar status de conhecimento) para pessoas que não deveriam ter acesso à informação.

Dessa forma, é importante estruturar o processo de segurança da informação. Lembro sempre a todos com quem mantenho contato que esta composição por dimensões é uma divisão didática. Quando o problema acontece, ele vem único. Por exemplo: uma pessoa estranha aos quadros de usuários da organização roubou o notebook da mesa do seu presidente! Neste caso podemos identificar rapidamente alguns tipos de problemas:

- Acesso físico: uma pessoa não autorizada não deveria ter acesso físico à sala do presidente.

- Confidencialidade da informação: os dados armazenados no equipamento deveriam estar criptografados. Como não estavam, quem possuir o computador vai poder acessar essas informações.

- Conscientização do usuário: o cabo de proteção do equipamento não foi utilizado ou o equipamento deveria estar guardado em um local trancado, quando não estivesse em utilização pelo usuário. (Ôpa! Mas é o presidente! E agora? Quem vai dizer isso a ele?).

- Treinamento: o presidente não foi treinado adequadamente. Faltou no dia do treinamento. Ele mandou o assistente dele!

- Tecnologia: o projeto que possibilita a realização de cópia de segurança automática, quando o usuário está ligado na rede da organização, está atrasado. Talvez seja adiado para o próximo ano!

Esta análise deve ser feita para que seja avaliado o que falhou e que medidas específicas devem ser tomadas. Evidentemente que do ponto de vista do usuário, o problema foi: estou sem meu equipamento e sem os meus dados e ainda a organização está com sérios riscos de ter havido vazamento de suas informações confidenciais.

Estruturar essas dimensões é utilizar uma arquitetura de segurança da informação. A arquitetura que descrevo abaixo está baseada na norma NBR ISO/IEC 27002 e está mais detalhada no meu livro "Praticando a segurança da informação", Editora Brasport, 2008.

De uma forma simples, uma arquitetura de segurança da informação deve:

* possibilitar que os controles de proteção sejam implementados de forma estruturada,

* ser padronizada para todas as plataformas de tecnologia,

* considerar todos os tipos de usuários,

* atender de forma corporativa aos requisitos legais,

* garantir que o acesso à informação utilize autenticação e autorização semelhantes em todos os ambientes,

* considerar a necessidade da disponibilidade dos recursos de informação para a realização do negócio corporativo,

* ter flexibilidade para manter a efetividade da proteção, e

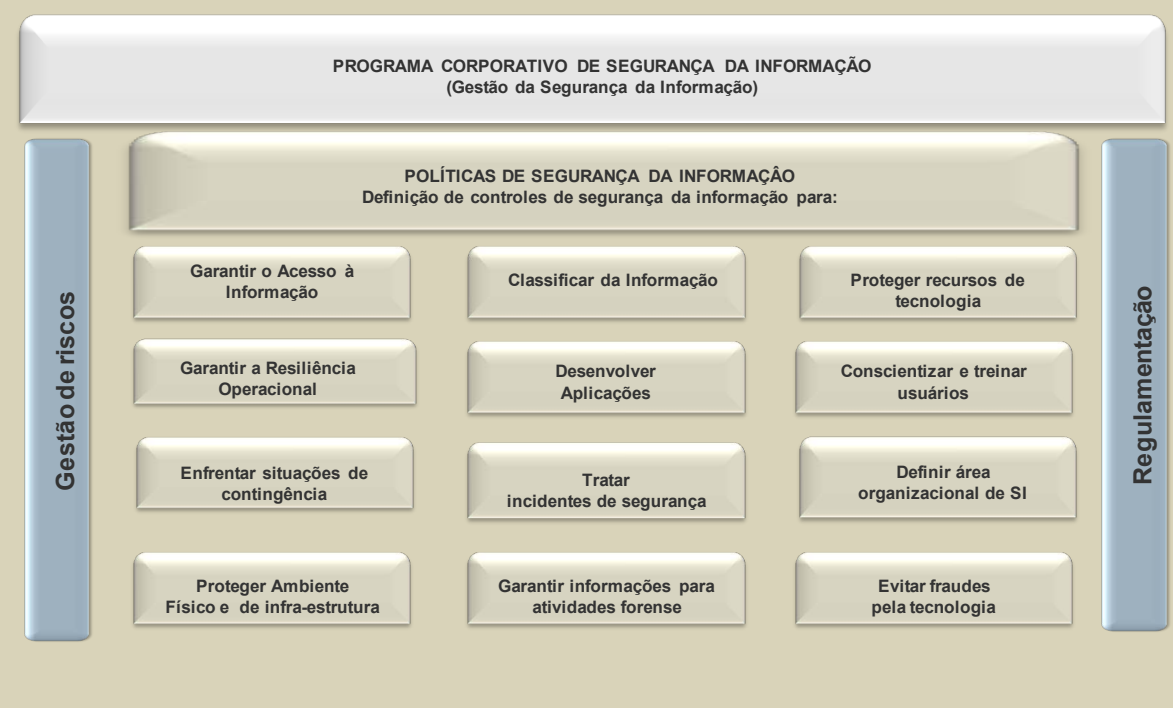
* estar visceralmente comprometida com os requisitos do negócio.

Quando se busca uma arquitetura, se deseja que exista uma solução (ou estrutura de solução) que seja válida para a corporação e não apenas para departamentos específicos, que quando considerados juntos, a solução parece um conjunto de retalhos diferentes, costurados de maneira artesanal.

Os controles de segurança devem ser possíveis de serem implementados em todas as plataformas de tecnologia, evidentemente considerando as características e limitações de cada uma.

Segue abaixo uma visualização dos elementos da Arquitetura de Segurança:

Arquitetura de Segurança



2. DIMENSÕES DA SEGURANÇA DA INFORMAÇÂO

2.1 Políticas e demais regulamentos de segurança da informação

A política, normas e procedimentos definem os controles que devem existir para a devida proteção da informação. A política principal descreve a filosofia e as regras básicas para o uso do recurso informação.

Esses controles devem existir independentemente do ambiente em que a informação seja utilizada: ambiente convencional ou ambiente de tecnologia. Com a existência da política fica explicitado o que cada pessoa da organização deve cumprir no que se refere à proteção da informação.

Mas, a política não pode, ou melhor, não deve surgir do nada. É necessário que a política esteja alinhada aos objetivos da organização. A partir dos objetivos de negócio, são definidos os objetivos da segurança da informação, que tem como destaque: possibilitar a realização do negócio no que depende do uso dos recursos de informação.

A política e demais regulamentos definem estratégias, regras, padrões e procedimentos que direcionarão todas as ações para atingirmos os objetivos de segurança da informação. Essas ações podem ser atividades técnicas ou atividades de usuários. Sem uma política ficamos sem saber para onde queremos ir, sem saber qual é a filosofia da organização sobre o assunto segurança e qual o nível de proteção desejado para a organização.

Para se ter uma estrutura adequada, recomendo que deva existir uma política principal, descrita em um documento curto e simples, de forma que todos os usuários entendam facilmente como a organização deseja que a informação seja tratada e quais são as principais responsabilidades dos usuários. Outros documentos, como políticas específicas e normas, podem e devem complementar esses requisitos básicos.

Para que a política e o conjunto dos demais regulamentos tenham uma existência efetiva (eficiência e eficácia ao longo do tempo) é necessário:

a) Ter o apoio e patrocínio explícito do nível executivo da organização

Preferencialmente a política principal deve ser assinada pelo presidente da organização. Desta forma fica explícito que o conjunto dos requisitos de segurança descritos na política é resultado de uma decisão estratégica da alta direção e não uma simples adoção de melhores práticas de segurança

b) Representar a verdade da organização

O que for escrito na política e nos demais regulamentos deve exprimir a verdade e os valores da cultura (ou do que se quer como cultura) da organização.

c) Ser possível de implementação e de execução pelos usuários

Não podemos especificar requisitos que não podem ser implementados ou são impossíveis de serem cumpridos pelos usuários. As regras devem ser adequadas ao nível atual de proteção e ao nível desejado de proteção.

Após a elaboração, devemos ter algumas ações para que a política seja de conhecimento e de aplicação pelos usuários. É necessário que:

* exista uma divulgação ampla, geral e irrestrita para os usuários;
* o acesso a essa política pelos usuários seja fácil; e
* exista um processo que garanta que essa política e os demais regulamentos de segurança estejam sempre atualizados.

2.2 - Acesso à informação

O acesso à informação é uma das dimensões que mais sofrem com ações de erros e falta de profissionalismo do usuário, bem como com ações de má fé (fraudes). Também a questão de vazamento de informação, por pessoas não autorizadas ou por pessoas autorizadas, é explorada nesta dimensão.

Esta dimensão se divide em três grandes blocos de ações:

a) Gestão da identidade do usuário

Trata de como o usuário se apresenta para o ambiente computacional e o ciclo de vida dessa identidade. Este último aspecto trata de como a identidade do usuário é criada na organização, como ela é mantida e como ela será desligada do ambiente computacional, quando o usuário não tiver mais vínculos profissionais com a organização. Isto vale para funcionários, como também para prestadores de serviços e estagiários.

b) Gestão de autenticação do usuário

Verifica a veracidade do usuário (se ele realmente é quem diz ser) e da definição das técnicas de autenticação que serão utilizadas. O usuário pode se autenticar de três maneiras: por algo que sabe (senha), por algo que possui (cartão, token, outro) ou por algo que é (característica biométrica). Cada uma dessas opções possui seu nível de segurança e custo. Para cada situação deve ser feita uma avaliação de "custo x benefício", considerando as características da organização e os riscos associados.

c) Gestão de autorização para acessar a informação

Verifica se o usuário está autorizado a acessar a informação. Essa autorização deve considerar o perfil do usuário e será feita de maneira individual, em grupo, ou baseado em perfil funcional. Para a efetividade dessa ação de autorização devem existir o gestor da informação e as regras explícitas e de conhecimento de todos para a autorização de acesso.

2.3 Classificação da informação

É a definição de níveis de sigilo da informação, do gestor da informação e do custodiante da informação.

Para cada nível de sigilo são indicados os procedimentos que devem ser realizados ou proibidos em relação à informação com aquela classificação. Por exemplo: uma informação confidencial não pode ser enviada via uma mensagem de correio eletrônico pela Internet, de maneira aberta e sem criptografia.

Normalmente as informações são classificadas em três ou quatro níveis de sigilo. Um exemplo de níveis de sigilo: pública, interna e confidencial. Algumas organizações possuem uma classificação mais sofisticada, mas aconselho esta classificação de três níveis para as organizações que estão em um nível inicial de maturidade em segurança da informação.

O Gestor da Informação é a pessoa que, dentro da organização, tem o poder de liberar (ou negar) o acesso à informação para qualquer usuário. Ele deve ser o executivo da área que possui as informações. Por exemplo: as informações de recursos humanos, para serem acessadas, devem ser autorizadas pelo executivo da área de recursos humanos da organização.

O custodiante é a pessoa ou área que administra o recurso que utiliza a informação. Por exemplo: os recursos computacionais, normalmente, possuem como custodiante a área de tecnologia da informação.

2.4 Enfrentar situações de contingência

Tem como objetivo a definição da solução para o tempo suportável de indisponibilidade dos recursos de informação, antes que o negócio atinja um nível de impacto financeiro, operacional ou de imagem que comprometa a continuidade da organização.

Sem dúvida alguma, os recursos de informação são críticos para a realização do negócio da organização. Uma indisponibilidade nesses recursos e o impacto (financeiro, de imagem ou operacional) será sentido de imediato na organização. Sendo assim, é imprescindível a existência de um plano de continuidade de negócio para possibilitar que, de uma forma mínima, o negócio da organização continue operando durante o período necessário para a recuperação dos recursos de informação originais ou substitutos.

As etapas para a definição de um plano para situações de contingência são:

a) Definição do escopo e cenário

Escopo: recursos, ameaças e ambientes que serão considerados.

Cenário: situação em que acontecerá o desastre.

A definição do escopo e cenário é fundamental e deve ser a primeira etapa a ser definida. Cada versão do plano deve ter explícito o seu escopo e em que circunstâncias foi considerado que a contingência acontecerá (cenário).

Um exemplo de limitação é considerar a contingência apenas para um local (escopo) e considerar que não haverá perda de pessoas no desastre (cenário).

Vale lembrar que as limitações de escopo e cenário têm por objetivo possibilitar a elaboração de versões de plano compatíveis com a maturidade da organização na questão "continuidade de negócio".

b) Avaliação de ameaças e riscos

Esta etapa não é obrigatória, porém é recomendável que ela seja executada. Considerando o escopo e cenário, deverão ser analisadas as ameaças consideradas e avaliada como está a situação da organização em relação às mesmas.

Normalmente existem ações simples que podem ser implementadas de imediato e trazem uma melhoria na proteção da informação.

Essa avaliação pode ser feita considerando valores qualitativos (alto, médio, baixo), pois valores quantitativos são muito mais difíceis de obter. Na utilização de valores qualitativos, o que vai valer é a comparação de um valor com outro valor. O valor isoladamente significa pouco.

c) Análise de impacto no negócio

Nesta etapa a área de negócio precisa responder qual o potencial impacto (financeiro, de imagem e operacional) para organização, caso um determinado recurso ou conjunto de recursos esteja indisponível.

A resposta da área de negócio é que permitirá a elaboração do produto final dessa etapa: qual o tempo de indisponibilidade que o negócio suporta, considerando o potencial dos impactos financeiro, de imagem e operacional.

d) Identificação de soluções

Nesta etapa, baseada nas informações das etapas anteriores, são avaliadas as diversas opções de processamento alternativo para a informação. A opção que melhor se adequar deve ser implementada.

e) Elaboração do Plano

Esta etapa é a construção do conjunto de documentos e manuais que formarão o plano de continuidade do negócio. Esses documentos deverão permitir que, em uma situação de contingência, as pessoas sigam as suas instruções e tenham, consequentemente, uma solução alternativa para a situação de contingência.

f) Plano de teste

Deve ser elaborado um plano de teste e treinamento para garantir que as pessoas continuem sabendo executar o plano. Nesses testes também podem ser identificadas situações não previstas no plano e que precisam ser incorporadas.

g) Plano de manutenção

Esse plano define como será feita a manutenção, com o objetivo de garantir que os documentos estarão sempre atualizados. Chamamos a atenção para o fato de que deve haver uma manutenção periódica e uma manutenção para situações específicas.

2.5 Garantir a resiliência operacional

A existência de gestão de problemas, gestão de mudanças, gestão de recursos, gestão de capacidade possibilita que a organização suporte situações adversas sem que haja ruptura na operação do negócio, no que se refere aos recursos de informação.

Essas quatro vertentes de controle podem ser expandidas caso a organização possua situações específicas.

2.6 Proteger o ambiente físico e de infraestrutura

Esta dimensão tem por objetivo buscar a garantia de que o ambiente físico está controlado e protegido, e que os elementos de infraestrutura (água, energia, temperatura, condições do ar) estão adequados para o uso pelos recursos de informação.

Este aspecto permite que se pratique uma maior interação entre a segurança patrimonial/corporativa com a segurança da informação. A sincronização de controles é fundamental para a identificação de falhas. Por exemplo: um usuário que obtém de forma fraudulenta a senha de outro usuário poderá ser identificado pelo sistema de monitoramento visual. Neste exemplo, o usuário lesado irá negar que fez determinada transação. Pela identificação do terminal e sincronizando com a gravação de imagens do local, poderemos identificar o fraudador.

O plano para situações de contingência será beneficiado com o bom desempenho da dimensão de proteção do ambiente físico

e da infraestrutura. Muitas situações poderão ser evitadas ou caso aconteçam serão minimizadas.

2.7 Desenvolver aplicações

Do ponto de vista de segurança da informação, quando do desenvolvimento, manutenção e aquisições de sistemas, devem existir: uma metodologia, os requisitos de segurança, a proteção do ambiente de desenvolvimento de sistemas e uma documentação para garantia da manutenção do conhecimento.

Descrevemos abaixo alguns requisitos de segurança quando do desenvolvimento de sistemas.

a) Modularidade

Um sistema aplicativo deve conter vários módulos/programas estruturados, de forma que cada um execute uma ou apenas algumas funções.

b) Documentação adequada

O sistema deve ter uma documentação de funcionalidade e de operacionalidade adequado à sua criticidade para o negócio da organização.

A documentação deve ser suficiente para que outro profissional do mesmo nível técnico da pessoa que executa a tarefa, lendo a documentação, entenda o programa/módulo ou similar.

c) Controle de versão

Algumas plataformas computacionais possuem produtos que possibilitam o controle de versão de programas e módulos; outras não. Independentemente da facilidade existente, um controle de versão deve existir e possibilitar o registro de tudo que foi feito.

d) Ambiente de produção não é para desenvolvimento e teste

Devem existir pelo menos dois ambientes: de produção e de desenvolvimento. Uma solução profissional e adequada é a existência de um terceiro ambiente para homologação e testes do sistema. Se a organização não puder ter esses ambientes, que não desenvolva seus sistemas.

e) Programas fontes devem ser controlados

O acesso ao ambiente de desenvolvimento deve ser restrito, mesmo aos programadores e analistas. Cada profissional deve ter acesso apenas aos elementos de que necessita para desenvolver o sistema ou sistemas.

f) Registros para a auditoria

Todos os acessos realizados nos dados dos sistemas devem ser registrados para auditorias e investigações.

g) Avaliação da qualidade do desenvolvimento

Deve existir uma área de Software Quality Assurance, que testa o que foi desenvolvido com o que foi especificado e acertado em termos de nível de serviço.

2.8 Tratar incidentes de segurança

Esta dimensão cuida de registrar incidentes, responder em tempo adequado e encaminhar para a solução definitiva.

Na medida em que a organização já possua elementos da Resiliência Operacional, o tratamento de incidentes será facilitado e, muitas vezes, evitado.

O importante é que, quando da ocorrência de um incidente, as pessoas envolvidas saibam o que devem fazer e quais são as suas responsabilidades.

2.9 Garantir informações para atividade forense

Esta dimensão possibilita a definição de ações preventivas, treinamento de usuário para tratar situações desse tipo, infraestrutura mínima de tecnologia, realização de análise forense de situações de fraude, erro ou recuperação de informação.

2.10 Proteger recursos de tecnologia

Tem como objetivo principal a proteção da rede computacional da organização contra ataques externos e internos, proteção de cada recurso de tecnologia, definição da autenticação entre recursos de tecnologia, garantia de utilização de produtos atualizados, bem como as correções desses produtos e do SW básico.

Esta dimensão está diretamente ligada à Área de Tecnologia da Informação.

2.11 Conscientizar e treinar os usuários

Esta dimensão trata de definir procedimentos para conscientização, implementar treinamentos necessários e implementar, garantir engajamento da direção e garantir o alinhamento com regulamentos internos e externos. A Área de Segurança da Informação

deve contar com o total apoio da área de recursos humanos, pois aqui estamos falando de pessoas.

Deve haver um treinamento contínuo e devem existir eventos específicos que destaquem a segurança da informação. O importante é que tudo isso seja feito com o apoio explícito da alta direção.

2.12 Definir área organizacional da segurança da informação

A área de segurança da informação deve ser formalmente definida. Deve-se ter, de forma explícita, o escopo de atuação, a definição da estrutura de pessoas e recursos, a identificação das áreas gestoras de informação, a identificação das áreas que utilizam a informação, a identificação dos processos necessários para a gestão da segurança da informação e a definição da posição organizacional.

2.13 Evitar fraudes pela tecnologia

É a dimensão dedicada, considerando as possíveis fraudes, à análise dos sistemas e processos de negócio, à definição/avaliação das contramedidas, à definição de monitoramento constante, à definição de medidas preventivas, à definição de maneiras de detecção de fraude e à existência de respostas rápidas.

2.14 Aspectos legais e conformidade com regulamentos

Os aspectos legais e outros requerimentos que a organização é obrigada a cumprir devem ser considerados nesta dimensão, em uma visão corporativa, possibilitando uma única implementação. Questões que atinjam áreas específicas continuam tendo uma abordagem corporativa; porém, com uma implementação específica.

2.15 Gestão de risco

A gestão de risco deve existir, permeando todas as dimensões citadas anteriormente. Isto significa que em cada dimensão devem ser feitas as perguntas:

* Quais são as ameaças existentes?
* Quais dessas ameaças devem ser consideradas na prática?
* Qual o risco (probabilidade) desta ameaça se concretizar?
* Qual será o impacto (financeiro, de mercado, de imagem ou operacional) que essa ameaça trará, caso se concretize?
* Que contramedidas preventivas, ou corretivas podem-se implementar?

3. CONCLUSÃO

A proteção da informação tem um grande número de elementos, situações, recursos, sujeitos e formas, que precisam ser considerados. Inicialmente você pode ter a sensação de que não é possível fazer uma boa proteção.

Mas é possível fazer uma boa proteção; porém, existem ações estruturais que facilitam o sucesso. Você deve:

* Definir o escopo e abrangência da proteção a ser feita.
* Garantir o apoio da direção executiva.
* Considerar com prioridade: políticas/normas, acesso à informação e conscientização/treinamento de usuário.
* Garantir a existência de recursos. Não só financeiros.
* Conhecer o assunto segurança da informação.
* Conhecer soluções de organizações similares.
* Gostar do tema e ser persistente.
* Pertencer à associação de profissionais em que experiências como esta possam existir e fazer com que você possa acelerar seu conhecimento.

Edison Fontes, CISM, CISA.

É Consultor, Professor, Orientador de alunos, Colunista ITWEB e Autor de livros em Segurança e Proteção da Informação. Foi Coordenador de Segurança do Banco Banorte, Gerente do Produto Business Continuity Plan da PricewaterhouseCoopers, Security Officer da GTECH Brasil, Gerente Executivo da CPM Braxis Brasil e Consultor Independente para várias organizações.

Outsourcing de Gestão em Segurança

Hugo Tisaka

A terceirização de serviços em empresas - ou outsourcing - é uma ferramenta administrativa que já se firmou como uma alternativa viável e bastante flexível, atendendo às necessidades do competitivo mercado globalizado e também da legislação vigente.

De acordo com a autora Giovanna Lima Colombo, a terceirização é "a transferência de atividades para fornecedores especializados, detentores de tecnologia própria e moderna, que tenham esta atividade terceirizada como sua atividade-fim, liberando a tomadora para concentrar seus esforços gerenciais em seu negócio principal, preservando e evoluindo em qualidade e produtividade, reduzindo custos e ganhando competitividade."

No mercado de segurança, a terceirização de serviços foi a forma viável para que fossem implementadas atividades de vigilância e portaria, escolta de carga, segurança VIP e outras, devido à rígida legislação que rege a segurança orgânica, patrimonial, pessoal e mais recentemente, a questão do porte de armas.

Em 2007, segundo a FENAVIST, este setor foi responsável por 2,02 Milhões de empregos diretos (sendo que 57% deste contingente é formado por vigilantes e VSPP) e o total dos gastos das empresas que contrataram este tipo de serviço, neste mesmo ano, foi de 12 Bilhões de Reais.

Ainda, se somarmos aos outros custos relacionados à atividade de segurança em empresas, estas cifras podem chegar a quase 19 Bilhões de Reais – um pouco menos da metade do orçamento do Ministério da Educação para 2009.

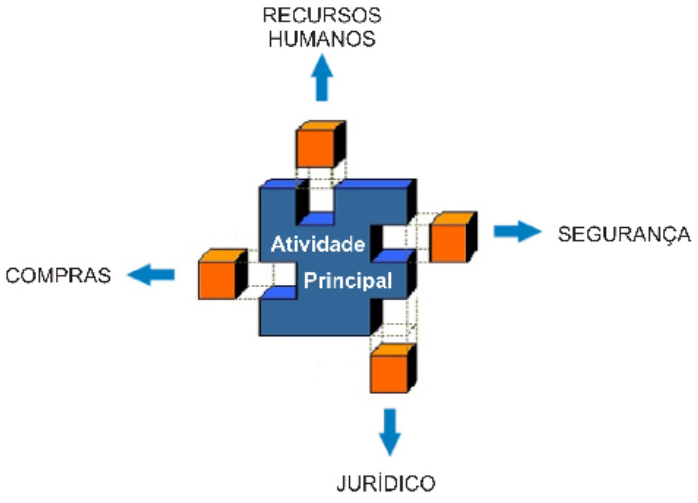


Figura 1 - Atividades corporativas que se beneficiam desta ferramenta

Por definição, a atividade do gestor de segurança de uma empresa é coordenar a administração dos recursos financeiros, patrimoniais e humanos dentro de uma organização, e é justamente neste processo que entra o outsourcing em gestão.

Muitas empresas, por várias razões, não possuem a disponibilidade – ou ainda a necessidade – de contratar um profissional que realize as atividades de gestão de forma dedicada. Um gerente de segurança pode custar para a empresa mais de R$ 200 mil/ano e a posição de um diretor, algo em torno de R$ 550 mil/ano.

Nestes casos, a gestão terceirizada é a solução mais adequada, já que ela se adapta às necessidades de segurança da empresa, já que o mesmo profissional (ou grupo de profissionais) trabalha de forma compartilhada e com outros clientes, reduzindo-se dessa forma o investimento individual de cada contratante.

NEM TUDO SÃO FLORES

Os benefícios são muitos e em sua maioria conhecidos, como foco no core business, flexibilidade, eliminação de custos com recrutamento e seleção, substituições quando necessárias, redução de custos internos, etc.

No entanto, uma atividade de gestão terceirizada possui uma série de consequências que devem ser contornadas e que é

costume chamá-las de "armadilhas do outsourcing de gestão". Essas armadilhas são percebidas somente durante o decorrer das atividades, onde é frequente a colisão de interesses e responsabilidades.

Costumo citar alguns exemplos de conflitos:

* Uma manhã, durante o feriado, o gestor de segurança terceirizado recebe um telefonema do Diretor Administrativo da empresa, informando que o alarme da planta de Vitória da Conquista foi acionado e, segundo ele, "parece haver um princípio de incêndio". – O que fazer?

* O veículo da empresa, conduzido pela esposa do Diretor Administrativo, colidiu com uma moto a caminho da fábrica e ela liga para o celular do gestor pedindo auxílio. – É responsabilidade dele atender essa ocorrência? Quem pagará a conta?

* Um funcionário foi acusado de extravio de produtos acabados e o advogado da empresa desconfia de um possível envolvimento das autoridades policiais; e diz que conseguiu uma autorização do presidente da empresa para realizar uma investigação "paralela". – Está dentro do seu escopo de responsabilidades?

Esses exemplos servem somente para ilustrar o nível de complexidade que esse serviço representa. A melhor forma de resolver tais conflitos é combinar antes, através de um Acordo de Nível de Prestação de Serviço, também conhecido como Service Level Agreement – SLA.

O SLA - SERVICE LEVEL AGREEMENT

Esse documento, que normalmente é um anexo do contrato de prestação de serviço, irá discriminar o escopo do trabalho, as atividades que compõem esse escopo, o nível de prontidão, entre outros.

O SLA deverá ainda, determinar quais são os indicadores de desempenho para que o trabalho do gestor possa ser mensurado.

Ainda, as decisões do gestor de segurança nem sempre agradam determinado setor da empresa; do financeiro ao de operações, sempre haverá uma decisão difícil de tomar e essa responsabilidade não pode ser somente desse profissional, mas sim de um colegiado, onde as decisões estratégicas serão tomadas em conjunto, de forma a reduzir o estresse desses processos.

Também existe um certo "preconceito" dos funcionários da empresa com relação aos terceirizados, dificultando ainda mais a aderência às novas normas e regras. Portanto, é imprescindível a adoção do staff da empresa e o suporte por eles prestado.

Este suporte deve ser abrangente, desde o acesso para as dependências que estão relacionadas no escopo de trabalho, até o fornecimento de crachá, e-mail, vaga de estacionamento (se outros profissionais do mesmo nível tiverem esse direito), acesso ao restaurante (ou vales-refeição), enfim, tudo para que o gestor de segurança se encaixe no perfil dos funcionários da empresa.

OS TRÊS PRINCÍPIOS BÁSICOS

Existem alguns dilemas corporativos que permeiam a decisão de contratar o serviço de terceirização da gestão de segurança de uma determinada empresa:

* Princípio da Utilidade – A empresa precisa de um gestor de segurança 24/7 (vinte e quatro horas por dia, sete dias da semana)? Muitas vezes, a demanda interna desse serviço, ou então o faturamento global da empresa, não podem suportar um

gasto que pode chegar a R$ 1 Milhão por ano (se considerarmos um cargo de direção, com todos os encargos trabalhistas e sociais, benefícios, assistente, infra-estrutura e equipamentos);

* Princípio da Especialidade – A organização pode acumular as atividades da gestão de segurança para outro executivo (por exemplo: facilities ou RH)? A gestão da segurança de uma corporação possui uma série de modelos/metodologias, cercada de inúmeros detalhes - legais e operacionais - que precisam ser seguidos, para diminuir o risco de onerosos processos judiciais, que costumam consumir muitos recursos da empresa. O profissional que irá coordenar os esforços de segurança deverá ser um especialista em segurança privada e possuir conhecimento e experiência para que seja possível implementar as melhores e mais eficientes práticas de mercado. Além disso, nossa experiência nos mostra que o network com outros profissionais da segurança pública e privada possibilita que as eventuais crises sejam resolvidas com muito mais rapidez, com melhores resultados;

* Princípio da Continuidade – A empresa pode sobreviver ao longo do tempo sem um profissional de segurança? A busca de novos mercados, novos produtos exige necessariamente a inserção em regiões ou atividades pouco conhecidas. A segurança permeia todas as outras atividades da empresa e seu correto balanceamento fará com que os recursos sejam gastos de forma eficaz. A continuidade da empresa também deve ser considerada, já que certas ocorrências podem ter consequências catastróficas em termos financeiros, operacionais ou até mesmo de imagem. O mundo dos negócios está em permanente mutação. As condições em que as empresas operam sofreram significativas alterações, quer pela globalização dos mercados, quer pela mutação da condição sócio-econômica nas localidades em que atuam.

FATORES CRÍTICOS DE SUCESSO

Para que a implementação de um processo de outsourcing em uma determinada empresa atinja o sucesso esperado, devem-se observar os seguintes fatores críticos:

* Alinhamento de objetivos da empresa contratante/contratada;

* Visão e plano estratégico;

* Gerenciamento dos contratos já existentes;

* Contrato de outsourcing devidamente estruturado;

* Comunicação aberta entre os grupos/indivíduos impactados pelo processo;

* Envolvimento e apoio da alta diretoria.

As práticas mencionadas neste artigo estão em constante mutação para adaptar-se aos novos princípios da administração moderna e este serviço – oferecido de forma estruturada e com uma metodologia própria - ainda é muito recente.

O desenvolvimento da metodologia deve ser permanente, assim como a adoção das melhores práticas de mercado para este segmento. O know-how dos consultores que prestam este serviço deve ser "de ponta" e todas as suas ações devem ser formalizadas no sentido de dar o back-up documental necessário em caso de disputas.

Entendo que a atividade de segurança - ainda que não produza receita direta, ao contrário do que pensam alguns outros autores – é uma alavancadora de resultados, permitindo que a empresa reduza seus prejuízos em caso de incidentes e possibilite ganhos competitivos em relação aos seus concorrentes.

A atividade de gestão de segurança corporativa é extremamente especializada e suas inúmeras variáveis precisam ser controladas adequadamente de forma a otimizar os sempre escassos recursos destinados a este fim.

Hugo Tisaka

Diretor Executivo da NSA Brasil – empresa de consultoria internacional em segurança e Diretor de Relações Governamentais da ABSEG – Associação Brasileira de Profissionais de Segurança. Atualmente coordena os grupos de trabalho - Gerenciamento de Crises Relacionadas a Sequestros e Núcleo de Orientação Profissional para Militares e Policiais, ambos da ABSEG. Membro do Corpo Docente do MBA da UNIP. Graduado em Administração de Empresas pela FAAP e pós-graduado em Estratégia Militar para Gestão de Negócios, pela mesma instituição. Especialista em gerenciamento de crises, proteção corporativa e segurança em logística. Responsável por chefiar múltiplas equipes em diversos países, na proteção de clientes ultra-VIPS e escolta de mercadorias de alto valor agregado. Criador do PREVICON - Programa de Redução da Violência em Condomínios, assim como responsável pela introdução do conceito Security by Design na América Latina.

Gestão Estratégica da Segurança

Isaac de Oliveira e Souza

1 CONTEXTUALIZAÇÃO

Acredita-se que, pelo fato de ser citado, muitas vezes, em todo momento, um termo possa ser conceitualmente compreendido por todos, no âmbito de uma organização[1]. Entretanto, a realidade dos fatos indica exatamente o contrário. É o que acontece com a utilização dos termos gestão, estratégia e segurança, citados com freqüência, nas organizações de nossos dias, notadamente, naquelas que têm a responsabilidade da gestão estratégica da segurança.

Assim, realizar a gestão estratégica da segurança pressupõe, inicialmente, o entendimento de o que seja gestão, estratégia e segurança.

Inicialmente, é importante considerar que, no termo gestão, encontram-se o entendimento de governo e de gerenciamento, desenvolvidos com técnica e ética. Nesse contexto, elaboram-se as diretrizes e princípios coerentes, com a missão e a visão, e convergentes à estratégia pretendida para alcançar os objetivos estabelecidos para as atividades ou processos de segurança a ser empreendida.

Atualmente, as inovações tecnológicas fomentam, a todo instante, modelos de gestão, os mais diversos, plenamente adaptáveis às organizações, principalmente naquelas instituídas para os serviços de segurança. Nessas organizações há talentosos gestores de segurança, nos diversos níveis organizacionais.

Por outro lado, na maioria das vezes, não se considera que a segurança deva ser entendida como uma função e vista de forma holística. Ignora-se, também, que uma organização de segurança é dividida em sistemas operacionais e organizacionais e deve se esforçar para satisfazer, e jamais ameaçar, as necessidades de proteção indispensáveis ao desenvolvimento das pessoas, dos bens (produtos e serviços) e preservação do meio ambiente.

Eis, portanto, a importância da segurança das pessoas, dos processos e demais bens patrimoniais e institucionais, no desenvolvimento político, social e econômico de uma Nação. Essa situação pode ser comprovada, na análise comparativa dos textos constitucionais de 1946 e 1988, onde se verifica que o termo segurança é amplamente utilizado, ora caracterizando um Direito assegurado ou um Mandado, ora adjetivado para conceituar determinadas funções estatais. Observa-se, também que, na Constituição de 1946, a segurança individual, citada no Art. 141, considerada entre os principais direitos, é considerada um dos valores supremos, a serem assegurados pelo Estado Democrático de Direito, de acordo com o texto do preâmbulo da Constituição da República Federativa do Brasil de 1988.

Mas, além de valor supremo, na Constituição Federal (CF) de 88, a segurança é considerada um direito devido aos brasileiros e aos estrangeiros residentes no País (Art. 5°); um direito social (Art. 6°) e um direito no trabalho (inciso XXII do Art. 6°). Caracteriza o Mandado competente e capaz de proteger direito líquido e certo, não amparado por "habeas-corpus" ou "habeas-data", quando o responsável pela ilegalidade ou abuso de poder for autoridade pública ou agente de pessoa jurídica no exercício de atribuições do Poder Público (inciso LXIX do Art. 5°). Quando adjetivado, o termo faz, ainda, referência à segurança do trânsito (inciso XII do Art. 23); segurança interna do país (inciso IV do Art. 85); segurança pública (Art. 144 e parágrafo 7° do mesmo citado artigo) e segurança nacional (Art. 173).

Quanto ao termo segurança pública, percebe-se que é descrito, pela primeira vez, na CF 88, evidenciando a condição de [...] dever do estado, direito e responsabilidade de todos [...], a ser [...] exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos: [...]. Não há outros esclarecimentos conceituais, na CF de 88, sobre a segurança pública ou ordem pública. A respeito da ordem pública, há quatro referências[2] específicas sobre o termo. Contudo, tem-se, nas lições de renomados juristas, que a ordem pública é a situação de convivência pacífica e harmoniosa da população, fundada nos princípios éticos vigentes na sociedade. Nesse caso, a ordem pública não se limita ao espaço público, mas, sugere a inexistência de uma ordem privada. Decorrente da CF de 88, o entendimento vigente da proteção individual, ao cidadão, e, coletiva, às comunidades, são realizadas com as atividades preventivas de polícia ostensiva, na preservação da ordem pública, de exclusividade das polícias militares. Isso ocorreria, apenas, nos espaços públicos, mais especificamente, nos logradouros públicos, enquanto que a atividade repressiva, na forma da Lei, ocorreria, inclusive, nos espaços, públicos ou privados, diversos dos logradouros. Essa situação tem sido verificada nos últimos dezenove anos.

Por outro lado, ainda que nos espaços públicos, diversos dos logradouros – porquanto de acesso ao público em geral – onde se desenvolvem atividades diversas, as atividades de proteção são executadas, de forma ostensiva, nos últimos vinte e seis anos, por setores orgânicos dos respectivos empreendimentos, ou por empresas especializadas de segurança contratadas,

nos termos da Lei 7102, de 21 de junho de 1983 recepcionada pela CF de 88. Dentre as modificações daquela norma, verifica-se que, a partir de 1994, foi-lhe inserido o conceito de segurança privada.

A despeito de muitas divergências, há esforços para compreender a segurança, desejada por todos. Neste ano, dois movimentos distintos se reportam à segurança pública. Na Campanha da Fraternidade, da Conferência Nacional dos Bispos do Brasil, com o tema: Fraternidade e Segurança Pública. Também, nas atividades preparativas – que ocorrem em diversas localidades do Brasil – para a 1ª Conferência Nacional de Segurança Pública, a ser realizada, em Brasília, no período de 27 a 30 de Agosto de 2009.

Mas, independente de ser adjetivada, ou do respectivo espaço onde atue desde que observe o mandamento jurídico vigente, a segurança não pode ser vista de forma míope, segmentada ou divergente. Deve-se discuti-la de foram ampla, não-segmentada e convergente em favor do bem-comum devido ao cidadão, às comunidades e às atividades produtivas, sob o Pálio da Lei e da Ordem.

O fato é que a segurança é um processo[3] de proteção nos espaços públicos e privados. Tanto que efetivada após criteriosa análise diagnóstica, indica o emprego adequado de recursos humanos, tecnológicos e gerenciais, com o objetivo precípuo de evitar – e minimizar – os impactos dos perigos às pessoas, bens patrimoniais e demais ativos tangíveis e intangíveis, através da prevenção e recuperação de perdas[4] e danos. Os perigos são, normalmente, caracterizados pelos riscos, em função das vulnerabilidades, físicas[5] e materiais[6], e das ameaças ou desastres terroristas[7]; criminosos[8]; industriais e tecnológicos[9]; naturais[10]; ambientais[11] e político-econômicos[12].

Até aí, tudo bem. A gestão da segurança transcorre sem nenhuma novidade!

Mas, o verdadeiro desafio emerge diante da indesviável necessidade de os gestores de segurança ousarem um pouco mais! Isso quer dizer dar práxis à teoria que define o gerenciamento bem-sucedido, firmado no entendimento capaz de conceituar e estabelecer critérios, alcançáveis e mensuráveis. Essa situação não será possível, quando se tem estratégia. Daí, a gestão estratégica da segurança destinada a ampliar o limitado alcance e a inflexibilidade do planejamento estratégico e favorecer a verificação periódica, individual e coletiva, dos envolvidos nos processos organizacionais, com vistas a objetivos bem-sucedidos.

Assim, o objetivo do texto é colaborar com os gestores da segurança, no contexto da gestão estratégica da segurança, a partir da seguinte indagação: as estratégias clássicas auxiliam a compreensão, formulação, implementação e monitoramento de estratégias de segurança mais efetivas?

Os fundamentos da estratégia são demonstrados, neste texto, em duas partes específicas. Na primeira, denominada visão de conjunto da estratégia, há orientações sobre o escopo político e conceitual, finalidade, subdivisões e alguns aspectos fundamentais à decisão e aplicação da estratégia.

Na segunda parte, o foco é direcionado para a arte da estratégia desde tempos remotos, no início das primeiras guerras, até nossos dias, quando a estratégia tem sido compreendida e difundida, a partir de ambientes acadêmicos, por meio de a criatividade do artesão, centralização do cliente, regeneração e revolução organizacional, capacidade de ser diferente na arte da execução.

Na formulação, implementação e monitoramento da estratégia de segurança, são destacadas os dois momentos do desenvolvimento da estratégia ex ante e da estratégia ex post. Destaca-se a utilização do Balanced Scorecard, indispensável ferramenta do sistema de gestão estratégica, com as orientações para a elaboração de um mapa estratégico e as precauções adicionais na implementação e monitoração da estratégia da organização de segurança.

2 VISÃO DE CONJUNTO DA ESTRATÉGIA

A visão de conjunto facilita a focalização da estratégia[13] e clarifica o entendimento conceitual que favorece a formulação de estratégias. Nesse sentido, o propósito é demonstrar alguns fundamentos que compõem a arte da estratégia aplicada, apesar de o nome estratégia ser mencionado intensamente no cotidiano organizacional, a arte da estratégia é pouco compreendida e, ainda, menos praticada.

2.1 A Arte da estratégia

A compreensão do que é estratégia passa necessariamente pelo exato entendimento do que é política[14]. Esse termo expandiu-se por meio da clássica obra de Aristóteles, intitulada Política, e, nos tempos atuais tem significação mais comum de arte ou ciência do Governo. Discorre, sobre a natureza – funções e divisão do Estado – e as várias formas de Governo, independente de serem intenções meramente descritivas ou também normativas, dois aspectos dificilmente discrimináveis, sobre as coisas da cidade[15].

Da política, considerada arte ou ciência do governo, emerge o poder, ou a capacidade de estabelecer os objetivos desejáveis e capazes de tornar a organização bem-sucedida. Mas, isso será possível, somente se houver decisões coerentes e utilização adequada dos meios disponíveis e necessários. Eis o papel fundamental da estratégia, uma arte simples, mas toda de execução, na sábia expressão de Napoleão Bonaparte[16].

O tempo evidenciou a tendência de clarificar a relação entre a estratégia e a política. Primeiro, com Clausewitz, nas afirmações de que a guerra é a continuação da política por outros meios. Depois, com Liddell Hart, ao afirmar que a melhor estratégia é aquela que atende ao objetivo político por meio de hábeis demonstrações de força, pela mobilidade, eventualmente sem travar a batalha. Por fim, com Beaufre, ao enfatizar que a guerra total é concebida em nível de política governamental, que fixa os domínios das estratégias militares, políticas, econômicas e diplomáticas[17].

Mas, foi a partir de o termo grego strategos[18] – surgido, provavelmente, no Século IV a.C. – que se obteve a informação preliminar do termo estratégia[19] e as respectivas derivações. Há, ainda, registros históricos, noticiando que, nos últimos sete séculos, as lideranças detentoras das decisões políticas e das ações estratégicas realizaram governos bem-sucedidos, principalmente àqueles fiéis às lições de Maquiavel e Clausewitz. Isso porque souberam dimensionar adequadamente as duas parcelas fundamentais de governo e a utilizar, também, a tática, às vezes confundida com a estratégia, e a logística, no momento certo e nos lugares apropriados.

Porém, para se compreender o que é a estratégia, é preciso cuidado e considerar, pelo menos, três inconveniências[20] consideráveis. A primeira delas é sobre o próprio nome, estratégia, pois, a despeito de citado com frequência, as realidades que o encobrem são, geralmente, ignoradas. Certamente, porque essa velha palavra designou, durante muito tempo, apenas a ciência e a arte do comandante-chefe. Eis, portanto, um dos motivos porque a estratégia não foi assimilada pelo grande público, nem nos meios militares, onde se continua a pensar técnica e taticamente[21].

Outra inconveniência é o entendimento de que estratégia, enquanto a arte de fazer a força seja exclusivamente uma arte militar. Esse entendimento prevaleceu durante algum tempo, pois, àquela arte, comparava-se a estratégia e, depois, a tática e a logística. Ora, a tática – ou a arte de empregar as armas no combate para obter o melhor rendimento – e a logística – ou a ciência dos movimentos e dos suprimentos[22] – são artes análogas à arte do engenheiro, porquanto cuidam de coisas materiais. Assim, situada em plano diverso daqueles ocupados pela política, tática e logística, a estratégia repousa no jogo abstrato, resultante da oposição de duas vontades[23].

A terceira inconveniência é apresentada em duas partes. Na primeira, ressalte-se, a estratégia não pode mais ser apanágio dos militares, e, na segunda, precisa perder seu caráter esotérico e especializado. Quando isso acontecer, a estratégia será o que são as outras disciplinas, e o que ela sempre deveria ter sido: um corpo de conhecimentos cumulativos, que se enriquece a cada geração, em lugar de um redescobrimento perpétuo, ao azar das experiências vividas. [24]

Há, ainda, orientações[25] especificando que a política é a arte de fixar objetivos e orientar o emprego dos meios necessários à sua conquista, e a estratégia é a arte de preparar e aplicar o poder para conquistar e preservar objetivos, superando óbices de toda ordem. Assim, à Nação brasileira, foi repassada a exata dimensão do significado dos conceitos de Política e Estratégia – Nacional, de Estado e de Governo – que têm a finalidade de orientar a aplicação do Poder Nacional, fundamentado – no homem, terra e instituições – e manifestado por meio das expressões política, econômica, psicossocial, militar e de ciência e tecnologia. Esses fundamentos doutrinários são pilares para empreendimentos de segurança. Soma-se, ainda, a importância da estratégia nas relações – política e poder – organizacionais. Eis um motivo de reflexão sobre a análise da estratégia.

Nesse sentido, é aceitável rejeitar[26] qualquer conceito de estratégia baseado unicamente no antigo entendimento de estratégia militar. Isso porque, a arte de empregar as forças militares para atingir resultados fixados pela política não visam apenas os objetivos militares, em tempos de paz ou de guerra. Amplia-se, então, a utilização do conceito, exclui-se a possibilidade de prevalência de um único segmento e ratifica-se o verdadeiro entendimento da estratégia, que é a arte de fazer a força concorrer para atingir os objetivos estabelecidos pela política.

Então, fica claro que não há uma única estratégia nas organizações, tampouco há predominância de uma estratégia sobre as demais. Sabe-se, contudo que, ao longo dos últimos séculos, as estratégias militares foram as que mais prosperaram – associadas aos grandes conflitos travados nos arredores do mundo – e adaptadas, de forma bem-sucedida, às mais diversas atividades das organizações produtivas. Essas organizações aprenderam que o escopo político organizacional delineia os objetivos a serem alcançados num horizonte estratégico possível, inclusive, com meios necessários e exequíveis. Assim a finalidade da estratégia é atingir os objetivos fixados pela política, com a utilização da melhor maneira os meios que se dispõe[27].

Com efeito, há, basicamente, duas opções básicas, que se desdobram, no tempo e no espaço, em função da melhor decisão. Na primeira opção, o objetivo decorre da necessidade, ou iniciativa, de conquistar e ocupar uma posição e/ou um espaço mais favorável, num menor tempo possível e com recursos menos dispendiosos. Nesse caso, alcançam-se os objetivos, com ações ofensivas, naturais ou impostas, consequentes de imposições de determinada necessidade, ou vontade.

Na outra opção básica, o objetivo decorre da necessidade, ou iniciativa, de defender posições e/ou espaços ameaçados,

num menor tempo possível e com recursos menos dispendiosos. Desenvolvem-se, portanto, ações defensivas para se alcançar os objetivos previstos.

Para alcançar os objetivos estabelecidos, utilizam-se, então, ações ofensivas e defensivas, direta ou indiretamente, dependendo do tempo, lugar e meios disponíveis. Por isso, é certo que uma estratégia se consolida plenamente com a decisão consequente de uma escolha acertada e de adequada combinação dos meios disponíveis. Na escolha é muito importante confrontar nossas possibilidades com as vulnerabilidades do adversário[28].

Os meios utilizados pela estratégia são: materiais e morais. Sem esses meios não se formulam, implementam e monitoram estratégias capazes de tornar os objetivos exequíveis, mensuráveis e consistentes.

A estratégia, embora una, pelo seu objeto e pelo seu método, se subdivide em estratégias especializadas[29], de acordo com a situação. Nesse caso, pode-se afirmar que há, basicamente, duas estratégias fundamentais que se complementam e asseguram a unidade dos esforços capazes de alcançar os objetivos estabelecidos. A primeira é denominada Estratégia Geral ou Grande Estratégia. A outra é denominada Estratégia Operacional. A Estratégia Geral se desdobra numa verdadeira pirâmide de estratégias distintas e interdependentes. Mas, a cada uma delas, há lugar para uma categoria distinta de estratégia, denominada Estratégia operacional.

A Estratégia Organizacional/Empresarial é formulada, implementada e monitorada com a finalidade de alcançar os objetivos organizacionais estabelecidos e relacionadas às diversas atividades da organização. Desse modo, tem-se, consequentemente, as denominadas estratégias de pesquisa & desenvolvimento, de produção de bens e/ou serviços; comerciais e/ou de marketing; financeiras; de recursos humanos e Jurídico-Legais, dentre outras, formuladas de acordo com as dimensões e importância da organização.

O objetivo da estratégia consiste na escolha do ponto decisivo, em função das vulnerabilidades e na escolha da manobra preparatória para alcançar o ponto decisivo escolhido. Assim, duas manobras preparatórias se opõem, mutuamente. Em consequência, logrará êxito aquele oponente que desestabilizar a manobra do adversário e conduzir a respectiva manobra com liberdade de ação e economia de meios. Nesse sentido, a essência da estratégia é atingir o ponto decisivo graças à liberdade de ação obtida por uma boa economia de meios. [30]

Na decisão estratégica[31], deve-se considerar, ainda, o raciocínio estratégico em relação ao raciocínio tático, logístico ou político. O raciocínio tático ou logístico obedece a um metodismo que orienta a aplicação racional dos meios disponíveis para atingir um dado resultado. Ao raciocínio político incumbe apreciar aquilo que a opinião deseja, ou pode admitir, e confere lugar preponderante à psicologia e à intuição. Por sua vez, o raciocínio estratégico, deve combinar dados psicológicos e materiais, através de uma elaboração abstrata e racional. Resulta, portanto, da análise e da síntese diagnóstica que propicia uma boa escolha, ou decisão.

Na decisão estratégica exercita-se, portanto, a arte de escolher bem. A melhor escolha será aquela em que se consegue a supremacia de possibilidades em confrontação com as vulnerabilidades do oponente. Os resultados mais favoráveis serão alcançados pelo oponente que detiver a necessária autoridade de cooptação, negociação, dissuasão ou confronto.

A melhor escolha consiste, então, em saber conjugar o tempo, o lugar e a quantidade dos meios disponíveis segundo o fator de manobra, as doutrinas de manobra e o fator de variabilidade[32].

Na dialética da disputa, o fator manobra direciona os demais elementos da decisão e assegura a iniciativa, considerado o fator essencial da manobra, caracterizada pela metáfora do teclado do jogo estratégico[33]. Nesse caso, o fundamento principal é combinar os tipos de ações ofensivas e defensivas e tomar a decisão adequada.

Utiliza-se, normalmente, a guisa de ilustração de um duelo entre dois competidores, uma disputa entre dois esgrimistas. Cada um deles pode utilizar as ações ofensivas – de ameaçar, enganar, fatigar, fingir, forçar, perseguir e surpreender – ou defensivas – de desengajar, esquivar, guardar, parar, responder e romper[34]. A melhor decisão será do oponente que for capaz de concentrar, dispersar, economizar, aumentar e reduzir, no tempo e lugar certos, os meios disponíveis por intermédio de cada uma das ações ofensivas ou defensivas.

Na formulação de estratégias para a organização de segurança, os gestores considerarão as ações adequadas, ofensivas ou defensivas, para as diversas atividades ou processos desenvolvidos pela organização de segurança.

Afinal, se a estratégia é o meio da aplicação da política, a tática é o meio da aplicação da estratégia. Não existe, portanto, uma grande tática. As táticas devem subordinar-se à estratégia, não o contrário. A estratégia não deve, apenas, escolher as táticas. Deve, igualmente, orientar a evolução das táticas e a movimentação da logística, a fim de que estas possam desempenhar seu papel necessário em vista da decisão[35].

2.2 A arte da estratégia aplicada

A arte da estratégia está presente nas atividades do homem, em toda a história da civilização, e, mais intensivamente, nesses

tempos de modernidade, conforme se verá a seguir, nos feitos da guerra e na gestão das organizações.

2.2.1 Na guerra

Há registros históricos indicando que as fontes da arte da guerra encontravam-se no Médio Oriente, no Oriente mais distante, e no Ocidente. No Médio Oriente, foram escritos os textos da Bíblia Sagrada[36], onde se verifica, primeiramente, a existência do Deus dos Hebreus que é, ao mesmo tempo, o Senhor da guerra – YHWH[37] Nissi – e o Senhor da paz – YHWH Shalon. Há, no Antigo Testamento, pelo menos, 209 referências sobre a guerra e 192 sobre a paz. Ainda, no Novo Testamento, há 15 referências sobre a guerra e 86 sobre a paz. Nessas citações, há informações expressas ou indicativas sobre os reinados de Saul, Davi e Salomão e dos impérios Assírio, Babilônico, Persa, Grego e Romano, de onde se destacaram intrépidos estrategistas, tais como: Alexandre, Dario, Aníbal, dentre outros, além dos imperadores romanos, notabilizados pela condição de "senhores da guerra" no mundo ocidental.

Encontra-se, também, no Livro de Êxodo, nos Textos Sagrados, no Capítulo 18, um diálogo[38], entre Moisés e o sogro, Jetro, sobre os primórdios da gestão de pessoas. Especificamente, sobre a estratégia, na arte da guerra, há relatos, nos doze primeiros capítulos do Livro de Josué, destacando movimentos preparatórios, emboscadas e decisões estratégicas que levaram o líder hebreu a lograr êxito sobre 31 reis que dominavam na região do Médio Oriente.

Do Oriente mais distante, chegou até nós, os relatos de Sun Tzu[39] enfatizando os termos: preparativos, comando, comandante, posicionamento estratégico, vantagens e poder, vencer antes, manobras, mudanças, movimentação, observação do terreno, classificação dos terrenos, uso do fogo e usando espiões[40]. Tem-se, portanto, que Sun Tzu ou mestre Sun produziu o mais antigo tratado militar da história da humanidade [...], provavelmente escrito por seus discípulos pelo ano 500 a.C. [41]

Os temas estratégicos de Sun Tzu têm importância singular, inclusive, pela ampla divulgação e aplicabilidade evidenciadas nos últimos séculos. Pode-se afirmar que o texto de A Arte da Guerra constitui o mais antigo tratado militar da história da humanidade, mas, as primeiras orientações estratégicas de guerra, destacadas anteriormente, encontram-se nos Textos Sagrados, onde se verifica que Josué, no período entre 1400 e 1375 a.C., foi designado sucessor de Moisés[42] para conduzir os israelitas à terra de Canaã e cumpriu a missão com ousadia, intrepidez, coragem e inteligência, encontrada nos grandes estrategistas que já existiram.

Há, ainda, relatos, em a "Arte da Estratégia", sobre o "Livro dos Cinco Anéis" – Terra, Água, Fogo, Vento e Vácuo – que narra a experiência de Miyamoto Musashi. Além de destacar os principais pontos do livro citado, evidenciam-se, igualmente, alguns pontos específicos das filosofias que influenciaram os treinamentos militares chineses e japoneses[43].

No Ocidente, Frederico, o Grande, e Napoleão foram outros estrategistas na "arte da guerra", influenciados certamente pelas lições de estratégia propostas por Nicolau Maquiavel (1469-1527) em "Da Arte da Guerra". Atribui-se a esse escritor e estadista a formulação inicial dos conceitos de organização do exército, a hierarquia de comando, o Estado-Maior e os códigos de leis militares [...] formação de soldados e proclamou a suprema importância da disciplina.

2.2.2 Na criatividade do artesão

A criação de estratégias[44] é um processo altamente complexo e envolve os mais sofisticados, sutis e até mesmo inconsistentes processos cognitivos, humanos e sociais.

Ao ratificar[45] que a estratégia é uma das palavras mais utilizadas no ambiente empresarial, embora seja de origem do "pensamento militar", a estratégia é destacada comparativamente com a "criatividade do artesão", a fim de demonstrar que não é fruto de uma modelagem lógico-racional e convencional. A estratégia, ao contrário, é consequência de uma "manipulação criativa". Daí, o destaque dado à "analogia entre a criação da estratégia e a habilidade de um escultor", onde se verificam frequentemente a visão, intuição, criatividade, imaginação, domínio de detalhes e descoberta de novos padrões pela aprendizagem contínua que ocorre enquanto a obra é esculpida[46].

Mas, a criatividade do artesão encerra após a concretização da obra imaginada. Poderá ser admirada, ou odiada, por pessoas distantes do relacionamento do escultor. Por sua vez, a estratégia será boa ou má, após superar novos desafios emergentes, seja na fase da formulação, da implementação ou do monitoramento. Não há descontinuidade no processo, ao contrário. A efetividade de uma estratégia pode exigir modificações constantes e, quando isso acontece, há melhorias substanciais na consecução dos objetivos. Entretanto, esse entendimento foi ignorado durante muito tempo. Era visível a existência do fosso entre os "pensadores" e os "executores". A inexistência desse fosso é a condição que favorece a formulação e a implementação da estratégia. É a continuidade desejável para que a organização formule suas estratégias – com o comprometimento de todos os responsáveis, nas diversas fases – alcance os resultados satisfatórios.

2.2.3 Na centralização do cliente

A estratégia e o pensamento estratégico devem ser motivos de reflexão dos executivos comprometidos[47] com o sucesso do empreendimento. Não há possibilidades de buscar o desenvolvimento organizacional se a estratégia não for o conceito central do negócio e o cliente não for o foco principal do negócio.

A estratégia, Drucker adverte, exige conhecimento sobre o que é negócio empreendido e o que ele deveria ser. Por isso, toda organização opera sobre uma teoria do negócio, ou um conjunto de hipóteses que respondem aos seguintes questionamentos: Qual é o nosso negócio? Quais são nossos objetivos? Como são definidos os resultados pretendidos? Quem são nossos clientes? Que valor eles dão pelo que pagam?

Outro alerta do renomado guru aos condutores de negócios enfatiza que não basta querer fazer. É preciso saber fazer, para fazer bem feito. Consequentemente, somente faz bem feito quem domina o conhecimento sobre o que será feito. Isso significa "incorporar a reflexão e o conhecimento à ação estratégica", que "é uma teoria dos negócios por excelência" e no centro da teoria dos negócios, a partir do início da decisão de produzir um bem ou prestar um serviço, o foco central é o cliente. Tanto que "na definição da finalidade e da missão da empresa há somente um enfoque, um só ponto de partida: o cliente. O cliente define o negócio", pois, "só existe uma definição válida para a finalidade de uma empresa: criar cliente". [48]

2.2.4 Na regeneração e revolução organizacional

Nas três últimas décadas do século passado, a estratégia foi – e ainda continua – tema de estudos acadêmico-empresariais em várias partes do mundo. Especificamente, a colaboração[49, 50] de Gary Hamel e C.K. Prahalad, na regeneração e revolução da estratégia, ocorreu em quatro aspectos distintos. No primeiro momento emergiu a proposta de a organização competir no futuro a partir de uma prática utilizando os conceitos de intenção estratégica[51], competências essenciais[52], arquitetura estratégica[53] [...]. São conceitos que facilitam o entendimento da gestão estratégica integrada, na proposta dos criadores do Balanced Scorecard, enfatizado neste texto.

O segundo aspecto da colaboração de Hamel e Prahalad refere-se a pouca dedicação dos executivos responsáveis pela formulação das estratégias. Essa situação é consequência do envolvimento dos estrategistas com questões especificamente operacionais, deixando de envolver-se com o processo de criatividade e de implementação da estratégia. Nessa direção, os executivos precisam entender[54] que diminuir o tamanho, ser eficiente e tomar decisões rápidas, são importantes e necessárias, mas, às organizações comprometidas com resultados satisfatórios, impõem-se a capacidade de se reavaliar, regenerar as estratégias centrais e reinventar cada vez mais o respectivo setor.

A forma como utiliza a estratégia na organização ou o ensino praticado nas escolas de administração são pontos criticados e constituem o terceiro aspecto da colaboração de Hamel e Prahalad. O quarto aspecto da colaboração de Hamel e Prahalad indica a importância e o desafio das organizações na formulação de estratégia inovadora[55], criativa[56] e revolucionária,[57] para sobreviverem diferentemente das demais.

2.2.5 Na capacidade de ser diferente

A contribuição de Michael Porter para arte de ser diferente indica que a organização deve buscar as condições que a diferenciam das demais. Isso significa que o propósito de uma organização – instituição ou nação – é gerar riquezas para os stakeholders,[58] por meio de uma estratégia competitiva capaz de gerar vantagem competitiva.

O caminho para a geração da riqueza, numa organização, é a adoção de uma estratégia competitiva. Significa buscar uma posição competitiva favorável em uma indústria, a arena fundamental onde é verificada a concorrência. A estratégia competitiva visa a estabelecer uma posição lucrativa e sustentável contra as forças que determinam a concorrência na indústria[59].

A geração da riqueza não está centrada única e exclusivamente nos ganhos financeiros, mas na capacidade que assegure uma vantagem competitiva para os envolvidos na produção, distribuição e consumo de bens e serviços.

A vantagem competitiva é o principal foco da organização que se esforça para ser diferente, a fim de gerar valores em cada uma das etapas produtivas. Isso significa que não basta ter eficácia operacional (reengenharia, reestruturação, melhoria contínua, etc.), é preciso ter posicionamento estratégico diferenciado[60]. Desenvolver a eficácia operacional significa ter atividades semelhantes melhor que as dos concorrentes, melhorada pela convergência competitiva. Mas, é no posicionamento estratégico que a organização realiza atividades diferentes daquelas das concorrentes ou realizam atividades semelhantes de maneira diferente[61]. Fica, portanto, evidente o que a organização deve fazer para tornar-se diferente. No conceito atualizado de estratégia competitiva[62], há cristalina orientação de que uma estratégia competitiva precisa ser diferente, diferenciar-se ao máximo. Isso significa escolher deliberadamente um conjunto diferente de atividades em relação aos concorrentes para fornecer um mix único de valor[63].

2.2.6 Na execução da estratégia

Muitos questionamentos relacionados com a estratégia – seja na formulação ou na implementação, que preocuparam empresários, executivos e analistas de negócios – encontraram respostas no Balanced Scorecard de Robert Kaplan e David Norton[64]. Para esses autores, o conjunto de fatores que geraram a raiz do problema é constituído pela estratégia competitiva um pouco abstrata; pela dificuldade dos executivos da alta administração em traduzir a estratégia em objetivos da organização e a resistência natural das pessoas, em conseqüência da falta de entendimento do significado da estratégia e dos sistemas gerenciais.

As diversas considerações de Kaplan e Norton sobre a estratégia contribuem para a reflexão de todos no ambiente organizacional. Especificamente, são destacadas aquelas que afirmam que a estratégia: é um passo de um processo contínuo; é uma hipótese; consiste em temas estratégicos complementares; equilibra forças contraditórias; descreve uma proposição de valor diferenciada; alinha as atividades internas com a proposição de valor; transforma os ativos intangíveis.

Após essas considerações sobre os fundamentos essenciais da estratégia, serão analisados alguns aspectos funcionais que ajudarão a compreender os passos necessários para formulá-la, implementá-la e monitorá-la.

3 FORMULAÇÃO, IMPLEMENTAÇÃO E MONITORAMENTO DE ESTRATÉGIAS DE SEGURANÇA

A organização de segurança competitiva e bem-sucedida não apareceu num passe de mágica! Ao contrário, é programada e reprogramada e sobrevive, mesmo nos tempos de crise, porque tem o foco na gestão estratégica. Incorpora, sempre que necessário, as técnicas de gestão que orientam o downsizing, a reengenharia, o benckmarking e a qualidade total. Não se acomoda no ambiente intensivo de informações, utilizam-nas para agregar valores, e tudo faz para "aprender a aprender" e para formular, implementar e monitorar estratégias competitivas[65].

Os gestores estratégicos da segurança compreendem que a estratégia tem "dupla acepção de 'diretriz' e de 'curso de ação'" que a diferenciam em estratégia ex ante[66] e estratégia ex pos[67]. Tem-se, então, que as etapas desenvolvidas pelas estratégias ex ante e ex post correspondem ao processo decisório que sintetiza a formulação, implementação e monitoramento da estratégia de uma organização. Nessas, utiliza-se a Metodologia do Balanced Scorecard (BSC).

A melhor compreensão e a utilização do BSC é saber que essa importante ferramenta de gestão não é um sistema de controle gerencial ou um conjunto de indicadores. Tem o papel fundamental de colocar a visão em movimento, narrar a história da estratégia, criar consciência estratégica nos colaboradores, explicitar o destino estratégico da organização e estimula o diálogo na organização[68].

O BSC enfatiza que há quatro perspectivas de valor[69] – a financeira, do cliente, dos processos internos e de renovação e aprendizagem – são capazes de estimular, respectivamente, o diálogo entre a estratégia e os acionistas; os diferentes grupos de clientes; os líderes dos processos de negócios e os colaboradores da organização de segurança. É necessária a compreensão de todos que a missão e visão devam gerar os temas estratégicos, que geram os objetivos estratégicos, para cada uma das perspectivas e, no contexto de cada perspectiva, os objetivos estratégicos são desdobrados em medidas[70], metas[71] e iniciativas[72] estratégicas.

Numa organização de segurança orientada para a estratégia, os princípios fundamentais e indispensáveis à implementação do BSC, segundo os autores[73], são: traduzir a estratégia em temos operacionais; alinhar a organização à estratégia; transformar a Estratégia em tarefa de toda a organização; converter a estratégia em processo contínuo; mobilizar a mudança por meio da liderança executiva.

Nesse sentido, é importante esclarecer que o conhecimento do ambiente, interno e externo, de uma organização de segurança é condição indispensável para se saber exatamente onde se encontra e para onde se deseja ir. São fundamentais as potencialidades organizacionais e os desafios que se lhe impõem, com a finalidade de encontrar um equilíbrio desejável e tirar o melhor proveito possível rumo ao sucesso. Eis a importância da análise dos cenários possíveis e das forças macroambientais econômicas, sociais, político-legais, tecnológicas, ambientais e culturais e as respectivas variáveis que impactam as perspectivas de valor pretendidas pela organização de segurança.

No levantamento de outras informações que geram o conhecimento do ambiente organizacional, são utilizados diversos modelos ou técnicas[74], mas, os mais utilizados são o das forças competitivas e a análise de SWOT[75].

Do modelo proposto por Michael Porter, Professor de Estratégia de Harvard, compreende-se que as forças competitivas são representadas pelos competidores, novos concorrentes, fornecedores, clientes e substitutos. São, portanto, determinantes do ritmo de produtividade e competitividade da organização de segurança.

As potencialidades internas – forças e fraquezas – e externas – oportunidades e ameaças têm sido mensuradas pela conhe-

cida Matriz SWOT. Com os dados e informações sintetizados na matriz, é possível estabelecer uma relação entre as atividades atuais e as futuras. Assim, podemos indagar sobre: o que é ruim (pontos fracos), nos dias atuais, e o que será ruim (ameaças) daqui a cinco, dez, vinte anos? Ou o que é bom (pontos fortes), nos dias atuais, e o que será melhor (oportunidades) daqui a cinco, dez, vinte anos?

Outra importante metodologia para se analisar os pontos fortes e fracos de uma organização é a utilização de a Cadeia de Valor demonstrada por Michael Porter como fonte de geração da vantagem competitiva. Entretanto, há uma advertência para que essa análise não considere a organização como um todo. Deve-se, então, distinguir, principalmente quais são as atividades primárias e quais são as atividades secundárias, e onde, como, quando e porque são desenvolvidas. Normalmente, nas atividades primárias, são desenvolvidas as tarefas criativas e físicas de um produto ou serviço, passando pelo processo de venda e entrega ou transferência, até os serviços que asseguram o relacionamento desejável com os clientes. As atividades secundárias incorporam a criação de valor, insumos, recursos humanos, serviços de administração e finanças e a infra-estrutura de tecnologia da informação e de comunicação.

Na conclusão da análise macroambiental, são evidenciadas as principais informações sobre as forças e fraquezas da organização e quais as ameaças e oportunidades devem ser consideradas na análise das alternativas estratégicas. Em conseqüência disso, os pontos fortes e pontos fracos de uma organização indicarão o que deve, ou não, ser feito para que os resultados sejam alcançados. Nesse sentido, na busca de alternativas estratégicas, os teóricos da Escola de Posicionamento estratégico[76], dentre eles Michael Porter, optam pela utilização das estratégias genéricas, combinadas entre si, ou entre as estratégias internas[77]. As estratégias genéricas, como o próprio nome indica, são utilizadas para caracterizar determinada indústria, inclusive, a de segurança, onde os competidores se estabelecem, com os bens e serviços produzidos, através de liderança de custo; diferenciação e enfoque[78]. Além disso, as estratégias internas são respostas naturais às análises do ambiente, interno e externo. A cada consequência das potencialidades e fragilidades percebidas na Matriz de SWOT, há uma estratégia específica, indicando se a situação é de sobrevivência, crescimento, manutenção ou desenvolvimento.

Assim, na proposição da política organizacional, definida segundo os valores, missão e visão, a estratégia traduz os objetivos, medidas, metas, indicadores e iniciativas estratégicas fixadas e como serão efetivamente executados.

Os objetivos indicam para onde a organização deseja ir. Tem-se, então, uma referência, um ponto de partida para que a liderança decida se a organização deseja crescer, ampliar a participação no mercado; aumentar a rentabilidade, superar a crise, fortalecer a marca e a imagem e melhorar o atendimento do cliente[79]. Esses objetivos – comuns a qualquer organização que deseja ser bem-sucedida – serão destacados em outros, mas, com o foco específico para o sucesso financeiro, à satisfação do cliente interno e externo e à melhoria dos processos desenvolvidos pela organização de segurança.

Nessa direção, na fase da estratégia ex post, implementa-se o BSC, com o desenho do mapa estratégico.

O mapa estratégico converte-se, para os membros de uma organização de segurança, num veículo de comunicação, num sistema de informação, num sistema de aprendizado e num importante fator de motivação e alinhamento. Por meio dele são decodificados os complexos processos; a alta administração monitora o cumprimento da estratégia e se operacionaliza a vinculação do planejamento estratégico e o planejamento operacional.

No mapa estratégico da organização de segurança – onde a essência principal é alinhar a visão à estratégia – são inseridos os objetivos estratégicos, medidas, metas e ações/iniciativas nas perspectivas de valor projetadas.

Comparado a um simulador de vôo, ao invés de um painel de controle, o mapa estratégico tem a vantagem de dispor as informações das quatro perspectivas num único relatório. Isso impõe a necessidade de elaborar objetivos claros, corretos e concisos para favorecer o entendimento – de quem atua localmente – e a clarificar a visão de quem precisa "enxergar" holisticamente a organização. Desse modo, percebe-se o desempenho, ao mesmo tempo, das perspectivas projetadas pela organização.

Na elaboração do mapa estratégico, é importante considerar o arranjo sistêmico dos componentes, no desdobramento das relações de causa e efeito, nos objetivos estratégicos e as perspectivas de gestão e as medidas, as metas e as ações. Nesse caso, [...] a estratégia se apresenta como um conjunto de hipóteses; [...] exige escolhas para se promover a integração entre os diferentes objetivos e, finalmente, numa abordagem holística, ela procura estabelecer relações de causa e efeito entre os diferentes objetivos das quatro perspectivas de valor[80].

O arranjo sistêmico dos componentes é a condição estabelecida pelo BSC para que ocorra a integração vertical (da estratégia à ação) e a integração horizontal (ou lateral) entre as perspectivas/dimensões da gestão[81], num desdobramento das relações de causa e efeito donde se observa uma sequência lógica e exequível de afirmações do tipo "se-então".

Após a definição dos objetivos, das metas e ações, a elaboração dos indicadores constitui outro passo fundamental. Não é recomendável utilizar muitos indicadores, mas a quantidade necessária que permite manter o foco na estratégia. É importante considerar que há diferença entre medidas de diagnóstico[82] e medidas estratégicas[83], uma vez que àquelas são necessárias, mas

não suficientes para o alcance dos objetivos de longo prazo. É importante considerar, também, o entendimento dos termos indicador e medida[84].

Na definição de medidas, não se deve começar pelo conjunto de indicadores usados na empresa e tentar encaixá-los no mapa. Deve-se utilizar a ordem inversa e verificar qual é a melhor forma de captar o alcance do objetivo estratégico. O recomendável é utilizar medidas genéricas[85] e específicas[86], mesmo que ainda não praticadas pela organização de segurança, o que será feito doravante. O fundamental é compreender e distinguir as medidas de tendência e de resultados[87].

Para cada medida define-se uma meta[88] de desempenho necessária para o cumprimento dos objetivos estratégicos e da estratégia considerada. As metas devem expressar as hipóteses sobre a magnitude e a velocidade de mudanças necessárias para o cumprimento da estratégia. É fundamental iniciar com o estabelecimento de metas de longo prazo. A lógica de causação é: o longo prazo determina o curto prazo. O curto prazo é uma imposição do que se quer no longo prazo.

Os objetivos estratégicos são alcançados com ações/iniciativas estratégicas. Para cada meta planeja-se uma ação.

Na implantação de um sistema de gestão estratégica integrada, há, certamente, muitas barreiras, principalmente porque se estabelecerá, antes de tudo, um sistema de monitoramento e mensuração das atividades desenvolvidas na organização. As pessoas são resistentes a qualquer forma de controle, a não ser que percebam a utilidade e os benefícios decorrentes.

Dentre as barreiras encontradas para a implementação do BSC, destacam-se: objetivos confusos; confiança não justificada nos sistemas de feedback informais; resistências geradas por imposição de sistemas de mensurações, sem envolvimento da equipe; armadilha da atividade: quando a empresa foca a mensuração da atividade e não dos resultados.[89]

Dentre os problemas frequentes, nos sistemas de mensuração, destaca-se[90] a predominância de medidas de curto prazo sobre as de longo – levando a sacrificar desenvolvimento de longo prazo por ganhos imediatos; dos aspectos financeiros sobre outros da realidade – linguagem dos ganhos, retornos etc.; de medidas de eficiência sobre as de eficácia – a produtividade ganha precedência sobre o valor do produto; de medidas de economia sobre as de eficiência – muitas vezes sequer a eficiência no consumo de recursos é apurada. As medidas apuram apenas o quanto se gastou de recursos e de medidas funcionais sobre as relacionadas com os clientes - foco no desempenho do departamento, sem considerar a satisfação dos clientes.

O sucesso da implementação inicia com a conscientização dos envolvidos de que a metodologia do BSC não é panacéia gerencial que cabe em todo e qualquer tipo de empresa e que pode ser implantado como uma "receita de bolo".

O BSC é uma ferramenta eficiente e eficaz. Quando implantado sem os equívocos percebidos em diversas experiências de implantação que muitas empresas que admitiram utilizar o BSC, quase três quartos das medidas ainda são financeiras, ou seja, não existe um verdadeiro balanceamento entre as medidas financeiras e não-financeiras[91].

Sobre a quantidade de indicadores – e qual será o mix mais indicado entre as diferentes perspectivas que o BSC deve conter? – a resposta é: a quantidade deve variar entre 20 e 25 indicadores (5 Indicadores - 22% - para a perspectiva financeira; 5 Indicadores - 22% -para a perspectiva do cliente; 8 Indicadores - 34% - para a perspectiva dos processos internos e 5 Indicadores - 22% - para a perspectiva de aprendizado e crescimento). [92]

Os desafios observados a partir de relatos de experiências de implantação ou mesmo de observações de outros autores[93], estão sintetizados em quatro situações possíveis – antes da decisão de implementar e durante a decisão de implementar, do desenho da implementação e da implementação propriamente dita.

4 CONCLUSÃO

As organizações de segurança, instituídas ou organizadas, têm histórias interessantes, desde o primeiro dia de funcionamento.

Com o tempo, a maioria delas, aprende, supera dificuldades, cria, experimenta e torna-se bem-sucedida. Na contabilidade aferida – seja pela satisfação dos usuários, quando a ela se referem favoravelmente, ou dos clientes e consumidores, maximizando os lucros, com a aquisição dos bens e serviços produzidos – a organização percebe o senso de utilidade.

Com a organização de segurança, a situação é idêntica, tanto a que visa lucros financeiros quanto a que deseja apenas a satisfação plena dos usuários dos serviços e bens produzidos.

Mas, para trilhar nessa direção, é imprescindível colocar o trem nos trilhos. Isso implica, invariavelmente, rever conceitos, compreender os processos e as atividades, re-planejar funções, adotar algumas medidas que podem abalar pré-conceitos, modificar tradições, causar dissabores, quase sempre adiados.

Porém, é preciso fazer alguma coisa. Lembre-se de ousar, descubra novas realidades, encontre uma estratégia que lhe ajudará a realizar uma gestão plena, competente e exitosa.

A estratégia é um meio a ser buscado pela organização de segurança, com a finalidade de gerar valor num continuum dinâmico que favorece a satisfação do cliente, consumidor e usuário, que remunera – e agrada – o bem ou serviço recebido, que foi desenvolvido adequadamente por pessoas satisfeitas.

A estratégia é uma proposta para que o continuum descrito seja desenvolvido por todos os participantes, num comprometimento pleno, de corpo e alma.

A estratégia é uma proposta de decisões desafiadoras para gestores que desejam ser verdadeiramente bem-sucedidos.

Se é imprescindível realizar atividades ou processos de segurança, nas mais variadas formas, funções, atividades ou adjetivações, realizá-las com a estratégia formulada, implementada e monitorada, segundo as teorias e técnicas ora apresentadas, é inadiável.

Notas Explicativas

1 Para a finalidade deste texto, a organização pode ser uma corporação, pública ou privada, uma empresa, ou um setor corporativo ou empresarial, independente do seu tamanho.

2 As referências encontram-se: no Art. 34 – quando se enfatiza a intervenção da União, nos Estados e Distrito Federal, diante do grave comprometimento da ordem pública – e, no Art. 136, quando menciona o poder do Presidente da República para decretar, após ouvir o Conselho da República e o Conselho de Defesa Nacional, o estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social [...]. Depois no caput do Art. 144, destacado anteriormente, e no § 5° para definir que [...] às polícias militares cabem a polícia ostensiva e a preservação da ordem pública [...].

3 Para a finalidade deste texto, é o arranjo de ações, operações ou atividades lógicas, físicas, biológicas químicas e funcionais de uma organização de segurança.

4 "Perda é o rompimento da relação possuidor-objeto. É importante ressaltar a diferença entre dano e perda. Dano é a alteração no objeto. Perda é alteração na relação possuidor-objeto. Quando o corpo sofre dano, a pessoa sofre perda. Se um carro é furtado, o proprietário tem perda mesmo que o carro não sofra danos".

5 A vulnerabilidade física (VF) é a exposição involuntária dos bens materiais do empreendimento, a despeito de estarem em área de segurança protegida ou exclusiva. Ocorre em conseqüência de portas (janelas, portões, etc.) de escritórios (alojamentos, armários, etc.) esquecidos abertos.

6 A vulnerabilidade material (VM) decorre do esquecimento involuntário, ou "voluntário" dos bens materiais do empreendimento em locais diversos daquele em que deveriam ser acondicionados.

7 Com utilização de bomba, produto químico, biológico, nuclear, veículo – aéreo ou terrestre – com ou sem explosivo e seqüestro.

8 Com ameaças contra a vida, furtos e roubos (assaltos); extorsões, torturas, sequestros e cárceres privados.

9 Com incêndios, eletricidade, químicos, estruturas físicas, equipamentos mecânicos e radiação.

10 Com incêndios/descargas elétricas, inundação, tempestade, terremoto, furacão, epidemia humana ou animal.

11 Comprometimento da qualidade do ar, água, alimento.

12 Limitação, escassez ou falta de recursos básicos de abastecimento para as pessoas e os bens materiais indispensáveis à produtividade.

13 "[Do gr. strategía, pelo lat. strategia.] S. f. 1. Arte militar de planejar e executar movimentos e operações de tropas, navios e/ou aviões, visando a alcançar ou manter posições relativas e potenciais bélicos favoráveis a futuras ações táticas sobre determinados objetivos. 2. Arte militar de escolher onde, quando e com que travar um combate ou uma batalha. [Cf., nesta acepção, tática (2).] 3. P. ext. Arte de aplicar os meios disponíveis com vista à consecução de objetivos específicos. 4. P. ext. Arte de explorar condições favoráveis com o fim de alcançar objetivos específicos. 5. Fig. Fam. V. estratagema (2). (FERREIRA, 1999)

14 Matos (1996)

15 Bobbio (1998)

16 Beaufre (1998)

17 Matos (1998)

18 Estratego (é). [Do gr. strategós, pelo lat. strategu.] S. m. 1. General superior, ou generalíssimo, na Grécia antiga. (FERREIRA, 1999)

19 Ferreira (1999), Filho (2005), Júlio (2008) Luecke (2008), Sugai (2005), Tavares (2005) Vasconcelos Filho e Pagnoncelli (2001), dentre outros autores.

20 Beaufre (1998)

21 Beaufre (1998)

22 Beaufre (1998)

23 Beaufre (1998)

24 Beaufre (1998)

25 Com o tempo, Maquiavel, em O Príncipe e A arte da guerra, Clausewitz, em Da guerra, Liddell Hart, em Estratégia, Meira Matos, em Estratégias Militares Dominantes e André Beaufre, com a Introdução à Estratégia, concorrem para o estabelecimento das doutrinas sobre as estratégias militares.

26 Beaufre (1998)

27 Beaufre (1998)

28 Beaufre (1998)

29 Beaufre (1998)

30 Beaufre (1998)

31 Beaufre (1998)

32 Beaufre (1998)

33 Beaufre (1998)

34 Beaufre (1998)

35 Beaufre (1998)

36 BÍBLIA SHEDD (1997)

37 Pronuncia-se: yahwé que, em português, é Jeová.

38 "[...] representa o povo perante Deus, leva as suas causas a Deus, ensina-lhes os estatutos e as leis e faze-lhes saber o caminho em que devem andar e a obra que devem fazer. Procura dentre o povo homens capazes, tementes a Deus, homens de verdade, que aborreçam a avareza; põe-nos sobre eles por chefes de mil, chefes de cem, chefes de cinquenta e chefes de dez; para que julguem este povo em todo tempo. Toda causa grave trarão a ti, mas toda causa pequena eles mesmos julgarão; será assim mais fácil para ti, e eles levarão a carga contigo. [...]" (g.n) (BIBLIA SHEED, 1997)

39 "[...] difundida em toda a Ásia continental e no Japão, A Arte da Guerra somente chegaria à Europa em 1782, levada pelo Jesuíta francês Joseph M. Amiot, que vivia na China e a traduziu para esse idioma". Entretanto a obra permaneceria virtualmente ignorada no Ocidente até 1910, quando o Dr. Lionel Giles, destacado sinólogo do Departamento de Obras Impressas e Manuscritos do Oriente do Museu Britânico, fez a primeira tradução para o Inglês consistente e digna de confiança. Ainda hoje, decorrido quase um século, o trabalho de Giles impõe-se, pela erudição e fidelidade ao original, como marco de referência no estudo da obra de Sun Tzu e fundamenta numerosos ensaios e interpretações que o tema continuamente inspira". SUN TZU (2003)

40 Sugai (2005)

41 Sugai (2005)

42 "Disse o Senhor a Moisés: Toma Josué, filho de Num, homem em quem há o Espírito e impõe-lhe as mãos; apresenta-o perante Eleazar, o sacerdote, e perante toda a congregação; e dá-lhe, à vista deles, as tuas ordens. Põe sobre ele a tua autoridade, para que lhe obedeça toda a congregação dos filhos de Israel." (BÍBLIA SHEED, 1997)

43 Sugai (2005)

44 Mintzberg (2000) apud Filho (2005).

45 Filho (2005)

46 Filho (2005)

47 Peter Drucker apud Filho (2005).

48 Peter Drucker apud Filho (2005).

49 Filho (2005)

50 Tavares (2005)

51 "[...] é a expressão utilizada por Hamel e Prahalad para substitui o conceito de visão estratégica. (FILHO, 2005)

52 Hamel e Prahalad "utilizam a metáfora da organização como uma árvore para explicar o conceito: „O tronco e os galhos principais são os produtos essenciais; os galhos menores, as unidades de negócios, as folhas, flores de frutos são os produtos finais. O sistema de raiz provê a nutrição, a sustentação e a estabilidade é a competência essencial". As competências essenciais [...] representam acúmulo paciente e persistente de capital humano e capital estrutural de uma empresa. [...] podem ser definidas como „o aprendizado coletivo da organização, especialmente como coordenar as diversas habilidades de produção e integrar as múltiplas correntes de tecnologia". (FILHO, 2005)

53 "É o elo de ligação entre a intenção estratégia e as competências essenciais da organização; é a forma como a organização aborda as oportunidades emergentes. A arquitetura estratégica „mostra à organização que competências ela precisa começar a desenvolver agora, que novos grupos de clientes precisa começar a atender agora, que novos canais deveria estar explorando agora para interceptar o futuro."

54 Hamel e Prahalad apud Filho (2005):

55 "[...] a estratégia é entendida como a inteligência e a imaginação de empresários, executivos e colaboradores da organização que possibilitam a regeneração de estratégias já superadas pelo novo contexto dos negócios". (FILHO, 2005)

56 "[...] a estratégia deve ser considerada como a capacidade de uma organização desenvolver as competências essenciais que irão contribuir para a concepção de novas propostas de valor para os clientes". (FILHO, 2005)

57 "[...] a estratégia deve ser elaborada para transformação não só da empresa, mas principalmente do setor de atividade em que ela atua, pos-

sibilitando a liderança, na competição pelas oportunidades do futuro." (FILHO, 2005)

58 "Os Stakeholders de uma empresa são os Acionistas, Donos, Investidores, Empregados, Clientes, Fornecedores / subministradores da empresa, Sindicatos, Associações empresariais, industriais ou profissionais, Comunidades onde a empresa tem operações: associações de vizinhos, Governos locais, Governos estatais, Governo nacional, ONGs e Concorrentes. Todos estes Stakeholders são beneficiados ou prejudicados como resultado das ações da própria empresa. Disponível em http://pt.wikipedia.org/wiki/Stakeholders, acesso em 31/01/08. 59 Porter (1996 a),

60 Porter (1996 a),

61 Porter (1996 a),

62 Porter (1996 a) apud Filho (2005)

63 Filho (2005)

64 Filho (2005)

65 Tavares (2005)

66 "É uma diretriz superior que orienta a coordenação de esforços e a alocação de recursos com vistas à consecução de um propósito, de um objetivo específico" COUTO (2004)

67 "É um curso de ação, envolvendo programas, planos ou projetos, que almeja a consecução de um objetivo". COUTO (2004)

68 Filho (2005)

69 Representam a estrutura por meio da qual o processo de criação de valor para os stakeholders é visualizado. Por meio desse modelo, a estratégia é traduzida em objetivos que permitem a avaliação da performance da organização [...]. FILHO (2005).

70 "As medidas (ou indicadores) nos permitem avaliar até que ponto as atividades e ações que deveriam estar sendo desenvolvidas na organização estão progredindo, sendo completadas, ou ainda merecendo o foco e a atenção dos colaboradores da organização. As medidas de desempenho, que levam em consideração o ambiente dos negócios, devem ser derivadas da estratégia de negócios e precisam estar encadeadas entre si, nas perspectivas de valor". FILHO (2005)

71 "É o que permite avaliar ao longo do tempo a evolução da empresa, da unidade de negócios, da área funcional ou do indivíduo em direção aos objetivos estratégicos definidos nas quatro perspectivas de valor. As metas podem ser retratadas por fórmulas (que mostram a relação entre as variáveis) ou apresentam por meio de textos que retratem análises qualitativas, julgamentos, percepções ou insights dos colaboradores de uma organização". FILHO (2005)

72 "São as ações que uma empresa deve realizar, nas quatro dimensões do Balanced Scorecard, para alcançar os objetivos estratégicos. As iniciativas devem ser priorizadas em função de seu impacto de curto, médio e longo prazo na geração de valor e fortalecimento da posição competitiva da empresa". FILHO (2005)

73 Filho (2005)

74 "Técnicas de avaliação da posição estratégica: Estrutura Estratégica de Andrews, Matriz Produto/Missão de Ansoff, Curva de Aprendizagem, Curva de Experiência, Curva do Ciclo de Vida de um Produto, Matriz de Crescimento/Participação – BCG, Matriz Histórica, Matriz Ambiental, Matriz Portfólio da Mckinsey, Matriz Arthur D. Little, Modelo AM-PN, Modelo de Análise Estratégica de Austin, Modelo Delta e Metodologia GUT". AZEVEDO E COSTA (2001)

75 "[...] o conceito de SWOT – forças (Strengths), fraquezas (Weaknesses), oportunidades (Opportunities), ameaças (Threats), ou em sua tradução FOFA, relacionando em ordem diferente os mesmos significados –, [...] nesse enfoque, o planejamento contempla a relação entre as condições externas e internas. Na primeira residem as oportunidades que a empresa pode usar para melhorar seu desempenho, e ameaças que podem afetá-la adversamente. [...] Nas condições internas afloram forças e fraquezas. As forças correspondem a recursos, habilidades, posição de mercado, patentes, capital humano, além de outras competências distintivas. As fraquezas podem levar a empresa a um fraco desempenho. Métodos de produção obsoletos, carências de recursos tecnológicos, política de incentivo inadequada, entre outros fatores, podem comprometer o desempenho da empresa." TAVARES (2005) Para Lueke (2008) é a "Análise que investiga os pontos fortes, os pontos fracos, as oportunidades e as ameaças enfrentadas por uma empresa ou unidade operacional." (LUECKE, 2008).

"As oportunidades são situações externas, atuais e futuras, que podem influenciar positivamente o desempenho da empresa. Ameaças são situações externas, atuais e futuras, que podem influenciar negativamente o desempenho da empresa. Forças são características ou qualidades da empresa, tangíveis ou não, que podem influenciar positivamente o desempenho da empresa. Fraquezas são características ou qualidades da empresa, tangíveis ou não, que podem influenciar negativamente o desempenho da empresa." VASCONCELOS FILHO e PAGNONCELLI (2001)

76 Há dez escolas de pensamento estratégico, consideradas prescritivas e descritivas. Cada uma delas, descritas a seguir, tem, respectivamente, uma visão do processo de formulação da estratégia, autores, mensagem pretendida e mensagem Realizada. Dentre as Prescritivas, destacam-se a de: Design - processo de concepção - Selnick; Newman; Andrews – Ajuste – Pense; Planejamento - Processo formal – Ansoff – Formalize – Programe; Posicionamento - Processo Analítico - Porter; Shendel; Hatten – Analise – Calcule. As descritivas são: Empreendedorismo - Processo Visionário - Schumpeter; Cole - Visione/Vislumbre – Centralize; Cognitivo - Processo Mental - Simon; March – Crie - Preocupe-se; Aprendizado - Processo Emergente - Lindblom; Cyert & March; Weick; Quinn; Prahalad & Hamel – Aprenda – Jogue; Poder - Processo de Negociação - Allison (micro) Pfeffer & Salanick; Atley (macro) – Promova – Entesoure; Cultural - Processo Social - Rhenman & Normann – Combine – Perpetue; Ambiental - Processo Reativo - Hannan & Freeman; Pugh et. al. -Reaja – Capitule; Configuração - Processo de Transformação - Chandler; Mintzberg; Miller; Miles; Snow - Integre, Transforme – Acumule. Há, ainda, outras escolas que orientam mais a implementação e não a formulação (ainda que a separação entre esta duas etapas seja mais de caráter didático do que efetivamente ocorre): Administração por autocontrole (Drucker, 1994); Balanced Scorecard (Kaplan; Norton, 1992, 1996 e 2000); Destruição criativa (Foster; Kaplan, 2001) e Modelos de Ruptura – ou "disruptivos" (Christensen; Overdorf, 2000). Mas, o pensamento estratégico continua

sua evolução. CARVALHO E LAURINDO (2007)

77 Tavares (2005)

78 Porter (1985)

79 Júlio (2005)

80 Filho (2005)

81 Costa (2006)

82 "As medidas de diagnósticos são aquelas que monitoram se o negócio permanece sob controle e indicam quando eventos excepcionais ocorrem exigindo atenção imediata". COSTA (2006)

83 "Medidas estratégicas são aquelas que definem a estratégia". COSTA (2006)

84 "Quando se pensa em indicadores, na prática das empresas, imediatamente se visualiza uma razão (financeira ou não). O mesmo não acontece com as medidas, que sugerem uma abrangência maior, incorporando resultados qualitativos. Independentemente de como a empresa prefira chamar, o importante é definir como o desempenho será medido para ser monitorado. COSTA (2006)

85 As medidas "genéricas, tais como participação de mercado, rentabilidade, satisfação do cliente etc. direcionam o resultado final a ser alcançado e, por isso, são conhecidas como medidas de resultado [...] guardam uma relação direta de causalidade entre ação e resultado esperado". COSTA (2006)

86 "As medidas específicas são aquelas que vão identificar como a rentabilidade, a satisfação do cliente e a participação do mercado serão alcançadas". COSTA (2006)

87 "As medidas de tendência sinalizam que o alcance daquelas metas levará ao alcance de outras metas relacionadas por causa e efeito. As medidas de resultado de resultado já guardam uma relação de causalidade entre ação e resultado esperado". COSTA (2006)

88 "A meta é a quantificação do desempenho desejado a ser medido. Devem ser para o curto prazo, para o médio e para o longo". COSTA (2006)

89 Costa (2006)

90 Costa (2006)

91 Costa (2006)

92 Filho (2005)

93 Costa (2006)

Referências bibliográficas

ANSOFF, H. Igor. A nova estratégia empresarial. São Paulo: Atlas, 1990.

AZEVEDO, Marilena Coelho de. COSTA, Helder Gomes. Métodos para a avaliação da postura estratégica. Caderno de Pesquisa em Administração. V.8, nº 2, Abril/Junho de 2001

BÍBLIA SHEDD. Antigo e Novo Testamento. Editor responsável Russell P. Shedd; traduzida em português por João Ferreira de Almeida. 2. ed. – Revista e atualizada no Brasil. São Paulo: Vida; Brasília: Sociedade Bíblica, 1997, p. 1913.

BEAUFRE, André. Introdução à estratégia. Tradução de Luiz de Alencar Araripe. Rio de Janeiro: Biblioteca do Exército (Coleção General Benício, v. 336), 1998, 156 p.

BOBBIO, Norberto. Dicionário de Polícia I Norberto Bobbio, Nicola Matteucci e Gianfranco Pasquino; trad. Carmen C, Varriale et ai.; coord. trad. João Ferreira; rev. geral João Ferreira e Luis Guerreiro Pinto Cacais. - Brasília: Editora Universidade de Brasília, 1ª ed., 1998. Vol. 1: 674 p. (total: 1.330 p.)

CARVALHO, Marly Monteiro de. LAURINDO, Fernando José Barbin, Estratégia competitiva: dos conceitos à implementação. São Paulo: Atlas, 2007, 227 p.

COSTA, Ana Paula Paulino da. Balanced Scorecard - Conceitos e Guia de Implementação. São Paulo: Atlas S.A., 2006, 90 p.

COUTO, Luiz. DIAS, Evanio Dias, MACEDO SOARES, T. Diana L. v. A. Três estratégias para turbinar a inteligência organizacional. Rio de Janeiro: Editora FGV, 2004, 272 p.

FILHO, Emílio Herrero. Balanced Scorecard e a gestão estratégica: uma abordagem técnica. Rio de Janeiro: Elsevier, 2005 - 5ª. Reimpressão.

HAMEL, G.; PRAHALAD, C. K. Competindo pelo futuro: estratégias inovadoras para obter o controle do seu setor e criar os mercados de amanhã. Rio de Janeiro: Campus, 1995.

JÚLIO, Carlos Alberto. A arte da estratégia: pense grande, comece pequeno e cresça rápido. Rio de Janeiro: Elsevier, 2005, 9ª reimpressão. 150 p.

KAPLAN, R. S.; NORTON, D. P. A estratégia em ação: balanced scorecard. Tradução de Luiz Euclydes Trindade Frazão Filho. Rio de

Janeiro: Elsevier, 1997, 344 p. 24ª reimpressão.

_____. Organização orientada para a estratégia: como as empresas que adotam o balanced scorecard prosperam no novo ambiente de negócios. Rio de Janeiro: Campus, 2000a. _____. Mapas Estratégicos. Rio de Janeiro: Campus, 1ª ed. - 2004 - 504 p.

LUECKE, Richard. Estratégia. (Harvard Business Essentials - Consultoria de David J. Collins) tradução Ryta Magalhães Vinagre. Rio de Janeiro: Record, 2008.

MACHIAVELLI, Niccolò. A arte da guerra. Tradução de Jussara Simões. Rio de Janeiro: Elsevier, 2003. 218p.

_____. O Príncipe – a natureza do poder e as formas de conservá-lo. Tradução de Cândida de Sampaio Basto. São Paulo: DPL, 2008. 256p.

MATTOS, Carlos de Meira. Carlos de Meira. Estratégias militares dominantes: sugestões para uma estratégia militar brasileira. Rio de Janeiro: Biblioteca do Exército (Coleção General Benício, v. 239), 1986, 100 p.

_____. Geopolítica e modernidade: a geopolítica brasileira. Rio de Janeiro: Biblioteca do Exército (Coleção General Benício, v. 386), 2002, 160 p.

MINTZBERG, H.; AHLSTRAND, B.; LAMPEL, J. Safári de Estratégia. Porto Alegre: Bookman, 2000.

PORTER, Michael E. Competitive strategy: techniques for analyzing industries and competitors. Originally published: New York: Free Press, c 1980

_____.What is Strategy. Harvard Business Review. November-December – 1996, p.62-78.

_____. Strategy and the internet. Harvard Business Review. Mar. 2001, p. 63-78

SUGAI, Vera Lúcia. Arte da estratégia: obra que integra a Arte da Guerra e O livro dos cinco anéis. 2. Ed. – São Paulo: Sapienza, 2005. 138 p.

SUN TZU. Arte da guerra. Tradução de Armando Serra de Menezes. 2. Ed. – Biblioteca do Exército (Coleção General Benício, v. 400), 2003, 84 p.

TAVARES, Mauro Calixta. Gestão Estratégia. 2. Ed. – São Paulo: Atlas, 2005. 440 p.

TOFFLER, Alvin e TOFFLER Heidi. A riqueza revolucionária. Tradução Maiza Prande Bernadello, Luiz Fernando Martins Esteves. São Paulo: Futura, 2007, 591 p.

VASCONCELOS FILHO, Paulo de e PAGNOCELLI, Dernizo. Construindo estratégias para competir no século XXI. Rio de Janeiro: Campus, 2001. 370 p.

Isaac de Oliveira e Souza, MSc

Mestre em Gestão Estratégica de Segurança Pública, Especializado em Gestão Estratégica de Marketing, Gestão da Segurança Pública, Educação Física e graduado no Curso de Formação de Oficiais da Polícia Militar de Minas Gerais (PMMG). Coronel, com 30 anos de serviços prestados, foi Chefe de Gabinete do Comandante-Geral, Chefe da Terceira Seção do Estado-Maior e Subchefe do Estado-Maior da PMMG. Foi Diretor-Geral da Superintendência de Atendimento ao Menor Infrator e Diretor-Geral da Penitenciária José Maria Alkmim. Atuou como Professor de Chefia e Liderança; Educação Física; Trabalho de Comando, Defesa Social e Teoria Geral de Polícia em diversos cursos da PMMG. Foi Diretor de Projetos da TIS – Tecnologia e Inteligência em Planejamento da Segurança. É Consultor de Segurança, Professor de Pós-Graduação na Faculdade Pitágoras, Diretor da ABSEG em Minas Gerais e membro da Associação Brasileira dos Profissionais de Inteligência Competitiva – ABRAIC.

Técnicas de Negociações Complexas Aplicadas a Situações que Envolvam Reféns

José Luiz Cardoso Zamith

***Resumo:** Os conflitos cada vez mais têm mostrado que as soluções negociadas são mais efetivas e eficazes que as alternativas beligerantes. Partindo de um estudo sobre situações que envolvam reféns, torna-se relevante perceber que o aprimoramento da gestão destes casos é fator fundamental para expor cada vez menos a vida de todos os envolvidos. Destarte, a intenção de realizar uma discussão teórica a respeito de eventos dessa natureza é, ao final, chegar à conclusão da necessidade de inserção na doutrina, especificamente a brasileira, de novos mecanismos preliminares de avaliação de conflito e de mensuração do resultado para contribuir na preservação do Estado no processo, cujo saldo final sempre está ligado a um grande desgaste de todos os atores. Assim, analisando sob o ponto de vista das quatro etapas de criação de consenso de uma negociação empresarial, buscou-se realizar uma identificação dos pontos importantes e singulares no conceito utilizado pelas empresas, atentando para o que poderia ser transposto ou que acrescentasse, de forma significativa, o bom andamento das negociações envolvendo reféns. Sobressaltaram, na análise, os aspectos políticos e o relacionamento com a mídia como fatores capazes de alterar os rumos do processo e, consequentemente, pôr a vida dos reféns em perigo.*

1. Introdução

Os conflitos cada vez mais têm mostrado que as soluções negociadas são mais efetivas e eficazes que as alternativas beligerantes. Na conjuntura nacional e internacional que as crises se sucedem, já não se admite mais perdas sem responsabilização. E é neste contexto que foram escolhidos para serem tratados neste trabalho, os conflitos que tenham como pano de fundo, situações que culminem com a tomada de reféns.

Desde a morte de israelenses nas Olimpíadas de Munique em 1972 – evento que se tornou um marco para o desenvolvimento de doutrinas - até os dias atuais, é notória a dificuldade que os governos têm em resolver este tipo de situação. Mesmo assim, o progresso na forma de tratar estes assuntos e o aprimoramento de todos os fatores envolvidos no gerenciamento da crise fizeram com que diminuíssem em muito as perdas de vidas. Isto não quer dizer que episódios desta natureza não tenham um final como o da escola de Beslan1, ou, no caso brasileiro, como no ônibus 1742.

Portanto, fica evidenciado que a gestão destes casos necessita constantemente de aperfeiçoamento da técnica no desenvolvimento do processo de negociação. Isto significa, em linhas gerais, ter uma estrutura de gerenciamento de crise preparada e treinada com doutrina específica, meios adequados e, mais do que isto, estar em consonância com os anseios da sociedade:

"A necessidade de uma postura organizacional não-rotineira é, de todas as características essenciais, aquela que talvez cause maiores transtornos ao processo de gerenciamento. Contudo, é a única cujos efeitos podem ser minimizados, graças a um preparo e a um treinamento prévio da organização para o enfrentamento de eventos críticos." (MINISTÉRIO DA JUSTIÇA, 2001, p.7).

Destarte, discutir sobre o assunto torna-se relevante, em virtude dos impactos e das consequências geradas por estes tipos de acontecimento. A partir do momento que passaram a vir a público as políticas que delineiam a forma de conduzir estas situações, tornou-se possível haver críticas e, de uma maneira mais ampla, demonstrar as satisfações e insatisfações, e o que pode ser suportado ou não como efeito destes tipos de crise. Hoje, não se pode mais permitir que a participação da sociedade seja realizada apenas pelo acompanhamento do que é divulgado pela mídia. O pouco que se discute e se fala sobre as estratégias e conceitos em si, gera apenas um debate sobre as consequências, de forma bastante pontual (na existência de casos) e perene.

Este artigo tem por objetivo realizar uma análise das negociações envolvendo reféns, por meio de uma revisão bibliográfica e documental, à luz de aspectos doutrinários empregados pelo Departamento da Polícia Federal (DPF) e pelas polícias do Rio Grande do Sul e do Rio de Janeiro3, sob o ponto de vista das quatro etapas de criação de consenso de uma negociação empresarial (SUSSKIND, 2000): (a) Preparação para a negociação; (b) Criação de valor; (c) Distribuição de valor e (d) Execução da negociação propriamente dita. O propósito de realizar uma abordagem sob este enfoque está em auxiliar o processo

desenvolvido pelas autoridades brasileiras, no que tange a identificar melhor os riscos, os impasses e consequências e, com isso, sugerir elementos que possam ser inseridos na doutrina.

Salienta-se que este trabalho não se aterá a respeito dos aspectos legalísticos incluídos nestes tipos de ocorrência, isto é, só se analisarão as técnicas e a doutrina utilizadas pelos gerenciadores de crises. Não se levará em consideração possíveis restrições legais que puderem advir de determinadas abordagens sugeridas.

Neste artigo foi realizado um corte temporal abrangendo os últimos vinte anos, período este em que as instituições negociadoras brasileiras sofreram profundas alterações no seu preparo, principalmente após a ocorrência de eventos que tiveram grande repercussão e afetaram sobremaneira a imagem destas organizações. Pode-se citar como fatores originadores destas alterações, o caso Carandiru, em 22 de outubro de 19924 (como foi conhecido e intitulado pela imprensa), para as autoridades paulistas e o já citado Ônibus 174 para as autoridades cariocas.

2. Preparação da Negociação

O contexto de segurança pública é bastante interessante no que concerne aos procedimentos e técnicas adotadas: é um serviço fundamental que não pode ser passível de erro. Em São Paulo, por exemplo, que possui uma força policial de 130 mil policiais, o Secretário de Segurança, Saulo Filho, em entrevista à Revista Época, em maio de 2004, argumenta: "Se 1% errar, são 1.300 erros todos os dias. Se cada um deles matasse, haveria 1.300 mortes". Este alerta é um sinal que o problema do aprimoramento nos deveres policiais já é bem compreendido e, além disso, apresenta um sinal de mudança nas corporações, que já buscam conceitos empresariais de qualidade e aperfeiçoamento da gerência (EXAME, 2002), para superar os problemas e contingências do dia a dia da segurança. E estas contingências são muito maiores em situações de reféns.

As negociações que envolvem reféns são um tipo de negociação bastante sui generis, visto que dentre várias de suas características, abarcam sentimentos exacerbados, normalmente surpreendem a todos, possuem uma possibilidade de impacto de longa duração em toda sociedade e provocam uma altíssima pressão psicológica em todos os atores do contexto, principalmente em virtude do objeto finalístico ser a preservação de vidas. Assim, mais uma vez, revestem-se de grande importância a capacitação e a técnica para a condução deste tipo de atividade:

"As estatísticas têm demonstrado que a solução negociada, quando eficientemente conduzida, apresenta resultados muito superiores aos das soluções de força, que são quase sempre cruentas e com consequências traumatizantes para aqueles que se encontram na condição de reféns." (MINISTÉRIO DA JUSTIÇA, 2001, p.59).

A doutrina enfatiza que a fase pré-ocorrência do evento (planejamento específico) e a fase inicial da ocorrência (contenção e isolamento) são bastante singulares. Independente da particularidade da situação, ao mesmo tempo em que estas etapas se caracterizam como um espectro de incertezas (causadoras de uma dificuldade ímpar no planejamento), obrigam a estrutura do gerenciamento a estar pronta e preparada para os diversos tipos de contingências. Nessas fases então, a imprevisibilidade, a urgência e o curto período de tempo entre a tomada de consciência dos fatos e as ações advindas, fazem com que seja necessário haver procedimentos bem definidos, para evitar que se faça ou deixe de fazer algo que comprometa o processo como um todo. Vale ressaltar, que conforme análises do FBI e da própria DPF, os primeiros quarenta e cinco minutos de uma situação que envolvam reféns são os mais críticos do contexto.

Sendo assim, além de procedimentos (que são afetos ao aspecto operacional da resolução da crise), é necessário que haja um rigoroso preenchimento de regras por parte do Estado, a fim de criar uma linha bastante rígida na condução das negociações por parte da autoridade encarregada e, de modo conjunto, dar respaldo a uma situação tão crítica como as que envolvem reféns. Olhando no ambiente internacional, podem-se citar como exemplo de políticas públicas sólidas e rígidas, as posturas inflexíveis dos governos americano e israelense em relação aos sequestros terroristas que acontecem frequentemente no Oriente Médio (MNOKIN e HACKLEY, 2004). Certo ou não, todos sabem que não há negociações por parte das autoridades em eventos desta natureza.

Já no Brasil esta posição não é tão clara. Apesar da aplicação da lei nortear (ou deveria) a negociação, algumas brechas têm ocorrido, propiciando uma potencialização do desgaste em todos os envolvidos e, assim, acentuando ainda mais as consequências (em sua maioria, bastante danosas), principalmente pela discricionariedade de determinadas decisões que não poderiam ter esta possibilidade. Há de se considerar, como fator fundamental na fase da preparação, o aspecto e a dimensão política do problema. Hoje, a doutrina atém-se basicamente ao grau do risco e ao consequente nível de reposta por parte das instituições policiais5. Entretanto, é possível manter uma política que tenha como cerne o que já é preconizado: "A aplicação da lei pode esperar por alguns meses, até que sejam presos os perpetradores da crise, ao passo que as perdas de vidas são irreversíveis." (MINISTÉRIO DA JUSTIÇA, 2001, p.11).

Para exemplificar o problema, é possível citar a situação de negociação no Rio de Janeiro – um dos estados com os índices

mais altos de crimes contra a vida no Brasil, segundo dados estatísticos do sistema DATASUS, divulgados pela Assessoria de Planejamento, Orçamento e Modernização da Polícia Militar do Estado do Rio de Janeiro. Especificamente, na atuação em casos que envolvam reféns, o Batalhão de Operações Especiais da PM/RJ (BOPE), no período de 12/06/2000 até 25/09/2004, participou diretamente de 05 (cinco) ocorrências de assalto interrompido, 03 (três) incidentes domésticos e 09 (nove) rebeliões em estabelecimentos prisionais, totalizando 140 reféns salvos, e 02 reféns mortos, em decorrência da utilização da doutrina do gerenciamento de crise. Nos casos em que não houve sucesso, os motivos sugeridos para o fracasso foram decorrentes da falta de manutenção na utilização da doutrina, de ingerências políticas e da mídia que alteraram o contexto da situação (FONTENELLE, 2005).

Numa análise em que a delimitação dos interesses e das alternativas é extremamente importante nas consequências futuras, os exemplos citados têm mostrado que a política não pode ficar de fora da avaliação da ocorrência. Isto não quer dizer que as decisões da gestão da crise devam ser políticas, mas sim, que este fator seja avaliado e acompanhado desde o início do problema e que influencie na determinação do grau de risco6. Espera-se que as autoridades públicas definam as opções de negociação e delimitem a consequente ZOPA - Zone Of Possible Agreement (MNOOKIN, 2000) 7 a fim de estabelecer de forma clara e transparente até que ponto os negociadores poderão ir (obviamente que a colocação da vida dos reféns em risco já é uma restrição específica) e quais exigências poderão ser atendidas ou não - em que pese a possibilidade de realização do acordo e da entrega ou não dos reféns. Sabe-se, contudo, que o que se busca são linhas gerais e a própria legitimação da estrutura de gerenciamento para a tomada de decisão na crise, principalmente devido à diferenciação dos riscos para cada ocorrência (RAIFFA, 1982).

Outro elemento que deve ser levado em consideração, ainda na realização do diagnóstico, é a mídia e seu respectivo papel na veiculação da informação. Propõe-se uma melhor definição de como a imprensa deve ser tratada pela estrutura do gerenciamento da crise, desde a ocorrência do evento, e de como devem ser atendidos seus interesses (transmissão de dados para a opinião pública e outros afins). Hoje, as redes de informações dos meios de comunicação são interligadas e bastante rápidas, e não obstante, sabem das ocorrências e as divulgam muito antes que uma autoridade pública tenha sequer sido notificada do problema. Portanto, é inafastável a necessidade de relacionar-se com os meios transmissores de notícia para que alguns problemas, já no início, sejam minimizados ou se evite o acréscimo de dificuldades a serem gerenciadas. Alguns motivos justificam tal posição:

a. Os momentos iniciais da crise são os mais críticos e a possibilidade de acesso à informação é muito fácil. Portanto, os tomadores de reféns têm uma capacidade muito grande de ter conhecimento de informações deturpadas que podem afetar ainda mais a instabilidade da situação;

b. A opinião pública, ao receber dados dos momentos iniciais, de forma bastante incipiente e desencontrada, pode interferir e gerar uma pressão muito grande na estrutura do gerenciamento da crise, alterando o próprio risco e o nível de resposta das autoridades. Consequentemente, aumentando ainda mais o risco político na condução das negociações.

O isolamento da imprensa é muito perigoso e pode afetar um ambiente que por si só já é instável e propício a ser abalado. Sendo assim, independente da forma sensacionalista como alguns organismos de divulgação queiram lidar com o caso, é importante o diálogo e a passagem das informações para que sejam retransmitidas ao público. O estabelecimento da confiança não pode ser buscado apenas junto aos tomadores de reféns. Quanto mais repórteres e jornalistas confiarem no que lhes é passado, menos problemas a serem gerenciados (SUSSKIND, P. 177, 1987).

3. A criação de valor na Negociação

O interesse de toda e qualquer situação na ocorrência de reféns é a vida. Com isso, nesta fase, estabelecer uma BATNA (Best Alternative to Negotiation Agreement), para este tipo de situação é inverossímil, visto que não há outra alternativa a ser conseguida do que a entrega dos reféns sãos e salvos8 (FISHER e URY, 1999). Contudo, ao se pensar nas possibilidades dos tomadores de reféns, há de se considerar realmente se as exigências ou alternativas poderão ou deverão ser aceitas, para que com isto se alcance o objetivo final. Mnookin e Hackley (2004) fazem uma crítica à postura americana de não negociar, em virtude das perdas que o povo americano vem sofrendo em relação a essas situações de crise:

"Falar com terroristas é diferente de ceder alguma coisa. Algumas vezes, uma boa prática de conhecer o que pensam ou fazer a linha de um bom ouvinte é importante para mantê-los perto como "amigos", do que longe como "inimigos". O FBI e os negociadores de reféns da polícia sempre, em suas negociações, precisam angariar informações, observar coisas por meio de suas percepções e ganhar vantagens psicológicas.".

Dentre as regras de engajamento que preconizam a conformidade9, a ética e a legalidade das ações como preceitos inquestionáveis em todo o processo de negociação, é lícito supor que a manutenção do uso da técnica durante todo o acontecimento

é a única via capaz de garantir que se tenha chance de libertar os reféns vivos, e com isso, mostrar que é possível criar valor dentro do processo. Desta feita, o acordo e a inserção destas garantias, de forma pública, fortalecem ainda mais o Estado em suas convicções e transmitem ao ofensor a conduta, a oportunidade e a certeza do que poderá alcançar em suas exigências. Ao mesmo tempo, tornam impessoais quaisquer medidas que sejam tomadas por parte dos negociadores e de todo o comitê de crise que possam ser julgadas como impopulares ou que, mesmo duras, evitem um mal maior.

Em consequência, o processo de criação de valor, ao longo de uma penosa duração, terá um fator importantíssimo e necessário para os desígnios da negociação: tranquilidade para os negociadores e para o próprio comitê de crise que, limitado dentro das políticas e linhas mestras definidas, amparar-se-á incondicionalmente nas estratégias operacionais de forma a conseguir o intento da libertação dos reféns (PRUITT, 2001). Quando isto não acontece, que garantias e que tipo de responsabilização poderão ser solicitadas às autoridades encarregadas quanto a possíveis danos ou insucessos obtidos? Em caso recente, no Rio de Janeiro, o grupo de negociadores do Batalhão de Operações Especiais da Polícia Militar do Rio de Janeiro (BOPE), em uma rebelião em presídio, foi substituído por um pastor evangélico10. Dessa forma, é impossível gerar uma conformidade que torne viável garantir um embasamento forte e racional (estrutura, legalidade, questões morais, culturais e éticas) à gestão da crise, gerando direta ou indiretamente um padrão que transmita confiança à sociedade e dissuasão naqueles que tentam realizar um intento com reféns.

Como na negociação empresarial, criar valor também é crucial para o sucesso da negociação. Se por um lado, os negociadores valoram a vida dos reféns, por outro, há uma busca constante em desestimular ao máximo os tomadores de reféns da situação existente, dissuadindo e minimizando as exigências e condições, para que seja possível a chegada de um acordo. É uma tarefa árdua de convencimento e persuasão para manter todos os atores na razão.

4. Distribuição de Valor na Negociação

As negociações com reféns são extremamente sensíveis no que concerne ao processo de tomada de decisão. Todos os passos dados nas fases que envolvem a crise têm a peculiaridade de pôr a vida de todos os atores em risco11.

Em virtude disto, desde o princípio do problema, torna-se fundamental a estabilização das tensões, a fim de se obter o início do processo – ultrapassar os momentos críticos e iniciar o processo calcado numa estratégia já pode ser considerado uma vitória parcial (DIXIT e NALEBUFF, 1991). Vale a pena frisar, que nem sempre a ocorrência de reféns pode gerar a negociação propriamente dita (esta deve ser encarada como uma conquista), principalmente devido a circunstâncias cujo grau de imprevisibilidade seja muito alto, não proporcionando uma oportunidade de aproximação dos negociadores. Situações desse gênero podem ser exemplificadas em casos do tipo assalto interrompido (situações de assalto, em que a polícia chega antes da fuga dos bandidos e estes fazem reféns para garantir sua segurança) e outras, cujos tomadores de reféns tenham distúrbios comportamentais ou sofram de algum tipo de doença psíquica.

Mesmo assim, num contexto de decisões imediatas revestidas de poucos subsídios e envoltas em extrema pressão, é fator preponderante o levantamento de elementos que possam minorar as obscuridades e melhor situar os negociadores com o problema, além de delinear e mapear todos os envolvidos. Independente de qualquer doutrina que seja adotada, os negociadores invariavelmente precisam rapidamente conseguir filtrar os interesses, opções e posições que poderão ser assumidas no decorrer da ação e que possam ser barganhadas, no intuito de distribuir valores e conseguir o intento maior. Esta não é uma tarefa fácil e, com o passar do tempo, dependerá de fatores como o próprio diálogo com os tomadores de reféns e a busca constante de dados em campo, para que favoreçam no resultado esperado. É possível que esta empreitada possa se valer de diversos tipos de agentes ou fontes que tenham algo a acrescentar. Entretanto, dois problemas poderão vir a ocorrer, se isto não for coordenado com toda a equipe:

a. A possibilidade de envolver pessoas que possam entrar em contato com os tomadores de reféns é muito grande. Hoje, os meios de comunicação permitem que haja um perfeito diálogo em todos os pontos do planeta, o que pode gerar uma desestabilização da crise ou a inserção de outro ator que, invariavelmente, vai prejudicar as negociações;

b. A valorização de uma ou outra informação pode gerar erros precoces de avaliação. O ambiente de confinamento normalmente é muito incerto. Não se sabe quantos são, quem são e o que está por trás do fato. Avaliações errôneas também podem desestabilizar o contexto ou encaminhar a negociação para um lado que não seja de interesse dos negociadores.

Desta feita, a arte de conduzir estas situações dependerá em muito do pragmatismo dos negociadores. Experiências, linhas de conduta pré-estabelecidas e outras técnicas específicas são garantias de que a negociação pode levar ao objetivo maior, que é a libertação de reféns12 (RAIFFA, 1982). A existência de uma estrutura sólida, consistente e focada na atividade fim, pode vir a trazer benefícios, que por si só, serão alcançados pela sistemática reafirmação dos compromissos dos atores envolvidos e facilitar o processo decisório, apesar dos problemas já levantados:

• O Estado, ao manter uma estrutura específica para tratar destes assuntos e ter pessoas experientes e com bastante

tempo de serviço na condução, mostra a todos a sua política e, passa indiretamente, o que se pode esperar em casos desta magnitude;

• A sociedade sabe quem são os responsáveis e se é possível confiar nestes para a preservação da vida dos reféns;

• O Comitê de crise tem seu papel bem definido e, por meio de uma missão, estrutura, processo de recrutamento, estratégias e experiência, possui todo o know-how para conduzir uma negociação;

• Os tomadores de reféns, ao realizarem o crime, sabem com quem vão lidar e o que poderão conseguir em termos de exigências, além do tratamento que lhes será despensado.

Vê-se, portanto, que o processo de tomada de decisão fica progressivamente facilitado à medida que aspectos como estruturação, relacionamentos, comunicação e compromisso sejam mapeados e definidos, tanto internamente quanto externamente, já desde antes da ocorrência de uma crise (COMBALBERT, 2004).

5. Execução da Negociação - o engajamento

No complexo emaranhado de aspectos críticos e atores envolvidos, o fator tempo é uma das poucas certezas existentes. Enquanto os negociadores buscam dilatá-lo ao máximo, os tomadores de reféns querem ter suas exigências atendidas o mais rápido possível. Diferentemente das negociações empresariais, a premência dos acordos é definida pelo risco de perda da vida de um refém, que pode vir a alterar a conduta para a resolução do conflito. A duração de um episódio desta natureza está, em sua maioria, condicionada à necessidade de aumento de informações, a estratégias operacionais e à própria conduta dos tomadores de reféns.

As escolas doutrinárias no mundo têm bastante diferenciação quanto à forma de conduzir o processo relacionado ao tempo. Existem escolas que buscam o diálogo ao máximo, podendo admitir a ocorrência de danos a algum(ns) do(s) refém(ns) – a preocupação maior é com o todo – outras já determinam um prazo limitado para a abordagem tática13. Contudo, apesar das diferenças, todas consideram que a segurança do refém está condicionada muito mais ao estabelecimento de uma relação negociador-tomador de refém (relação de confiança e diálogo) e tomador de refém-refém (síndrome de Estocolmo14), do que a urgência de resolução do conflito (MINISTÉRIO DA JUSTIÇA, 2001). Em dezembro de 2004, pôde-se observar num sequestro de ônibus na Grécia, realizado por dois albaneses, que, apesar do prazo fatal dado por estes e pela tensão existente, o transcorrer das horas foi fundamental para que houvesse um desfecho favorável, sem nenhum dano aos passageiros.

Uma das dificuldades encontradas pelos comitês de crise, e que tem uma influência no tempo é perceber quais são as reais intenções quando se encontram dialogando com os tomadores de reféns. Muitas vezes, o rol de exigências feitas por estes é muito mais um despistamento ou uma maneira de expor o Estado (principalmente em rebeliões em estabelecimentos prisionais), do que uma demonstração clara dos reais interesses. Enquanto isto, apesar da busca constante da estabilidade do conflito, à medida em que o tempo passa, os riscos sofrem constantes alternâncias, maximizando ou minimizando a possibilidade de diversos tipos de perdas. Desse modo, conclui-se que é impositivo uma gestão que se atenha ao todo, contrariando a tendência de se preocupar exclusivamente com o diálogo.

Para conseguir cumprir estes requisitos da gestão faz-se necessário um acompanhamento permanente, tanto do ambiente interno (o conflito), quanto do externo (a observância do comportamento de todos os atores envolvidos direta ou indiretamente no processo), a fim de propiciar uma mensuração permanente dos riscos e possibilitar que o gestor da crise consiga gerenciá-los e tratá-los de acordo com a importância e a premência de cada um deles. Em contrapartida, a inobservância ou esquecimento disto conduzirá a desestabilização da relação criada entre negociador-tomador de refém. A coordenação não é fácil e necessita de uma equipe que tenha papéis definidos e, consiga, inexoravelmente, estar comprometida com o todo.

Portanto, é possível e muito comum, a ocorrência de impasses que coloquem de um lado a técnica e do outro, os interesses pessoais (SUSSKIND, 1999). Como já dito no início do artigo, a existência de elementos políticos e a importância que a mídia possa vir a dar ao caso são fundamentais no gerenciamento destes riscos. O tratamento que deve ser dado à imprensa e sua consequente delimitação no contexto devem ser monitorados em todas as fases. Na preparação, levantou-se a influência desta sobre o grau do risco do conflito e como tratar a informação com os órgãos de difusão. Agora, já durante a negociação, o relacionamento não pode se limitar apenas no que a doutrina preconiza como uma maneira de informar o que é estritamente necessário para evitar que haja interferência no processo. Há um papel educativo e há também a preocupação em como esta informação poderá se tornar formadora de opinião junto à sociedade. É importante salientar que não se está querendo com isso sobrevalorizar aspectos que pareçam mais importantes que o objetivo de salvar vidas. O que se quer é ressaltar a existência de diversos outros fatores envolvidos que, se não observados, farão com que a situação se torne tão instável que, indiretamente, possa vir a colocar a vida dos atores à prova.

Por si só, a negociação já exigirá muito daqueles que estiverem diretamente obrigados a ter a responsabilidade das vidas

de outrem nas mãos. Dessa feita, tudo que possa vir a criar problemas e tornar o ambiente mais incerto do que já é deve ser gerenciado (RAIFFA, 1995). Vários foram os casos brasileiros em que, com o decorrer da situação, os negociadores foram trocados por autoridades que não eram preparadas para a tarefa, mas que pela dimensão que o caso tomou, se viram obrigadas a assumir o papel, por falta de uma política definida e pela própria descrença na capacidade da equipe em resolver o problema. Já foi afirmado, e é bom que se frise novamente, que o decorrer do tempo é um bom resultado e não uma sequência de derrotas do comitê de crise junto aos tomadores de reféns. O importante é saber administrar este transcurso das horas para que, à medida que as exigências sejam abrandadas, o convencimento dos negociadores sobrepuja os interesses dos tomadores de reféns e, assim, consiga o objetivo da soltura de todos. A sociedade precisa saber e cooperar com isso.

O negociador terá, ao longo do processo, que conviver com diversos dilemas e tensões durante o caso (LAX e SEBENIUS, 1986). Não há como fazer com que todos saiam ganhando no acordo. Muito pelo contrário, todos perdem. Apesar de, se bem sucedida, a crise conseguir a libertação dos reféns e a aplicação da lei sem que haja qualquer vítima, ao final, todos saem com algum tipo de sequela:

- Os reféns necessitarão de um bom tempo para superar o acontecido;
- O comitê de crise, invariavelmente, sairá desgastado, apesar de ter alcançado seu objetivo, e
- O Estado, por permanecer sempre exposto, mesmo com desfechos favoráveis, será questionado.

6. Considerações Finais

Não se pretendeu com este artigo simplificar o gerenciamento de crise envolvendo reféns por meio de uma conjuntura de elementos e indicadores que, inserida na doutrina existente, tornasse capaz de alcançar os objetivos para quaisquer que sejam os casos, de forma simples e infalível. Muito pelo contrário. Num ambiente tão envolto em incertezas e que, desde o seu início, já apresenta consequências tão graves, buscou-se ao máximo, por meio de um enfoque diferente, utilizando conceitos já firmados para negociações complexas, agregar valor e levantar fatores que precisam ser observados em eventos dessa natureza.

Portanto, na fase de preparação, sugerem-se dois fatores para que sejam avaliados e analisados para o estabelecimento do contexto:

• O risco político – Deve-se quantificá-lo e utilizá-lo na qualificação do grau de risco e na resposta a ser dada. Apesar de uma preocupação operacional para a resolução do problema, o gerente da crise deverá considerar os aspectos políticos e, já nos momentos iniciais, buscar respaldo junto às autoridades superiores, para que este risco possa ser gerenciado;

• O estabelecimento do contato inicial com a mídia. Tratar a mídia como peça fundamental, não apenas delimitando o que deve saber ou não, é preponderante para o estabelecimento do silêncio e tranquilidade na criação de valor. A integração gerada, com regras pré-definidas possibilita o compartilhamento de pontos de vista de forma aberta, apesar da confidencialidade da negociação em si.

Ao final, apesar de ter sido afirmado que as consequências geradas levam todos os atores a algum tipo de perda, é possível que esta perda possa ser avaliada e mensurada, no intuito de subsidiar futuras negociações e de aprimorar a própria doutrina:

a. Preservação da vida – Se não se conseguiu preservar a vida de todos, consequentemente, a negociação não foi bem sucedida. Não se pode esquecer que a vida dos tomadores de reféns também deve fazer parte dessa avaliação. É obrigação do Estado fazer com que a aplicação da lei seja realizada, e isso, para ocorrer, dependerá do aprisionamento destes;

b. Imagem – Este fator deve considerar em que grau o Estado conseguiu sair fortalecido com a resolução do conflito. Isto é importante, à medida que cria exemplos para outros que queiram realizar um mesmo tipo de intento e, conjuntamente, demonstra a capacidade de amparo junto aos seus cidadãos;

c. Saldo político – O resultado para as autoridades públicas, em maior ou menor proporção, trará consequências na forma de governar e no relacionamento com o legislativo. Num caso de negociação de reféns, todos ficam muito expostos e as consequências são maximizadas na ocorrência de insucessos;

d. Impacto na opinião pública – A quantificação irá fortalecer ou enfraquecer o relacionamento da opinião pública com o governo, gerando fortalecimento na estrutura de governo;

e. Consequências no ambiente (dia-a-dia do presídio, tensões, crime) – O exemplo da eficiência e regras utilizadas na negociação tornam-se referências como forma de agir do Estado e nos resultados impostos aos tomadores de reféns.

Apesar de delinear e delimitar o processo em etapas, invariavelmente é necessário que a decisão fundamental seja seguir uma doutrina que tenha um compromisso com as vidas (reféns e tomadores de reféns). Isto quer dizer que, mesmo na aplicação das leis, é necessário que se demonstre preocupação e se transmita para a sociedade que a conduta postar-se-á de forma singular: preservar a vida de todos. Como efeito indireto, o Estado brasileiro se fortalece e torna-se um ente permanentemen-

te capacitado em defender os direitos dos cidadãos em situações em que estes se tornem vítimas e precisem de racionalidade e preparo para a solução do conflito.

Notas de final de texto

1. No dia 3 de setembro de 2004, um mal sucedido gerenciamento de crise numa escola em Beslan, na República de Ossétia do Norte, na Rússia, acarretou na morte de reféns, incluindo crianças.

2. No dia 12 de junho de 2000, um ônibus foi tomado no bairro do Jardim Botânico, no Rio de Janeiro, por um assaltante drogado que fez os passageiros como reféns. Erros no gerenciamento da crise acarretaram na morte de uma jovem que era feita refém.

3. As autoridades brasileiras que realizam negociações extremas utilizam a doutrina americana preconizada pelo FBI (Federal Bureau Investigation).

4. No intuito de debelar uma rebelião na Casa de Detenção em SP, a Polícia Militar invadiu o presídio ocasionando a morte de mais de 100 presos.

5. Classificação da crise que leva em conta fatores como ameaça, quantidade de reféns e ambiente da ocorrência para determinar o tipo de reação por parte da autoridade pública.

6. Como exemplo, o ocorrido com o empresário de televisão Silvio Santos, em agosto de 2001, que foi feito refém em sua própria casa, num evento de duração em torno de 7 horas e transmissão ao vivo em várias cadeias de TV do mundo todo, teve a negociação conduzida diretamente pelo Governador do Estado de São Paulo, que independente do resultado obtido, isto é, sem uma avaliação técnica do gerenciamento, alterou sensivelmente o grau de risco da crise, acarretando numa disponibilização de meios e em uma infra-estrutura bem acima do que seria preconizado pela doutrina.

7. A ZOPA define uma faixa de acordo possível, dividida entre as partes envolvidas.

8. Aqui, apesar da alternativa existente de uma ação tática como sendo uma opção na negociação, não se pretende garanti-la como uma alternativa, visto que isto não reflete a preservação da vida dos reféns e, como consequência, não se configura em um interesse por parte da sociedade. Considerar-se-á isto como uma possibilidade exclusivamente operacional.

9. Entenda-se conformidade como atitudes tomadas durante a negociação que não firam os valores morais e de bons costumes.

10. No dia 31/05/2004 (3º dia de negociações), na Casa de Custódia de Benfica, o Secretário de Segurança do Estado alterou o responsável pelas negociações, enquanto estavam sendo mantidos 23 reféns em posse dos presos.

11. Quando se aborda a vitimação dos envolvidos, há também uma preocupação com a vida dos tomadores de reféns. A autoridade pública não pode se ater apenas a um dos lados da crise, deve pensar no todo.

12. Como exemplo, pode-se citar um órgão específico da França chamado Le RAID – Recherche Assistance Intervention Dissuasion, que dentro de sua estrutura, em sua terceira seção, se compõe de policiais antigos e experientes para atuarem como negociadores em situações desta natureza. Realizando uma análise bastante superficial verifica-se que a utilização de profissionais com este perfil tem a finalidade de, cada vez mais, definir o comitê de crise e, ao utilizar pessoas experimentadas, tentar minimizar as incertezas por meio de experiências ou casos parecidos já presenciados.

13. As negociações envolvendo reféns têm como estratégias duas tendências características: buscar o acordo e, ao mesmo tempo, viabilizar uma ação tática, isto é, a utilização de grupos especiais para retomada e resgate dos reféns.

14. As doutrinas acreditam que o estabelecimento da Síndrome de Estocolmo é uma ocorrência benéfica, pois cria uma relação de confiança e cumplicidade em ambos os lados e se torna uma garantia de segurança para os reféns.

Referências Bibliográficas

AXELROD P. The evolution of Cooperation. Nova York. Basic Books, 1984.

COMBALBERT, Laurent. La négociation de crise au service de l'enterprise. Revue Française de Gestión. Paris, vol. 30, nº 153, p. 281-295, novembro/dezembro, 2004.

DA SILVA, J. Segurança pública e polícia: criminologia crítica aplicada. Rio de Janeiro: Forense, 2003.

DIXIT A.; NALEBUFF, Larry. Thinking strategically: the Competitive edge in business, politics and every day life. Harvard University Press. 1991.

FERNANDES, Nelito; MARTINS, Elisa; LIBÓRIO, Roger. Mortos pelos homens da lei. Revista Época, São Paulo,nº 311, p. 94-102, de 3 de maio de 2004.

FISHER Roger; URY, William; PATTON, Bruce. Chegar ao Sim. Harvard Program on Negotiation. Rocco: 1999.

FONTENELLE, Alexandre. O gerenciamento de crise – preservar vidas no estado do Rio de Janeiro, Monografia apresentada ao Curso de Especialização em Políticas Públicas de Justiça Criminal e Segurança Pública. UFF, 2005.

KAHNEMAN D; TRESKY, A. Conflict Resolution: A cognitive perspective. In: K. Arrow et al. (eds). Barriers to Conflict resolution,

2004.

LAX Robert; SEBENIUS, James. The manager as negotiator, bargaining for cooperation and competitive gain. Free Press. 1986.

LEMPEREUR, A. P et COLSON A. Méthode de négociation. Paris, Dunod, 2004.

MINISTÉRIO DA JUSTIÇA. Programa de treinamento de especialistas e instrutores policiais - curso de controle e resolução de conflitos e situações de crise, módulo básico. Plano Nacional de Segurança Pública. Brasília: junho de 2001.

MNOOKIN, Robert; SUSSKIND Lawrence (eds.) Negotiating on behalf of others: Advice to lawyers, business executives, sports agents, diplomats, politicians and everyone else. Thousands Oaks, CA: Sage Publications, 1999.

MNOOKIN, Robert. Beyond winning: Negotiation to create value in deals and disputes. . Harvard University Press, 2000.

MNOOKIN, Robert; HACKLEY. Susan. Disconnecting 'Quid' From 'Quo'. Los Angeles Times. Los Angeles, 26 set. 2004

OGAWA, Alfredo. (In)segurança pública. Revista Exame, São Paulo, p. 14-15, de 28 de junho de 2002.

PATTON, Bruce. How to manage difficult conversations. Harvard Negotiation Project. Penguin Books, 1992.

PRUITT, D. Escalation, Readiness and third party functions: In: FAVRE, G. O.; ZARTMAN, I.W. IASA, Luxemburg, Austria, 2001.

RAIFFA, Howard. The art and science of negotiation. Harvard University Press. 1995.

ROSS, L.; MNOOKIN, Robert. Barriers to conflict resolution. In: K. Arrow et al. (eds). Barriers to Conflict resolution, 2004.

SCHELLING, T. C. Arms and Influence. New Haven, Yale University Press: 1966.

SUSSKIND Lawrence. Breaking the impasse: Consensual approaches to resolving public disputes. Basic Books, 1987.

_____ . Dealing with an angry public. Harvard-MIT Public Dispute Program. Free Press. 1999.

_____. The Consensus Building Resolutions. Sage Publications. 2000.

WATZALAWICK P. How real is real? Communication, disinformation, confusion. Nova York. Random House: 1976.

José Luís Cardoso Zamith, MSc., CPP

Corporate Security Manager da Nokia Siemens Networks para o Mercosul, Capitão de Corveta Fuzileiro Naval da Reserva da Marinha, carreira desenvolvida em assessoramento na área de segurança, prevenção de perdas e gerenciamento de crises para organismos internacionais (PNUD e HABITAT) para o Governo Federal (Ministério da Justiça, nos Jogos Pan-Americanos do Rio de Janeiro) e empresas transacionais (Petrobras, Vale do Rio Doce, CSN, entre outras), além de VIPs e familiares. Mestre em Administração pela FGV, MBA em Segurança Corporativa pela FGV e CPP (Certified Professional Protection) pela ASIS International. Participante de redes de segurança privada internacionais e nacionais (ASIS, ABSEG, OSAC). Professor de diversos cursos nacionais e internacionais e pesquisador da FGV dos Núcleos de Negociações Complexas e Justiça e Segurança.

O Mercado de Segurança Eletrônica nas Empresas Brasileiras

Mauro De Lucca

O mercado vem evoluindo, e com isso, pouco a pouco, as empresas começam a profissionalizar sua área de segurança, o que reflete na melhoria dos processos de aquisição e na aplicação de equipamentos eletrônicos. Infelizmente, essa evolução ainda é bastante restrita e caminha devagar. Por exemplo, muitas empresas de porte ainda não entenderam os benefícios de ter um setor, departamento ou divisão composta por pessoal especializado em segurança, e delegam essa função, que deveria contemplar atividades como gestão de riscos, recuperação e administração de emergências e continuidade operacional para setores como Recursos Humanos, Administração ou Manutenção. Como uma das consequências, a seleção e as implementações de produtos e soluções eletrônicas acabam muitas vezes não sendo as ideais.

O resultado é que, quantitativamente falando, os equipamentos mais aplicados não são aqueles que proporcionam o grau mais adequado de proteção e de gestão para cada tipo de instalação. O critério "preço" acaba muitas vezes prevalecendo, em detrimento da qualidade e da aplicabilidade, o que resulta, muitas vezes, em investimento mal planejado, projeto mal elaborado, ou outros eufemismos para dinheiro jogado fora. Muitos dos sistemas de CFTV não proporcionam condições de monitoramento e recuperação de imagens de qualidade, vários sistemas de detecção de intrusão não fazem mais do que gerar uma quantidade insuportável de alarmes falsos ou gerados por ruídos, e inúmeros sistemas de controle de acesso são compostos por relógios de ponto.

Para muitos, parece lógico que cada projeto de segurança se baseie nas vulnerabilidades de uma planta e que haja equipamentos básicos, indicados para todos os tipos de gestão. Mas, em muitos casos, não é o que acontece. De qualquer modo, equipamentos básicos que se podem relacionar são câmeras, gravadores, sensores, controladoras, software de gerenciamento e computadores. Uma das formas de definir a importância desses dispositivos é classificá-los por finalidade. Por exemplo, sensores, câmeras e leitores realizam a tarefa de capturar informações no campo; controladoras, a de processamento da parte mais crítica dessas informações; softwares e computadores executam a parte de monitoramento e gestão.

Muitas vezes nos pedem para definir os equipamentos mais indicados e, consequentemente, mais utilizados pelas empresas, bem como quais as evoluções tecnológicas pelas quais passaram ao longo dos últimos anos.

Vamos nos ater aos mais indicados: as principais evoluções têm acompanhado a evolução da eletrônica e da tecnologia da informação. Os equipamentos vêm ganhando componentes mais modernos, processadores mais rápidos e processos mais precisos de fabricação e de controle de qualidade. Os sistemas de gerenciamento, por sua vez, têm aproveitado as condições de confiabilidade, estabilidade e capacidade de integração proporcionadas pelas inovações constantes das ferramentas de software, de comunicação e conectividade.

Mas eu insisto que sua eficácia depende de um projeto adequado. Não basta usar tecnologia de ponta. Para citar um exemplo bem prosaico, mas que ilustra bem o problema, a grande maioria dos locais onde há um equipamento de identificação biométrica controlando o acesso a uma porta não possui nenhuma detecção de intrusão. Uma empresa decide investir em tecnologia de ponta para a segurança, por exemplo, de uma sala de servidores; adquire um controle de acesso por biometria e por falta de projeto ou de conhecimento mínimo de quem vende o equipamento, não protege a mesma porta contra arrombamento, a janela, o forro ou piso contra intrusão. Investe, digamos, R$ 5.000,00 num equipamento para controlar as pessoas que vão proceder corretamente para requisitar um acesso, enquanto que as mal intencionadas podem facilmente ingressar naquele ambiente sem serem detectadas, por conta, por exemplo, da falta de um sensor que custa R$ 30,00. Falsa sensação de segurança que traz riscos maximizados, resultado totalmente contrário ao pretendido.

Outra pergunta frequente é em que se deve basear um projeto de segurança, no que se refere a equipamentos. Temos que ter em conta que, primordialmente (pois sempre há vários fatores), na capacidade de proporcionar o melhor gerenciamento possível dos riscos, minimizando-os, e levando em conta as particularidades de cada instalação, como o tipo de construção, localização, tipo de ocupação e atividade, histórico de problemas, riscos inerentes, ameaças, etc. Apenas após ter todos esses dados em mãos é que se deve verificar quais são os equipamentos que podem ser aplicados e avaliar suas condições de tecnologia, durabilidade, os serviços providos por seus instaladores, as referências que carrega e, é claro, seus preços. Não é por que um equipamento ou sistema custa caro, que pode ser considerado o melhor, até por que, realizada a análise dos riscos e

a avaliação dos produtos aplicáveis, pode-se chegar à conclusão de que não vale a pena investir R$ 100 mil para proteger um ativo cujo valor (valor não apenas em termos de preço, mas de importância operacional ou estratégica), é de R$ 80 mil. O que é fundamental é que um projeto deve tomar os equipamentos como uma consequência, e não como a razão. Para citar um exemplo simples, um projeto de controle de acesso não deve começar pelas catracas, mas sim chegar a elas depois de se concluir que as mesmas são dispositivos necessários.

A tecnologia, no entanto, anda cada vez mais depressa, e com isso vemos comumente equipamentos em utilização que já estão ultrapassados, e perdem a razão de serem utilizados, pois já não atuam de forma eficaz. Um usuário, muitas vezes, fica perdido, mas também as empresas provedoras se vêm com inúmeras dúvidas. Um dos grandes desafios dos desenvolvedores de equipamentos e de sistemas é chegar a produtos com baixo nível de obsolescência e que tenham capacidade de agregar atualizações. Os produtos que, por conta de suas limitações técnicas, impedem o usuário de agregar novas funcionalidades que lhe são importantes na gestão de segurança, devem ser substituídos. Não há regra ou fórmula pronta, mas a partir do momento em que se desenvolve um novo projeto ou se avalia um sistema existente, e desde que esse trabalho seja realizado por pessoal especializado, fica claro o que deve ser evitado ou trocado.

São muitos os equipamentos mais novos, que ainda não possuem uma grande escala de uso no Brasil, mas que têm uma tendência de franco crescimento. Para relacioná-los, a lista poderia ser extensa, mas podemos destacar os sistemas que oferecem uma maior capacidade de processamento distribuído, mas com melhores condições de gerenciamento e monitoramento centralizado ou distribuído, de acordo com cada situação. Nisso se inclui, com destaque, o aproveitamento de aplicações Full Web e das infraestruturas de redes, especialmente baseadas no protocolo TCP/IP. Além de proporcionar maiores possibilidades de processamento e gerenciamento, muitas vezes essas inovações trazem também vantagens econômicas, não só por conta da execução mais eficiente de suas tarefas, mas também por aproveitar estruturas existentes. Com relação à aplicabilidade, essa sempre é uma questão de avaliações caso a caso.

O grande dilema de um contratante é ter confiança de que os equipamentos que lhe foram indicados são realmente essenciais. Isso, por que segurança é aquele tema do qual "todo mundo entende", mas os resultados dessa pseudo autossuficiência são certamente os mesmos que eu teria como técnico da seleção brasileira: ruins. Se a empresa procurou uma consultoria foi por que provavelmente entendeu não ter recursos próprios para elaborar o melhor projeto e, consequentemente, definir a melhor especificação para equipamentos e sistemas. O problema é que, justamente por conta da especificidade da matéria, apesar de contarmos com excelentes profissionais de consultoria, por vezes esses serviços são prestados por pessoas que não possuem a formação adequada. O jeito é tomar cuidados básicos como verificar as referências fornecidas, a formação do profissional ou dos profissionais, a estrutura de sua empresa, a transparência com que as informações são passadas e se estas evitam linguagem excessivamente técnica ou rebuscada, além de supervisionar a forma como o consultor realiza o levantamento das informações de campo.

Além disso, é importante contratar uma consultoria não apenas para fazer o projeto, mas para participar do processo de seleção de fornecedor, realizando a equalização entre preços e parte técnica, e permanecer durante a implantação e fiscalização da obra mantendo seu acompanhamento e responsabilidade sobre a solução, pelo menos até que a mesma esteja implementada e operando a contento. É fazer com que a consultoria seja parte, não só da concepção, mas também da geração, do desenvolvimento e da maturidade daquele projeto. Como um filho.

Há ainda, claro, o papel fundamental do gestor de segurança nesse processo. O gestor de segurança deve estar atualizado com relação a produtos e serviços prestados pelos provedores, inclusive pós venda. Deve possuir uma boa cadeia de relacionamentos e lançar mão de grupos de discussões e associações como a ABSEG e a ASIS, acompanhando também a mídia especializada, e ainda participando de feiras do setor. Tudo isso, para que possa desempenhar corretamente o seu papel de elemento de grande influência ou, preferencialmente, de decisão na seleção de um equipamento ou sistema. Deve ter capacidade de relacionamento, especialmente com as áreas mais diretamente afetadas num processo de aquisição, como TI, RH e Suprimentos, além de habilidade para levar à Alta Administração as informações, no conteúdo e na forma, necessárias para que esta o apóie em suas escolhas.

Por fim, um ponto que sempre desperta curiosidade é saber se os projetos de segurança realizados para empresas brasileiras são muito diferentes, no que se refere à segurança eletrônica, daqueles feitos em outros países.

Existe na segurança, como nas demais áreas de conhecimento, uma diversidade cultural muito grande. O fato é que o grau de penetração da "cultura de segurança" é o que acaba por determinar essas diferenças. Certos fatos podem parecer estranhos como, por exemplo, o investimento médio em segurança física nas empresas suíças serem maiores do que o que é realizado no Brasil; afinal somos um país com vários problemas e a Suíça um lugar muito mais seguro. Todavia, por lá a segurança é vista como um investimento e por aqui, via de regra, como um gasto. Os investimentos estrangeiros no Brasil e a adoção de "culturas matriciais" por empresas multinacionais têm contribuído para diminuir essa distância, mas a preponderância de uma cultura que vê segurança como custo, compele as empresas a procurar o "mais barato", e esse mais barato dificilmente seria

o recomendado em um projeto bem elaborado.

Mauro de Lucca, PSP

Primeiro brasileiro a receber a certificação Physical Security Professional da ASIS International, trabalha no segmento de segurança física, especialmente eletrônica e integração de sistemas, desde 1993, em empresas como Graber e Telemática, tendo em seu currículo projetos em clientes como Petrobrás, Volkswagen, Telemar, Brasil Telecom, Ulbra, Serpro, Cargill, dentre vários outros.

Sócio fundador da ABSEG, desde 2004 atua como diretor da integradora FMB Sistemas, por ele fundada, e também desempenha o papel de diretor da fabricante americana Apollo Security para o Brasil.

Consultoria Empresarial Aplicada à Segurança

Nino Ricardo de Menezes Meireles

***Resumo:** A busca pelo serviço de consultoria em segurança empresarial tem crescido muito nos últimos anos. A demanda por este tipo de prestação de serviço tem levado muitos profissionais da área a buscarem este tipo de atividade, mas poucos a exercem de forma profissional. Para a grande maioria é uma atividade complementar e esporádica, ou seja, não contínua.*

1.1. MERCADO

Wallace Vieira, consultor autônomo do SENAI, afirma que estão surgindo novos nichos de consultoria em decorrência da revolução do trabalho versus emprego, o que causa a reorganização das empresas e a reconversão do trabalho. Esse processo, provocado pela adoção do neoliberalismo, está diminuindo as empresas, reduzindo a oferta de emprego, mas não de trabalho.

Outros nichos são criados pelo andamento da reforma do Estado, como a administrativa. A passagem do público para o privado altera os padrões administrativos e os objetivos finais, pois em grande parte a função social perde espaço para a obtenção imediata do lucro. Essa mudança de prisma leva à necessidade dos antigos funcionários públicos serem despertados e reciclados para as novas exigências. Esse tem sido um trabalho típico de consultores que atuam em educação e treinamento.

A questão ecológica também representa outro nicho potencial, trazendo a ISO 14000. Hoje, qualquer investimento leva em conta a recidanização da empresa, que exige novos valores, procurando estabelecer um novo paradigma: a empresa cidadã.

A cobrança dos ecologistas que levou os governantes a adotar leis de proteção ambiental, não pode ser esquecida, sob pena de "arranhar" a imagem da empresa junto ao cliente, preocupado com a melhoria da qualidade de vida.

O aumento da criminalidade aliado à falência do sistema público de segurança e o surgimento de uma cultura de segurança têm aberto o caminho para a atividade de consultoria em segurança empresarial, tendo como principais vertentes o planejamento do sistema de segurança e a análise do risco corporativo.

Antônio Andrade, diretor do IBCO, observa o aparecimento de possibilidades para os consultores em função da dinâmica da estabilidade econômica e do acirramento da concorrência motivado por fatores internos e principalmente externos por causa da inserção do Brasil no processo de globalização. Entretanto, o mercado exige cada vez mais competência e qualificação dos consultores, independentemente de sua especialização.

A descoberta dessas novas oportunidades obriga os consultores a deixarem de ser repetidores de projetos. Principalmente agora, pois o mercado vem recebendo profissionais qualificados de diversas empresas em virtude de terem perdido os seus empregos pela reestruturação das organizações. Eles dominam tecnicamente o trabalho que antes executavam, mas não possuem o domínio de outros valores importantes para o exercício da consultoria. Não possuem visão conceitual tática e operacional.

Além dos nichos apresentados, existem algumas tendências que precisam ser percebidas:

- Virtualização do mundo;
- Capital intelectual valendo mais que o capital financeiro;
- Diferenciação pela inovação;
- Tempo valendo mais que dinheiro;
- Personalização de produtos;
- Aumento do trabalho sem vínculo empregatício;
- Aumento da informalidade nas empresas;
- Crescente desregulamentação;

- Valorização da qualidade de vida;
- Responsabilidade social;
- Crescente violência social.

1.2. CONSULTORIA EMPRESARIAL

O trabalho de consultoria, como se conhece nos dias atuais, é algo muito mais abrangente do que já foi no passado. Apesar disso, consultoria é uma atividade muito antiga e que está presente em muitos momentos da nossa vida. Por exemplo, quando nós ajudamos uma criança a aprender a fazer alguma coisa, como comer, nadar, falar, no fundo estamos sendo consultores desta criança-cliente. Na prática, você está passando certo know-how a essa criança, para que ela possa seguir seu próprio caminho. Consultores, em essência, realizam isso profissionalmente o tempo todo, fazendo da transmissão de conhecimento seu modo de vida.

Ao se falar de transmitir conhecimento, estamos nos referindo a conhecimentos gerados e desenvolvidos pelo próprio consultor ou disponíveis publicamente, que o consultor recebe por toda a vida profissional e que disponibiliza para seus clientes da maneira e no momento mais adequado.

O consultor deve dispor de senso crítico, ter poder de liderança e capacidade de persuadir. Ele costuma ser contratado para resolver aquilo que supera a capacidade administrativa dos clientes, aquilo que a empresa necessita resolver naquele exato momento. A empresa busca nesse profissional externo a solução para seus problemas internos. Isso porque, entre outras coisas, o consultor não está ligado afetivamente com a empresa-cliente, tendo assim meios de atuar com visão crítica, usando mais razão do que a emoção.

Poderíamos dizer que consultoria empresarial é um processo interativo entre um ou mais agentes de mudança e uma determinada organização, visando à identificação de soluções ou oportunidades de melhorias que auxiliem a tomada de decisões por seus profissionais ou executivos.

A consultoria visa:

- Analisar o ambiente interno identificando as fraquezas e potencialidades;
- Analisar o ambiente externo identificando oportunidades e ameaças;
- Auxiliar na tomada de decisão com imparcialidade;
- Utilizar a expertise e transferir tecnologia.

As principais áreas de atuação da consultoria empresarial são:

- Planejamento estratégico;
- Planejamento estratégico de TI;
- Reestruturação empresarial;
- Redesenho de processo/padronização;
- Análise de clima organizacional;
- Remuneração e incentivos;
- Recrutamento e seleção;
- Avaliação de desempenho;
- Gestão financeira;
- Gestão contábil/tributária;
- Marketing/Comunicação;
- Logística;
- Análise de risco corporativo;
- Sistema de segurança empresarial;
- Outras.

A consultoria pode atuar de diversas formas, pois pode abranger a organização com um todo ou apenas alguma área específica. Além disso, os projetos podem ser de curta ou longa duração ou também na forma de intervenções pontuais.

A atividade de consultoria exige do profissional algumas características pessoais que serão a base para o seu sucesso. As principais são:

- Ética;
- Empatia;
- Flexibilidade;
- Confiabilidade;
- Sigilo;
- Fidelidade;
- Competência.

Poderíamos dividir a consultoria em: consultoria interna e consultoria externa. Ambas apresentam vantagens e desvantagens que precisam ser levadas em conta no momento da organização decidir por uma ou outra.

A consultoria interna apresenta como vantagens e desvantagens:

Vantagens

- Maior conhecimento dos aspectos informais da empresa;
- Maior acesso às pessoas;
- Participação ativa na avaliação e no controle do processo.

Desvantagens

- Menor aceitação nos escalões superiores;
- Geralmente tem menos experiência;
- Menor liberdade para revelar anomalias.

Já a consultoria externa apresenta as seguintes vantagens e desvantagens:

Vantagens

- Maior experiência;
- Maior aceitação pela alta administração;
- Pode correr riscos;
- Imparcialidade.

Desvantagens

- Menor conhecimento dos aspectos informais;
- Menor acesso informal às pessoas;
- Não convive com o dia a dia da empresa.

1.2.1. PESPECTIVAS

Uma pesquisa realizada nos Estados Unidos e comentada no livro Complete Book of Consulting (1996) demonstra que na década de 70 as empresas norte-americanas investiram um bilhão de dólares por ano em consultoria. Na década seguinte, esse volume subiu para dois bilhões e na década de 90 para quatro bilhões.

Esse desempenho ocorreu por causa de mudanças nas relações de trabalho. As empresas demitiram grande número de colaboradores e passaram a precisar de pessoas que lhes resolvessem os problemas, mas não representassem um custo fixo.

No Brasil, uma pesquisa do Instituto Brasileiro dos Consultores de Organização (IBCO), realizada em 1996, indicou que o mercado de consultoria movimentou mais de 250 milhões de reais por ano, excluindo-se as atividades de treinamento, seminários e palestras.

De acordo com o IBCO, as perspectivas imediatas e futuras da consultoria organizacional no Brasil mostram-se favoráveis em razão de as empresas terem que se adaptar às novas realidades conjunturais do mercado, buscando procedimentos inovadores e ousados, com a finalidade de crescer e sobreviver em muitos casos.

No setor da segurança empresarial, a mesma tendência se observa, não apenas pelos aspectos anteriores, mas também pelo aumento vertiginoso na necessidade de soluções de segurança eficientes, eficazes e efetivas e, dessa forma, capazes de minimizar o nível de risco ao qual as organizações estão expostas. Ao lado disso, temos outros fatores incrementadores da atividade de consultoria, como: o aumento da criminalidade, a falência do sistema público de segurança e o aumento do nível de exigência do cliente.

1.2.2. POR QUE SE CONTRATA UM TRABALHO DE CONSULTORIA?

Existem algumas razões para que as empresas contratem serviço de consultoria. As principais são:

- Projetos de curta duração, sem aumento de efetivo;
- Visão especialista;
- Ponto de vista independente;
- Treinamento dos colaboradores de uma empresa;
- Projetos para órgãos públicos ou fontes de financiamento;
- Necessidades de segurança.

Projetos de curta duração, sem aumento de efetivo

Depois da reengenharia, do downsizing, da readequação da economia à globalização e ao plano brasileiro de estabilidade econômica, as empresas necessitaram ter quadro de pessoal muito enxuto. Restaram menos profissionais para dar conta da rotina e dos assuntos extras que surgem inevitavelmente. O consultor pode ser contratado para fazer trabalhos que os colaboradores não conseguem fazer.

O excesso de trabalho do dia a dia não tem permitido, aos colaboradores, desenvolver e realizar projetos especiais, imprescindíveis para a modernização e o crescimento das organizações. Nesses casos, a contratação temporária de um consultor pode ser uma opção vantajosa. Ele não participa da rotina diária e será pago para dedicar seu tempo integralmente à empresa, enquanto durarem os serviços.

Visão especialista

A visão de especialista também é motivo para a contratação de serviços do consultor. Às vezes, a organização tem um problema específico, não há ninguém que entenda em profundidade daquele assunto e não quer agregar mais um profissional ao seu quadro. Nesse caso, é muito importante a visão do especialista, e não a do generalista.

Ponto de vista independente

Muitas vezes as empresas contratam um consultor para lhes apresentar uma visão independente do negócio, sem que haja um problema específico a ser tratado, mas apenas para contar com mais uma pessoa que pense em conjunto em uma avaliação estratégica. De fora da estrutura organizacional, detentor de experiência profissional diversificada e rica, o consultor tem condições de visualizar alternativas e soluções que atendam de forma ideal às necessidades da empresa.

Treinamento dos colaboradores de uma empresa

Muitas empresas não têm recursos financeiros para pagar horas de consultoria. Então, contratam profissionais que transferem conhecimento ao pessoal interno, para que possam fazer, posteriormente, os trabalhos sozinhos. Poderíamos chamar este tipo de consultoria de coaching consulting. O consultor treina toda uma equipe em novas técnicas ou abordagens e depois dá assessoria complementar para implementação e consolidação.

Projetos para órgãos públicos ou fontes de financiamento

As empresas frequentemente contratam serviços de consultoria para desenvolver projetos destinados a obter recursos de fontes de financiamento internacionais ou nacionais, como é o caso do BNDES, Finame, Penep etc. Outros casos estão ligados à necessidade de realizar projetos que atendam às exigências de órgãos públicos, como é o caso de projetos ambientais ou projetos que dêem suporte técnico a discussões com órgãos governamentais, seja na esfera federal, estadual ou municipal.

Necessidades de segurança

Diversas são as razões que levam uma organização a necessitar de consultoria na área de segurança. As razões variam deste um elevado índice de furto interno, passando pela sensação de insegurança causada pelo aumento indiscriminado da criminalidade, até experiências relacionadas a ações violentas de marginais, como: assalto, sequestro etc. Independentemente do fato gerador, a própria atividade de segurança, por ser uma atividade meio, não importando se a empresa possui um serviço terceirizado ou orgânico, já justifica o serviço de consultoria, pois a empresa não tem conhecimento necessário para desenvolver tal atividade com eficiência e eficácia.

Esse tipo de consultoria não se apresenta uniforme no nosso país, pois existem Estados como São Paulo, em que esse tipo

de serviço é comum, mas também temos a Bahia, onde esse tipo de serviço ainda é embrionário. De qualquer forma, a necessidade desse tipo de consultoria está em fase de crescimento em todo o Brasil.

1.2.3. QUEM CONTRATA CONSULTORIA?

Uma das perguntas mais comuns dos profissionais que querem prestar serviço de consultoria é: a quem vender esse serviço? Existem alguns segmentos do mercado que buscam esse tipo de prestação de serviço.

Grandes empresas

São clientes assíduos de consultorias de todos os portes. No entanto, esse segmento de mercado possui uma peculiaridade: geralmente são sociedades anônimas, comumente apoiadas por grandes empresas de auditoria, como Arthur Andersen, Coopers e Lybrand, Price Waterhouse etc. As empresas de auditoria que prestam serviço a tais tipos de cliente podem representar uma grande barreira ao novo consultor.

Para entendermos melhor esse contexto é necessário fazer um breve retrospecto das grandes empresas de consultoria e auditoria, as chamadas BIG SIX – Arthur Andersen, Coopers & Lybrand; Deloitte & Tauche; Price Waterhouse; KPMG Peat Marwick e Ernst & Young. Iniciaram suas atividades há muito tempo como empresas de contabilidade e, posteriormente, de auditoria. Pressionadas pelos clientes que necessitavam de aconselhamento, passaram também a prestar serviços de consultoria e treinamento.

Apesar da dificuldade, os consultores novos e independentes têm uma grande vantagem sobre as grandes consultorias: o preço. Hoje, como as empresas estão com orçamentos cada vez mais apertados, uma proposta mais econômica pesa muito na hora da decisão. Apesar disso, não é tarefa fácil iniciar um trabalho em uma grande organização.

Podemos dizer que existem duas maneiras prováveis dessa prestação de serviço se tornar realidade: iniciar sua atividade na empresa através de treinamento ou sendo contratado para um trabalho específico. Em ambos os casos, é importante aproveitar a oportunidade para fazer um trabalho de excelente qualidade não se descuidando de nenhum detalhe.

Médias empresas

Não contratam consultoria com a mesma frequência das grandes organizações, mas nesse setor ocorre um fato interessante: as associações de classe patronais costumam contratar muito treinamento para grupos fechados em seu segmento empresarial.

Outra forma de vender serviço para as médias empresas é realizar trabalhos por intermédio das federações de indústrias ou de comércio dos Estados.

Pequenas e micro empresas

Raramente contratam o serviço de consultoria sozinhas. É necessário para se conseguir vender o serviço várias visitas e muitas negociações.

O que geralmente ocorre são os fechamentos de projetos em cooperativa, com instituições que atendam às pequenas e micro empresas, como SEBRAE, SENAI e SENAC.

Com recursos de instituições de fomento

Existem no Brasil numerosas instituições que dispõem de linhas de crédito para fomento a projetos nas áreas de melhoria de competitividade, qualidade, tecnologia etc.

As duas instituições federais mais importantes são a Financiadora de Estudos e Projetos (FINEP) e o Conselho Nacional de Pesquisa e Desenvolvimento (CNPq).

SENAI, SENAC e SEBRAE

Essas instituições de ensino profissionalizantes têm sido grandes contratadoras de serviços de profissionais independentes, em parcerias ou como subcontratações de programas de desenvolvimento de tecnologia educacional, de treinamento técnico ou gerencial e de projetos variados.

1.2.4. O TRIÂNGULO DA VENDA

Os três pontos importantes na hora de vender trabalhos de consultoria:

1. O nome da empresa, as referências;
2. A metodologia do trabalho;
3. A reputação do consultor.

Até a década de 80, quando no Brasil ainda não era usual as organizações contratarem serviço de consultoria, o que pesava muito era o nome, ou a grife, das empresas que prestavam o serviço. O cliente não estava preocupado com a metodologia nem com quem seria o consultor.

No final da década de 80 e início da de 90 ocorreu uma mudança nos pesos relativos desse conjunto. A venda passou a ficar dividida entre o nome da consultoria e a metodologia de trabalho. Diante desse cenário, as empresas de consultoria lançaram novas metodologias, com o intuito de fortalecer sua imagem e aumentar as chances no mercado. Nesse momento, o nome do consultor ainda permanecia em segundo plano.

Atualmente, o nome do consultor é muito importante no processo de venda. Os clientes passaram a valorizar o profissional responsável pelo projeto e sua implantação.

De qualquer forma, é importante que o consultor se preocupe com os três pontos. Ele deve buscar construir uma imagem sólida e estabelecer parceria com especialistas de outras áreas. Além disso, deve ter uma metodologia que transmita confiança ao cliente e faça com que ele o veja como a solução para os seus problemas.

Tratando-se de consultoria externa, é necessário que o consultor tenha algumas preocupações na venda de seu serviço. A primeira delas é a forma de divulgação. É importante que exista preocupação com o marketing.

Os meios de divulgação também devem fazer parte da preocupação do consultor. É importante que várias fontes sejam utilizadas, tais como:

- Site na Internet;
- Participação em feiras, eventos etc.;
- Treinamentos;
- Artigos;
- Lista de telefones;
- Transdoor;
- Outdoor;
- Televisão;
- Jornal;
- Outras.

Outra preocupação importante é a forma de prospecção de novos clientes. É importante que o consultor estabeleça claramente o seu nicho de mercado, que deverá ter como norte a sua especialização.

Essas duas primeiras dizem respeito à busca de clientes. Após essa etapa, é necessário desenvolver uma excelente apresentação dos trabalhos e do folder, que deverá conter, no mínimo:

- Tipos de serviços;
- Tipos de treinamentos;
- Currículo resumido;
- Carteira de clientes.

É igualmente importante que o consultor tenha uma ótima habilidade de negociação e saiba quando e como fazer o fechamento da venda do seu serviço. Além disso, é importante perceber que a venda não pode ser vista como uma arte, mas sim, como uma ciência. Uma boa estratégia deve envolver todos os aspectos de uma venda, de identificação total do público-alvo ao relacionamento permanente com o cliente.

As últimas tendências do mercado na área de vendas são:

- Inovação – Não é necessário reinventar a roda, mas deve-se criar um diferencial para surpreender o cliente.
- Identidade total com o público-alvo – É preciso ter uma identidade total com os clientes para conseguir atraí-los e conservá-los.
- O consumidor valoriza a ética – Um número crescente de empresas e de consumidores procura conhecer o modus operandi de seus parceiros, para se proteger de fraudes.

- Oferta em múltiplos canais – Atualmente, é fundamental estar acessível ao cliente, de todas as formas possíveis.
- Visão global do negócio – É fundamental o consultor ter uma visão macro de sua atividade.
- Praticidade – É preciso oferecer comodidade e agilidade para o cliente.
- Relação personalizada – É fundamental perceber o perfil de cada cliente.
- Só prometer o que se pode cumprir – Entregar o que prometeu é uma premissa que deve ser aplicada a qualquer negócio.
- Pós-venda – Dar atenção após a venda é fundamental para manter os elos e fazer com que o cliente lembre-se de você.

1.2.5. FORMAS DE ATUAÇÃO

No início da carreira o consultor deve buscar estabelecer uma sociedade informal com alguém e, aos poucos, ir ajustando gostos e habilidades. Mas essas associações, formais ou não, só darão certo se forem formadas por pessoas diferentes, mas com algumas afinidades.

Se dois consultores, com os mesmos pontos fortes e fracos, tentarem uma experiência em conjunto, chegarão a resultados não muito satisfatórios, podendo ocorrer desentendimentos durante os trabalhos.

Consultores externos podem exercer suas atividades de diversas formas. As principais são:

- Consultor independente;
- Parceiro de um grupo;
- Líder de um grupo;
- Dono de empresa;
- Colaborador de empresa de consultoria;
- Cooperativa.

Consultor independente

Essa forma de trabalho é representada pela empresa de única pessoa, que pode ou não ter envolvimento com parceiros para trabalhos específicos.

O consultor tem que assumir todas as tarefas, sendo bom ou não na execução delas.

A principal vantagem desse tipo de atuação é que o consultor segue a sua intuição e filosofia de trabalho. Na atuação independente, o consultor tem total liberdade de decidir sobre sua vida profissional, inclusive no que se refere a tipo e forma do trabalho, a horários e carga de trabalho etc.

As desvantagens desse tipo de atuação são: a falta de parâmetros e a necessidade de assumir todas as atividades inerentes ao negócio, desde as estratégicas, até as operacionais.

Parceiro de um grupo

Outra maneira de atuar no mercado é fazer parte de um grupo de consultores associados, no qual um consultor mais experiente lidera os projetos. Nesse caso, os consultores têm missão, políticas e valores comuns, enquanto o modelo organizacional visa à redução dos custos fixos. Os recursos são compartilhados, o desenvolvimento de metodologias de trabalho ocorre em parceria, mas existe autonomia administrativa e jurídica. O escopo de atendimento é amplo, mas cada consultor é especializado em uma área específica.

O consultor pode escolher entre participar de um grupo ocasionalmente, como parceiro fixo ou como associado. Nos dois primeiros os consultores dividem a elaboração e a implantação de projetos conforme é combinado entre os parceiros.

É comum muitas empresas trazerem, depois de seus nomes, o complemento "& Associados". O que seria isso? O consultor que trabalha como associado de uma empresa encontra uma estrutura pronta, com carteira de clientes já formada e metodologia de trabalho definida.

Essa solução tem algumas vantagens. A primeira é de permitir que todos continuem com elevado grau de liberdade para trabalhar, pois não existe uma relação de trabalho e subordinação. Outra vantagem é a ampliação do escopo, do leque de opções de serviços, pois se acaba chegando a um grupo de profissionais grande e forte, com variedade de especialidades. Já para o cliente, as vantagens são a agilidade, a complementaridade e os custos fixos baixos.

A desvantagem fica por conta de alguns acertos que precisam estar sempre sendo feitos. Trata-se de uma sociedade cujas regras são informais, e por isso, é preciso estar permanentemente negociando cada situação.

Líder de um grupo

É muito parecido com a associação. A diferença é que, nesse tipo, um consultor começa a ter muita projeção em determinado tipo de serviço ou de mercado e acaba liderando um grupo, que o ajuda na execução dos projetos, em razão de não conseguir dar conta do volume de trabalho que lhe pedem.

Outra situação é o líder de um grupo ser alguém de projeção, em função de ter ocupado posto de alta visibilidade, como ex-ocupante de cargo privado ou público, ou autor de livros que se tornaram best-sellers, ou ainda um palestrante famoso.

Dono de empresa

Trabalhar como dono de empresa de consultoria significa ter escritório, mobiliário, estrutura de serviços, colaboradores e todos os problemas oriundos dessa situação. A principal dificuldade desse modo de atuação são os custos elevados.

Colaborador de empresa de consultoria

Quem pretende entrar para uma empresa como colaborador terá que se submeter à cultura dessa empresa, assimilando seus valores, sua missão e filosofia de trabalho.

Participar de uma empresa de consultoria tem prós e contras. As vantagens estão ligadas ao nível maior de segurança financeira e de carreira, à possibilidade de aprender continuamente novas tecnologias e à construtiva convivência com outros profissionais mais experientes. A maior desvantagem está ligada ao fato de que as empresas, pela necessidade de garantir padrões uniformes de qualidade através do trabalho de muitas pessoas, deixam pouca liberdade para criar.

Cooperativa

É uma alternativa pouco utilizada no nosso país. Como em outros setores que utilizam essa forma de trabalho, na cooperativa há uma taxa de participação para beneficiar-se de certos recursos compartilhados, como infra-estrutura de escritório ou acesso a tecnologias adquiridas.

1.2.6. CARACTERÍSTICAS PESSOAIS

A maioria das empresas que contratam um consultor valoriza muito o profissional que tem conhecimentos ecléticos e diversificados. Portanto, além de conhecimento técnico, talento e criatividade, o bom consultor é aquele que se destaca, também, por uma série de outras características, sejam elas profissionais, culturais, políticas e psicológicas. Dentre diversas características importantes, algumas se sobressaem:

- Gosto pela pesquisa;
- Cultura geral e especialização;
- Habilidade e sociabilidade;
- Capacidade de lidar com vários assuntos ao mesmo tempo;
- Perspicácia.

Gosto pela pesquisa

O consultor tem que ser uma pessoa curiosa e que está sempre procurando informações novas, que lhe chegam através de várias fontes. O que mais interessa são as notícias ligadas diretamente ao seu ramo de atividade, tanto as de caráter geral quanto às que contribuem de forma intensa para a melhoria de sua cultura técnica.

O consultor só se mantém atualizado se investir muito em pesquisa e desenvolvimento. Em consultoria, pesquisa e desenvolvimento têm conceito muito amplo. São a soma de todo tipo de informação a que o profissional tem acesso através dos mais variados canais. Na prática, o esforço de atualização se traduz pela leitura de jornais e revistas (técnicas ou não), acompanhamento de noticiários no rádio e televisão e navegação na Internet.

Frequentar exposições, feiras e congressos também representam uma forma de atualização, porque esses eventos apresentam novidades importantes que, normalmente, acabam se transformando em tendências. Além de se tornar público ao circular em ambientes que normalmente recebem empresários e homens de negócios, o consultor tem a chance de enriquecer sua

cultura geral.

Cultura geral e especialização

Cultura geral ampla é outra característica importante para o consultor. Ela deve parecer em vários níveis, como: gestão empresarial, comportamental e técnica.

Quanto mais desenvolver trabalhos com altas diretorias, mais generalista o consultor terá que ser, pois os altos dirigentes querem ao seu lado pessoas de visão e conhecimento amplos de negócio e do ambiente empresarial em que a empresa atua. Já se a atividade do consultor estiver voltada para os níveis operacionais, ele terá que ser um especialista.

De acordo com o consultor Fábio Rocha existem dois caminhos a serem perseguidos do ponto de vista da especialização:

- Se o tipo de trabalho é mais voltado para a alta direção de empresas, é fundamental investir tempo em desenvolvimento generalista, para ter conhecimento cada vez mais amplo das questões complexas da conjuntura e do mundo dos negócios.
- Se o foco principal estiver voltado para a média gerência e os níveis operacionais, é necessário investir na especialização dos serviços que se consideram essenciais na busca da excelência nas áreas de atuação.

Não existe um consultor totalmente generalista nem totalmente especialista. Todos têm formação básica com ênfase em uma área específica.

Habilidade e sociabilidade

Visão ampla também fornece ao consultor subsídios para ponderar adequadamente os componentes técnicos, econômicos e políticos da cultura das empresas, a fim de viabilizar a implementação das idéias e dos projetos que propõe para solucionar os problemas de cada empresa-cliente.

É importante frisar que não basta encontrar soluções para os problemas; é preciso saber como se relacionar com as pessoas em todos os níveis da organização, para obter colaboração e conseguir colocar idéias em prática. As habilidades pessoais e interpessoais podem representar a diferença entre um projeto bem sucedido e outro interrompido.

Capacidade de lidar com vários assuntos ao mesmo tempo

A depender da forma de atuação e do porte do negócio, o consultor terá que realizar várias tarefas praticamente juntas: planejamento do trabalho, marketing pessoal, elaboração e follow-up de propostas, venda de trabalhos, administração e execução de projetos e emissão de faturas dos serviços prestados.

Por outro lado, o consultor irá trabalhar para vários clientes, que têm problemas diferentes e cujos projetos estão em fases distintas, ou seja, alguns começando, outros em curso ou terminando. Cada um deles necessita de um tipo de acompanhamento, com várias ações e providências a serem tomadas.

Perspicácia

Significa saber captar as necessidades do cliente, considerando todas as peculiaridades do negócio. Pensar depressa e agir com perspicácia são outras duas qualidades importantíssimas.

Às vezes, um cliente não sabe ou não consegue explicar, com absoluta certeza, quais são suas necessidades. É preciso, então, ter habilidade de entender questões não explicitadas, de deduzir e seguir adiante. No final da exposição do cliente, o consultor deve encontrar uma forma de mostrar-lhe, sem ferir suscetibilidades, que ele deixou de se referir a outras questões importantes, dado às características do seu negócio.

Outra situação comum é o cliente chamar um consultor para resolver um problema que ele garante saber qual é. No entanto, à medida que o consultor vai tomando ciência da situação, percebe que não é bem aquele o problema que precisa ser resolvido.

O consultor não deve elaborar sugestões somente com base no que foi explicitamente apresentado. Além do seu conhecimento de determinado assunto, o consultor deve estar alerta para captar pequenos fatos que acabam por levá-lo a conclusões importantes.

1.2.7. HABILIDADES

Poderíamos agrupar as habilidades necessárias ao consultor em: técnicas, pessoais e interpessoais.

Técnicas

Inicialmente, é importante que o consultor tenha tido uma boa formação escolar e universitária. Essa formação é a base que sustentará uma posterior bagagem profissional.

A experiência de trabalhar em uma empresa que dá oportunidades de atuação a seus profissionais ajuda bastante um consultor em início de carreira. Além disso, é importante que ele tenha uma carreira diversificada e especializada.

Caso o profissional tenha ocupado várias posições em uma só empresa, ou trabalhado em diversas empresas de setores diferentes, achará mais fácil atuar como generalista. O profissional que se manteve durante anos em uma única área, mesmo que tenha trabalhado em empresas diferentes, atuará melhor como especialista.

Pessoais e interpessoais

Tratar com pessoas e negociar situações sem ter o poder nas mãos são habilidades que têm sido muito desenvolvidas entre os executivos. Há alguns anos, apenas, essa preocupação passou a fazer parte dos responsáveis pelo treinamento desses profissionais. Quando as pessoas fazem uma auto-análise, percebem que essa habilidade não foi desenvolvida durante a carreira, principalmente se tratar de profissionais da área técnica ou mais ligada às ciências exatas.

As principais características são:

- Saber ouvir;
- Saber observar;
- Saber investigar;
- Saber levantar dados e informações;
- Ter habilidade para deduzir;
- Saber raciocinar baseado em hipóteses;
- Dominar a arte de dar apoio e saber discordar sem romper o relacionamento com o cliente;
- Dominar a arte da comunicação;
- Dominar a arte de aconselhar.

Apesar de todas as características relacionadas serem importantes, quatro se apresentam como muito importantes:

TER HABILIDADE DE DEDUZIR

O consultor deve ter, além da visão cartesiana e exata, um raciocínio dedutivo, fazer uso do "feeling" e saber extrair das informações passadas pelo cliente as que realmente lhe interessam.

DOMINAR A ARTE DE DAR APOIO

O consultor precisa saber dizer NÃO com determinação e firmeza. Até porque, às vezes, o cliente pode estar precisando disso. Mas, por outro lado, também deve saber dar apoio na hora certa, seja quando as coisas dão certo ou errado.

Um dos papéis do consultor é ser o "ombro amigo". É comum o consultor ir a um cliente e, na reunião com a diretoria, estar tudo bem. Mas, na hora em que se resolve conversar separadamente com cada diretor, a mesma história se transforma em um mar de lágrimas, com reclamações de diversos tipos.

É nesse momento que o consultor percebe como as questões entre as pessoas são mal administradas. Nessa situação, tais habilidades vão fazer falta. Se o consultor não souber ouvir, filtrar as informações, dar apoio e dizer NÃO, ou seja, dominar a diplomacia interpessoal, terá dificuldade de administrar o relacionamento com pessoas que nem sempre são de trato fácil.

DOMINAR A ARTE DA COMUNICAÇÃO

Um consultor que não sabe se comunicar bem, falar em público, terá um grande problema a resolver. Não se trata de algo sem solução, mas esse tema não pode passar despercebido. É comum o consultor ter que apresentar idéias para uma pessoa, para um grupo pequeno ou ainda para um público maior. É necessário que a apresentação seja sempre muito boa. Consultores podem perder um trabalho por não saberem comunicar sua estratégia para o cliente.

DOMINAR A ARTE DE ACONSELHAR

Aconselhamento é a discussão de um problema visando sua solução, ou, no mínimo, apontar caminho de como melhor lidar com ele. Aconselhar não é a mesma coisa que treinar. Enquanto o treino está voltado a questões de habilidades o aconselhamento diz respeito a problemas pessoais.

O aconselhamento pode ser dividido em diretivo, não-diretivo e participativo. O primeiro é caracterizado pelo controle da situação por parte do consultor, pois ele irá ouvir o problema, decidir o que deve ser feito e dizer o que fazer. Já o não-diretivo parte da premissa de que as pessoas conseguem resolver seus próprios problemas com a ajuda de um ouvinte especialista e experiente. O consultor irá ouvir, repetir, sintetizar, compreender e dar feedback. Mas quem decidirá é o cliente. O terceiro tipo é um meio termo entre os anteriores, pois o consultor será um ouvinte ativo, porém desempenhará um papel mais afirmativo, oferecendo observações e conselhos. Devido ao conhecimento e a experiência, o consultor muitas vezes será capaz de discutir a situação de uma perspectiva mais ampla e poderá oferecer uma visão diferente sobre o problema discutido.

1.2.8. ÉTICA NA CONSULTORIA

Na atividade de consultoria não há muitas leis. Não existe conselho regional de consultores. Portanto, para reger a ética das atividades do consultor, existe muito mais a observância de preceitos morais, de regras práticas de conduta profissional e pessoal, ou simplesmente, do uso do bom senso.

A questão ética é bastante delicada, pois se refere a diferentes relacionamentos entre o consultor e:

- Seu cliente direto;
- Demais pessoas com as quais ele se envolve na empresa, para poder realizar o seu trabalho;
- Outros consultores;
- Mídia;
- Outros clientes.

Vivemos em um ambiente em que a ética costuma ser assunto de muito discurso e pouca obediência e entendimento práticos. Consequentemente, talvez haja entre nós pouca disposição para respeitar a ética em nosso país. O Instituto Brasileiro dos Consultores de Organização (IBCO) sentiu a necessidade de criar um código de ética no intuito de gerar um marco de referência para usuários e consultores.

A atividade do consultor, desde a fase de prospecção de mercado e contato inicial, passando pelas fases de entendimento e proposta, contrato, coleta de dados, diagnóstico, decisão, implementação e extensão, acompanhamento ou término, quase sempre está ligada a uma penetração no âmago dos assuntos e dos problemas do cliente.

É inevitável que o consultor tenha contato e conheça muitos dados considerados confidenciais. Assim, surge uma questão ética, de quão bem será guardado o sigilo de dados e informações na mão do consultor e de seus funcionários.

Serviços de consultoria em áreas que afetam as estratégias e os sistemas empresariais, como políticas financeiras, processos empresariais, políticas de mercado, de produção, de tecnologia, de investimentos, reestruturações, programas de qualidade e produtividade, segurança corporativa entre outros, envolvem responsabilidades complexas pelo sucesso futuro da empresa.

Resumidamente, iremos apresentar alguns pontos do código de ética do IBCO, nos tópicos: relações com o cliente e relações com a comunidade.

Relações com o cliente

É essencial que o consultor estabeleça inicialmente com o cliente os objetivos do trabalho, dos meios a serem utilizados, das dificuldades e limitações prováveis, da estimativa de tempo e da estimativa de gastos envolvidos.

Os trabalhos devem ser realizados visando à introdução de inovações que objetivem auferir um melhor desempenho do cliente, transferindo-lhe todos os conhecimentos necessários à perfeita continuidade do funcionamento dos serviços implantados, jamais retendo elementos ou mantendo reserva sobre conhecimentos que seriam importantes para que o cliente se torne independente em relação ao consultor.

Ao trabalhar para clientes que atuam em um mesmo ramo de negócios, sendo concorrentes entre si, e ainda, prestando serviços em áreas de natureza similar, o consultor deve deixar clara esta situação tanto para seus clientes atuais como para os potenciais.

O consultor deve adotar todos os cuidados para a preservação de sigilo com relação às atividades e informações de seus clientes, inclusive na guarda de documentos e na fidelidade de seus colaboradores.

Na determinação de seus horários, o consultor deve levar em conta as características dos serviços por ele prestados, e

nos casos em que ela estiver vinculada aos resultados alcançados pelo cliente em função de seus serviços é essencial que o referencial para os resultados seja o longo prazo, ultrapassando o período de sua atuação direta.

O consultor deve propor a execução de serviços para os quais está plenamente capacitado, evitando assumir tarefas em campos onde não se encontre tecnicamente atualizado, ou não tenha experiência.

Relações com a comunidade

A profissão do consultor implica em um aporte de conhecimento às empresas, criando perante a sociedade uma imagem de saber e influência. Esse prestígio caracteriza a visibilidade da profissão, gerando vínculos de responsabilidade para com a sociedade, que devem ser respeitados e levados em consideração.

A sociedade espera que o consultor atue como um agente de mudança e essa expectativa deve ser atendida pela contribuição que ele pode prestar ao desenvolvimento técnico, administrativo e tecnológico, bem como à modernidade e eficiência organizacional.

1.2.9. COUNSELING

Dentro da atividade de consultoria, o counseling é o nicho que mais cresce nos Estados Unidos, segundo a National Career Development Association. No Brasil, os sinais de evolução da atividade também são evidentes, embora em menor proporção. Esse é um tipo de serviço, no entanto, que não costuma constar no currículo das grandes consultorias. Os counselors, em geral, são independentes. A maioria trabalha para pessoas jurídicas, atendendo grupos de colaboradores indicados pelas empresas. Mas há alguns que estendem seus serviços a pessoas físicas.

O aconselhamento de carreira envolve três questões básicas: o que há de errado na vida profissional? O que vai bem? O que está faltando?

O objetivo do serviço é aliar sua experiência profissional às suas necessidades e expectativas. Para descobrir mais sobre valores, habilidades, traços de personalidade e objetivos das pessoas, a maioria dos consultores segue uma metodologia parecida. As abordagens podem ser diferentes. Alguns pedem ao cliente para elaborar um jornal com as principais manchetes de sua vida profissional. Outros sugerem que ele traga o currículo para, juntos, o avaliar. É comum serem utilizados pelos consultores testes psicológicos, questionários, jogos lúdicos e até dramatizações.

1.2.10. PROCESSO DECISÓRIO

Como o consultor é buscado, normalmente, para resolver problemas nas organizações é importante que o consultor compreenda o que vem a ser um problema e como se processa o processo decisório.

De acordo com Paulo Roberto Portella (2003), o processo decisório é uma sequência de etapas que forma uma decisão. Um aspecto particular deste processo chama-se planejamento, pois envolve características especiais. O ato de tomar uma decisão pode ser estudado sob duas perspectivas: do processo e do problema. A primeira é uma perspectiva muito genérica e se concentra nas etapas da tomada de uma decisão, ou seja, no processo decisório como uma sequência de atividades e relaciona-se quase que exclusivamente com o procedimento a ser adotado e não com o conteúdo da decisão. Envolve uma sequência de etapas em que se procura identificar o problema e as possíveis alternativas.

Herbert Simon afirma existir três fases distintas no processo de tomada de decisão: a atividade inteligente, a atividade de concepção e a atividade de escolha. A primeira é a fase inicial e consiste na procura dos fatores ou condições que demandam solução no ambiente. Esta seria uma fase de busca de informações, ou seja, uma atividade de inteligência. A segunda fase consiste em inventar, desenvolver e analisar possíveis alternativas de ação. Na última fase procede-se à seleção de uma alternativa particular de ação, dentre as opções desenvolvidas na segunda fase.

A perspectiva do problema é orientada para a resolução dos problemas e concentra-se, principalmente, na determinação e no equacionamento do problema a ser resolvido. Paulo Portella (2003) define um problema como uma discrepância entre a realidade e o que poderia ou deveria ser. Geralmente uma organização se defronta, ao mesmo tempo, com uma gama de problemas que variam consideravelmente em graus de complexidade.

Os problemas podem ser separados em dois grupos: os problemas estruturados e os não estruturados. O problema estruturado é aquele que pode ser perfeitamente definido, pois suas principais variáveis são conhecidas. Esse tipo de problema admite três tipos de decisão: decisão sob certeza, decisão sob risco e decisão sob incerteza. Na primeira, as variáveis são conhecidas e a relação entre a ação e as consequências é determinante. Na segunda, as variáveis são conhecidas, mas a relação entre a ação e as consequências é conhecida em termos de probabilidade. Na última, embora as variáveis sejam conhecidas, as probabilidades para determinar as consequências de uma ação são desconhecidas ou não podem ser determinadas com algum

grau de confiabilidade.

Um problema não estruturado é aquele que não pode ser claramente definido, pois uma ou mais de suas variáveis são desconhecidas ou não podem ser determinadas com algum grau de confiança.

1.2.11. PROPOSTA

A proposta é um pedido de ajuda, porque o cliente não sabe como solucionar o problema, precisa de recursos adicionais ou deseja estudar e avaliar idéias e abordagens diferentes, antes de escolher uma. Também há a consideração de que o cliente precisa de alguma coisa na qual basear uma avaliação dos concorrentes para um contrato e julgar a adequação de cada um. A solicitação de proposta é um indicador para o sucesso na redação de proposta, porque mostra ao consultor o que o cliente necessita. Segundo Herman Holtz (1997) a solicitação de proposta tem quatro elementos principais:

1. Uma carta introdutória;
2. Instruções sobre a proposta;
3. Informação padrão sobre a organização solicitante;
4. Uma exposição do trabalho, descrevendo o problema ou a necessidade do cliente.

Para que o cliente possa perceber se o consultor terá condições de realizar um bom trabalho, a maioria das solicitações de propostas pede:

- Uma análise da solicitação, demonstrando que o consultor entendeu a necessidade do cliente;
- Um planejamento preliminar do programa;
- Um programa específico, com os detalhes adequados sobre pessoal, organização, cronograma, produtos finais, produtos intermediários, procedimentos, controle de qualidade, prazos etc.;
- Qualificações do consultor;
- Registro verificável da experiência do consultor.

Do ponto de vista do consultor existem alguns pontos que precisam ser observados no momento da confecção de uma proposta: esfera de ação, formato, quantidade de esforço físico etc. Muitos consultores optam por não buscar negócios governamentais por considerarem as solicitações de propostas onerosas demais e a redação da proposta muito cara.

O tamanho da proposta depende do tamanho do projeto. Os pequenos projetos em geral exigem propostas simples e informais; na verdade, cartas de diversas páginas a que se incorpora a proposta. Frequentemente são chamadas de cartas-proposta.

Normalmente a proposta deve conter os seguintes itens:

- Objetivo;
- Abrangência;
- Produtos a serem gerados;
- Metodologia;
- Condições comerciais;
- Responsabilidades.

1.2.12. HONORÁRIO

Na consultoria, honorário e lucro não são sinônimos. O honorário é aquilo que o consultor cobra, normalmente por hora ou por dia, pelos seu serviço, através do qual espera realizar um lucro. Os honorários são o seu rendimento total.

Não existe um padrão de preços para os consultores. A própria natureza da consultoria quase que determina que cada consultor tenha um valor único, estabelecido de acordo com diversos fatores. As principais formas são:

- Por projeto/produto;
- Por hora;
- Por resultado/risco;
- Valor fixo;
- Por disponibilidade;
- Permuta.

O consultor, aceitando uma atribuição de um cliente, participa de um contrato com esse cliente, assim que os dois chega-

rem a um acordo. Um contrato não é um pedaço de papel, é um acordo. Assim, o acordo entre o consultor e o cliente é um contrato, mesmo que seja apenas verbal.

Os contratos verbais são perfeitamente válidos e representam um compromisso. Entretanto, a memória humana é falha, especialmente se e quando surge uma controvérsia a respeito dos termos do contrato (sobre o que foi acordado). Consequentemente, é sensato registrar o contrato especificando os seus termos no papel.

Provavelmente, é melhor não usar a palavra contrato, mas chamá-lo de carta de concordância ou simplesmente acordo. Se possível, visando à simplicidade e informalidade, é interessante fazer esse acordo em uma única página.

Nino Ricardo de Menezes Meireles

- ***Engenheiro Civil;***
- ***Especialista em Consultoria e Gestão de Recursos Humanos;***
- ***Especialista em Gestão Estratégica de Negócios;***
- ***Extensão em Administração da Segurança Empresarial;***
- ***Extensão em Gestão de Riscos Corporativos;***
- ***Membro da ABSEG (Associação Brasileira de Profissionais de Segurança).***

PRODUÇÃO ACADÊMICA

- ***Livro - Desmitificando a Segurança (Edufba – 2002).***
- ***Livro - Recursos Humanos no Setor de Segurança. O que você precisa saber. (Taba Cultural - 2005).***
- ***Livro – Sistema de Segurança (Étera - 2006).***
- ***Livro – Manual do Gestor da Segurança Corporativa (em edição).***
- ***Monografia – Recursos Humanos e a Segurança. Problema ou Solução? (2003).***
- ***Pesquisa motivacional do profissional de segurança (2003). Com atualizações em 2004 e 2005.***
- ***Pesquisa sobre a relação entre o vigilante e os subsistemas eletrônicos de segurança (2005).***
- ***Vídeo-aula – Recursos Humanos na Segurança (Jornal da Segurança – São Paulo, 2008).***
- ***Vídeo-aula – Sistema de Segurança (Jornal da Segurança – São Paulo, 2008).***
- ***Vídeo-aula – Planejamento Contingencial (em edição).***
- ***Vídeo-aula – Meios Ativos de Segurança (em edição).***

EXPERIÊNCIA PROFISSIONAL

- ***Consutor e Instrutor de segurança de grandes empresas, Professor do curso de graduação tecnológica em Gestão da Segurança Empresarial nas disciplinas: Teoria Geral da Segurança Física, Segurança Pessoal, Relacionamento Interpessoal e Logística.***
- ***Coordenador acadêmico do curso de graduação em Gestão da Segurança Empresarial.***
- ***Coordenador acadêmico do MBA em Gestão Estratégica da Segurança Corporativa.***

Segurança da Informação e do Conhecimento

Tácito Augusto Silva Leite

Parte 1 - Conceitos básicos e as fases do ciclo de vida das informações

O objetivo principal deste artigo é estudar as principais ameaças, vulnerabilidades, riscos dos ativos de informação de uma organização, bem como as ferramentas e práticas mais eficientes para elaboração de uma Política de Segurança de Informações, aplicável às instituições públicas e privadas.

Nas três próximas partes deste artigo, dando continuidade ao presente trabalho, abordaremos os seguintes assuntos: ameaças e vulnerabilidades que afetam as informações; os meios de proteção e um modelo de Política de Segurança de Informações.

Antes de darmos continuidade, vale questionar:

O que é informação? Informação é um recurso que, como outros importantes recursos de negócios, tem valor para uma organização e, por conseguinte, precisa ser protegido adequadamente (BRITISH STANDARDS INSTITUTE - BS 7799 –1, 1999). Para CARUSO (1999) , a informação é aquilo que sintetiza a natureza de tudo o que existe ou ocorre no mundo físico.

O que é ameaça? Para FONTES (2000) , a ameaça é a ação de uma pessoa, situação ou fenômeno que seja considerado um perigo para a disponibilidade do recurso ou para o seu uso indevido. SÊMOLA (2003) complementa informando que as ameaças exploram as vulnerabilidades existentes para se concretizarem, provocando danos como à perda da confidencialidade, integridade e disponibilidade dos ativos de informação.

O que é vulnerabilidade? As vulnerabilidades são os "elos fracos da corrente". São lacunas existentes na estrutura física, lógica ou administrativa, com potencial de ser explorado pelas ameaças, vindo a causar danos.

Em um passado próximo as informações nas organizações eram armazenadas apenas em papel, e o seu patrimônio era medido pelos bens materiais. Hoje este cenário está mudado: as informações são armazenadas em meios eletrônicos e cada vez mais estão se transformando no grande patrimônio das empresas.

No presente, as redes de computadores, em especial a Internet, chegaram para democratizar o acesso às informações. Porém, há que se considerar os requisitos de segurança envolvidos neste processo. E isto é um aspecto primordial, mas, muitas vezes, passa despercebido.

Por mais que os meios eletrônicos estejam armazenando a maioria das informações, não podemos esquecer os documentos nas mesas dos escritórios, que continuam existindo e sempre existirão, e são tão frágeis como as informações armazenadas eletronicamente.

Assim, necessário se faz definir os critérios para bom uso e proteção das informações. A POLÍTICA DE SEGURANÇA DE INFORMAÇÕES (PSI) é justamente o conjunto coordenado destes critérios. Tal Política é a formalização de todos os aspectos considerados relevantes por uma organização para a proteção e monitoramento de informações e conhecimento, tanto em meios computacionais como fora deles. A PSI deve contemplar, de forma abrangente e objetiva, todos os aspectos importantes para a proteção lógica e física das informações e dos recursos computacionais.

No que tange à objetividade da PSI, é preciso focar exatamente o que se quer proteger e como. É esse tipo de abordagem que permite a transparência e adesão do processo por todos os envolvidos, a saber: os usuários, a alta direção da organização e o pessoal responsável diretamente pela administração dos recursos. Os envolvidos precisam saber claramente quais são os seus direitos e deveres para que se possa garantir um real envolvimento de todos.

Vale ressaltar que uma PSI deve sempre ser aprovada e apoiada pela alta direção da organização. Este aspecto é de extrema relevância, vez que sem o envolvimento da alta direção, a PSI corre um grande risco de ser apenas mais um amontoado de documentos engavetados.

Com relação às vulnerabilidades dos ativos de informação, devemos identificá-las por meio de um Diagnóstico de Segurança e uma Análise de Riscos, procedimentos que também mapeiam as ameaças existentes.

Para podermos proporcionar segurança às informações, precisamos entender seu ciclo de vida. Lembrando antes que a Segurança de Informação é caracterizada pela preservação da confidencialidade, integridade e disponibilidade dos ativos de informação (BRITISH STANDARDS INSTITUTE - BS 7799-1, 1999).

As informações passam pelas seguintes fases:

1. Criação: Essa fase da vida da informação se caracteriza pelo surgimento de uma informação elaborada, que pode ser fruto do cruzamento de outras informações correlatas ou pode ser a materialização do conhecimento adquirido durante um processo. Essa é a fase mais sensível da informação, pois até estar pronta e acabada pode ainda não ter sido classificada e/ou protegida de acordo com o seu grau de sigilo.

2. Manuseio: Caracterizada pelo momento em que a informação é manipulada, pode ser durante a sua criação – acontecendo simultaneamente a essa fase – ou após a sua conclusão. Nessa fase deve-se controlar quem tem acesso.

3. Armazenamento: O próprio nome dessa fase é auto-explicativo. O armazenamento das informações pode ser feito de diversas formas: em computador, em um bloco de anotações, na memória humana e outros. Essa forma de armazenamento deve ser regulamentada.

4. Transporte: O transporte das informações, quando necessário, pode ser feito por meio eletrônico, por correio, mídias removíveis, fax ou por telefone. Nesse caso deve-se adotar o meio de transporte que seja mais adequando à classificação da informação transportada.

5. Descarte: Nessa fase tem-se a eliminação da informação ou, pelo menos, daquela cópia que está redundante, desatualizada ou que apresentou defeito no seu meio de armazenamento. O descarte pode ser físico (papel, pen-drive, CD) ou pode ser eletrônico ("deletando" um arquivo do computador). Essa é uma fase crítica da vida da informação, principalmente numa sociedade onde se costuma pensar que tudo que vai ao lixo não tem mais valor, e por esse motivo, não se têm os cuidados que deveriam ser tomados ao descartar uma informação considerada valiosa.

A segurança da informação deve estar presente em todas as fases do ciclo de vida das informações, da criação ao descarte, pois como diz o dito popular: "A resistência de uma corrente é medida pelo mais fraco de seus elos".

Vimos acima alguns conceitos básicos como informação, ameaça, vulnerabilidade, PSI, e o ciclo de vida das informações. Nas próximas partes, vamos procurar aprofundar tais tópicos e abordaremos mais alguns conceitos importantes para a Segurança das Informações.

Parte 2 - Ameaças e Vulnerabilidades que afetam as informações

Nesta parte do trabalho veremos as ameaças e vulnerabilidades que afetam os ativos de informação.

Antigamente, as vulnerabilidades relacionadas às informações estavam praticamente restritas a quantas chaves possuía o imenso arquivo metálico, ou seja, diziam respeito muito mais ao ambiente físico onde eram armazenadas. E as ameaças, por conseguinte, existiam em número quase inexpressivo, já que a informação não era valorizada como hoje, nem tão pouco disseminada como nos dias atuais.

Na era do conhecimento, essa realidade mudou. Essas ameaças e vulnerabilidades não são apenas externas, podem advir de dentro da própria empresa (por exemplo, por descuido dos funcionários, má utilização dos sistemas computacionais, entre outros) e por incrível que pareça, essas últimas são as mais perigosas e de difícil controle.

Assim, não nos custa nada estarmos atentos a alguns conceitos importantes dessa nossa era:

1. "HACKER": No seu sentido original (MITNICK, 2003) , significava uma pessoa que passava grande parte do tempo mexendo com hardware, seja para o desenvolvimento de programas mais eficientes ou para eliminar etapas desnecessárias. Hoje o termo se tornou pejorativo e abrangente, englobando todos os tipos de pessoas que detém um vasto conhecimento de informática e que usam esses conhecimentos para invadir e burlar sistemas de segurança com propósitos variados. Quando o propósito da pessoa é causar dano, o termo mais adequado é Cracker.

2. VÍRUS: São programas capazes de agregar-se a outros programas e arquivos, infectando-os, normalmente com más intenções. Dessa forma, quando o arquivo ou programa infectado é executado, dispara o vírus, a fim de causar modificações indevidas no processamento normal do sistema, podendo causar danos que podem ser leves ou irreparáveis.

3. CAVALO DE TRÓIA (TROJAN HORSE): Não são vírus, são programas que se instalam em computadores com intenções maliciosas; são utilizados para abrir portas no computador, possibilitando o ataque, remotamente. Vêm disfarçados em programas aparentemente inocentes, o que induz o usuário a executá-los.

4. FURTO E QUEBRA DE SENHA: Quando cadastramos nossas senhas em um PC, essa senha fica armazenada no servidor (ou no próprio PC) para que toda vez que ela for digitada possa ser comparada com o banco de dados. Esse banco de

dados, normalmente, é criptografado e escondido, mas, um invasor experiente sabe onde achá-lo. O arquivo de senha, depois de roubado de um servidor, é submetido à quebra da criptografia por uma ferramenta de crack. Assim são obtidas as senhas dos usuários que tiveram seu servidor invadido.

5. ENGENHARIA SOCIAL: A Engenharia Social ou Arte da Trapaça (MITNICK, 2003) pode ser empregada dentro ou fora do ambiente computacional. É a arte de persuadir. Para tal, é preciso entrar em contato com alguém, através de algum meio de comunicação (físico ou eletrônico) para que se possa dar início ao processo. Para chegar até seu objetivo, o atacante vai se deparar com várias dificuldades e é exatamente através da Engenharia Social que ele vai contornar essas barreiras.

6. VAZAMENTO DE INFORMAÇÃO: Além de vazarem de dentro da empresa, sem que sejam percebidas e/ou contidas, elas também podem vazar remotamente, de dentro dos ambientes computacionais, através da resposta à consulta de Ping, Traceroute, Telnet, SNMP, etc. As coletas de informação relativas à versão de sistema operacional e hosts dão ao invasor, informações que lhe permitirá planejar o ataque à rede (SCUA, 2004) . Outra forma de vazamento de informação se dá através da venda, troca ou furto de equipamentos onde os dados contidos nos HDs não estavam criptografados ou não foram apagados corretamente.

7. BACKDOOR E BUG: Após um ataque bem sucedido a um PC, o atacante normalmente procura deixar uma forma de retorno mais fácil, uma backdoor (porta dos fundos), para poder voltar, sem ter as mesmas dificuldades e para correr menos riscos de ser descoberto. Os bugs são defeitos em software ou protocolos e são explorados com a finalidade de criar raízes em uma máquina e, a partir daí, poder fazer tudo.

8. MAIL BOMB: Consiste em mandar uma série de mensagens (e-mails) para uma caixa postal. O objetivo do atacante é apenas enviar lixo para a caixa postal de alguém para congestionar a via de acesso individual ou corporativa à Internet, levando, por vezes, o servidor de e-mails a um colapso, com consequente negação de serviço. Existem diversos programas que automatizam o mail bombing.

9. SPOOFING: O IP Spoofing ficou famoso após ter sido utilizado para atacar a rede de Tsutomu Shimomura, um dos maiores especialistas de segurança dos Estados Unidos, quando através dele, na noite de Natal de 1994, o então mais famoso e procurado hacker americano, Kevin Mitnick, invadiu sua rede particular e roubou alguns dos seus programas. Esse ataque se baseia em disfarce entre computadores, para conseguir informações ou passar informações, fazendo-se passar por outro computador.

10. SCANNER DE PORTAS: São programas criados para encontrar portas TCP abertas em um computador; essas portas possibilitam ao atacante invadir o computador.

11. SMURF: É outro tipo de ataque de negação de serviço. O agressor envia solicitações Ping (um teste para verificar se um serviço da Internet esta acessível) para um endereço de broadcast. Usando spoofing, o atacante faz com que o servidor de broadcast encaminhe as respostas não para o endereço dele, mas para o da vítima. Assim o computador da vítima é inundado pelo Ping, podendo ficar inoperante.

12. SNIFFING: Quando se têm computadores interligados em rede, esses compartilham canais de comunicação, obviamente por ser muito mais barato - do que passar um cabo para cada par de computadores - e usar um switch (hub) pra controlar (comutar) as conexões. Nesses canais compartilhados, computadores podem receber informações enviadas a outros computadores. A ação de capturar informações destinadas à outra máquina é chamada sniffing (SCUA, 2004).

13. MAN IN THE MIDDLE (HOMEM NO MEIO): É aquele que envolve a conversação completa entre o atacado e o seu destino, pelo atacante. Este termo refere-se a qualquer ataque em que o atacante faz a comunicação mascarando-se como se fosse o destino pretendido pelo atacado. Muito usado para descobrir senhas de banco, quando o usuário pensa que está acessando o site do seu banco.

14. DENIAL OF SERVICE (DOS ou DDOS): Consiste em sobrecarregar, a partir de um computador ou de vários, um servidor com uma quantidade excessiva de solicitações de serviços (processamento de dados), impossibilitando o atendimento a outros PCs, ou gerar um grande tráfego de dados ocupando toda a banda disponível, não possibilitando o acesso a nenhum outro PC.

15. SPAM E HOAX: Spam é o termo usado para se referir aos e-mails não solicitados que chegam a nossas caixas de e-mails, geralmente enviadas para um grande número de pessoas. Os Hoaxs (boatos), apesar de na maioria das vezes serem inofensivos, podem comprometer a reputação e credibilidade de uma pessoa ou empresa por estar repassando uma informação, que na verdade, não passa de uma mentira.

Atentos a esses conceitos podemos identificar alguns dos principais riscos a que as informações estão expostas, por exemplo: o furto de backups de programas e de dados; a invasão de privacidade em e-mails e programas de mensagem instantânea; propagação de vírus por meio de programas de distribuição de arquivos (ex. Morpheus e Kaaza); ataques de engenharia social; atos de vandalismo; sabotagem; terrorismo digital; espionagem através de compartilhamento de máquinas e diretórios; inter-

ceptação não autorizada da comunicação telefônica e telemática; etc.

Tais práticas podem trazer prejuízos irreversíveis para a companhia e, a fim de reduzir a incidência destas, podemos realizar um processo de Análise de Riscos e estruturar uma eficiente Política de Segurança de Informações, como mencionamos na Parte I deste artigo.

Na Parte III, estudaremos ferramentas e meios de prover segurança às informações. Em nossa última Parte, traçaremos um pequeno roteiro de como elaborar uma Política de Segurança de Informações.

Parte 3 - Ferramentas e meios de prover segurança às informações

Dando sequência ao tema, após explicitarmos o ciclo de vida das informações e as principais ameaças e vulnerabilidades a que estão expostos nossos ativos de informação, veremos agora as melhores práticas e as ferramentas mais usadas e disponíveis no mercado, para proteger nossas informações e o nosso conhecimento acumulado, dentro e fora dos ambientes computacionais.

Lembramos que o objetivo não é esgotar o assunto e nem explorar profundamente os conceitos aqui levantados. Pretendemos sim, dar uma visão abrangente do universo da segurança de informações, suas principais ferramentas, perigos e as melhores práticas aplicadas no mercado.

Iniciaremos, então, pelo famoso Firewall, que é uma ferramenta constituída pela combinação de software e hardware com a finalidade de isolar, controlar e proteger o acesso entre redes e/ou computadores. O funcionamento de um Firewall parte da análise de conteúdo do que está tentando passar por ele. Esse conteúdo é analisado constantemente, tendo como referência as configurações feitas. Tais configurações dizem exatamente o que pode entrar e o que pode sair. Lembramos que um Firewall não faz o papel do antivírus, devendo trabalhar em conjunto com este.

Lembramos, porém, que a implementação em sua rede não é garantia 100% de segurança. Além de não ser infalível, existe a possibilidade de a invasão partir de dentro da rede, nesse caso, por trás do Firewall.

O IDS – Intrusion Detection System é uma ferramenta utilizada para detectar e alertar sobre tentativas de acesso não autorizadas, atividades incorretas, maliciosas, anômalas, no seu PC ou rede corporativa. Não é uma ferramenta desenvolvida para reagir; essa iniciativa deve ser do usuário, alguém tem que monitorar o IDS e reagir à invasão.

O Antivírus é um programa desenvolvido para identificar, anular e/ou remover os vírus de computador. Os antivírus mais modernos estão trazendo outros recursos agregados como detecção de Cavalo de Tróia, programas hostis e outros. O antivírus faz a identificação dos vírus através da comparação dos pacotes analisados com o banco de dados das assinaturas dos vírus conhecidos. Em função de aparecerem mais de 10 novos vírus por dia, é de fundamental importância a atualização diária dos antivírus, e mesmo assim, não teremos garantia 100% de que um vírus recém criado nos encontre.

Os Scanners de Vulnerabilidades são softwares que varrem as portas utilizadas pelo protocolo TCP/IP, com o objetivo de detectar vulnerabilidades. Várias informações podem ser obtidas, como por exemplo, os serviços que estão sendo utilizados, os usuários que consomem estes serviços, a possibilidade de conexão por usuários anônimos, a possibilidade de conexão por usuários sem autenticação e outras.

A Virtual Private Network (VPN) ou Rede Privada Virtual é um ambiente de comunicação com acesso controlado, ou também podemos definir como uma rede privada construída dentro da infra-estrutura de uma rede pública, como a Internet, utilizando recursos de Autenticação, Criptografia e Tunelamento. Essa estrutura visa garantir a integridade, a segurança e a confidencialidade dos dados trafegados e interligar redes e/ou computadores independentes. A VPN provê conexão segura através de três serviços conjuntos (RABENER, 2001 apud PELISSARI, 2002, P. 34) , vejamos:

1. Autenticação através da identificação do remetente e do receptor;

2. Criptografia;

3. Enclausuramento ou Tunelamento.

Os principais objetivos na Implantação de uma VPN, são:

- Disponibilizar acesso e comunicação seguros por meio de redes públicas (Internet) a baixo custo;
- Isolar uma rede distribuída contra interferência externa;
- Proteger a privacidade e a integridade de mensagens atravessando redes não confiáveis (públicas).

O Controle de Acesso aos Meios Computacionais é um mecanismo que proíbe o acesso de pessoas ou máquinas, sem autorização, a um determinado ambiente ou recurso do sistema. Podemos compará-los, aos sistemas bancários, da seguinte forma: Para que alguém entre em um cofre de banco é necessário que ela se identifique (Ex.: RG, senha numérica e biometria).

Após ter passado pela identificação positiva, deve existir um controle que diga o que essa pessoa pode e o que ela não pode fazer lá dentro. Outras características como: horário de entrada, quanto tempo pode permanecer e outros procedimentos podem ser incluídos.

O sistema de informação de uma empresa é o seu cofre mais valioso, portanto, devem existir meios de controlar o acesso a esse ambiente. Para uma pessoa entrar nesse ambiente ela precisa se identificar e autenticar sua identidade. Após a confirmação e aceitação do usuário, pelo sistema, é necessário que estejam definidos os limites do que pode ser feito por esse usuário e que informações estão disponíveis para ele.

Por sua vez, o objetivo principal da Criptografia, que também pode ser usado como recurso para prover segurança, é garantir que uma informação só seja lida e compreendida pelo destinatário da mesma. Dessa forma, teremos os seguintes benefícios com o uso da Criptografia:

- Confidencialidade: Ter certeza que apenas as pessoas autorizadas irão ter acesso à informação;
- Integridade: Ter certeza que a informação não foi modificada durante seu envio, ou seja, chegou ao destinatário do jeito que saiu do remetente;
- Autenticação: Quem enviou e quem recebeu têm a confirmação da identidade um do outro, bem como da origem e do destino da mensagem.

A Assinatura Digital é utilizada para autenticar uma mensagem enviada por meio eletrônico, através dela o destinatário poderá se certificar de que o remetente é realmente quem diz ser.

A Esteganografia é um ramo particular da criptologia que consiste em camuflar a mensagem, mascarando a sua presença. Já a criptografia torna a mensagem ininteligível, escondendo a informação da mensagem. Contrariamente à criptografia, que cifra as mensagens de modo a torná-las incompreensíveis, a esteganografia esconde as mensagens em arquivos de imagens, textos ou até mesmo áudio, que servem apenas de suporte para esconder a mensagem. Uma importante aplicação moderna da esteganografia digital é como "marca d'água". Uma gravação de vídeo de um sistema de segurança (DVR) que use esse recurso, caso seja adulterado, irá alterar essa marca, sinalizando a manipulação da imagem ou que ela não é original.

Demilitaryzed Zone ou DMZ, segundo Scua (2004) , é uma estratégia utilizada para enganar e detectar intrusos, em que alguns equipamentos são posicionados propositalmente sem proteção, ou seja, na frente do Firewall. Esses equipamentos são isolados da rede interna e monitoram tentativas de ataques. Este método traz diversos benefícios importantes:

1. Três níveis de segurança separam a Internet do meio interno;
2. Somente a sub-rede DMZ é conhecida na Internet, de modo que não há meio de se conhecerem rotas de acesso à rede interna;
3. Da mesma forma, somente a sub-rede DMZ é conhecida para a rede interna e não existem rotas diretas para o acesso à Internet.

O Backup é um elemento fundamental na recuperação dos dados e na retomada do processamento das informações, e muitas vezes das atividades normais da empresa. Para garantir que esse recurso esteja disponível quando necessário é recomendado que seja criada uma Rotina de Backup. Essa rotina vai determinar entre outras coisas:

- Qual a periodicidade dos backups da empresa;
- Quem é o responsável em fazê-los;
- Onde vai ser armazenada essa cópia;
- O que deve ser feito com as cópias ultrapassadas;
- Qual a periodicidade de teste dos backups.

Os backups devem ser armazenados em local externo à organização, em cofre antichamas. Deve ser mantida, ainda, uma cópia do backup atual no CPD, em cofre apropriado, para a rápida recuperação dos dados.

Compreendidas as principais ameaças e vulnerabilidades e vislumbrados alguns riscos e ferramentas de proteção dos nossos recursos de informação, iremos, então, na última parte desse artigo, sugerir alguns passos para a criação e implantação de uma Política de Segurança de Informações.

Parte 4 - 10 etapas para a elaboração de uma Política de Segurança de Informações

Nesta última Parte, após termos abordamos o ciclo de vida das informações, suas principais vulnerabilidades, ameaças e as ferramentas utilizadas na proteção dos ativos de informação, resta-nos elencar as 10 principais etapas para a elaboração de uma Política de Segurança de Informações.

Algumas empresas, implementando mecanismos de segurança de forma isolada, como por exemplo, um antivírus e/ou um firewall, acreditam ter seus ativos de informação protegidos. Na realidade, tais ferramentas servem para a proteção dos sistemas de informação (TI). Não devemos confundir proteção de computadores e de redes com a proteção de informações e do conhecimento. Estes não estão obrigatoriamente dentro dos meios computacionais. Desta forma, para atingirmos uma proteção abrangente e eficaz, necessário se faz elaborar uma Política de Segurança de Informações (PSI).

Lembramos que não existe uma "receita" pronta para ser aplicada em todos os casos. O que veremos abaixo, não passa de uma sugestão composta de 10 etapas genéricas para a elaboração de uma PSI.

Seguem:

1. Escolha da equipe responsável pela implantação e manutenção da segurança: O primeiro passo para o desenvolvimento de uma Política de Segurança de Informações é escolher a equipe responsável por sua criação, elaboração, implantação e manutenção. Frise-se que envolver pessoas da alta direção da empresa é de suma importância. Delimita-se, neste momento, o dever e as responsabilidades de cada componente da equipe.

2. Análise dos processos e procedimentos executados na empresa: Nessa etapa, devem ser identificados os processos e procedimentos existentes na organização, que tenham relevância e ligação com a segurança de informações. Todos os processos, informatizados ou não, podem afetar, direta ou indiretamente, os ativos de informação; assim, todos devem fazer parte da PSI.

3. Classificação das Informações: Tem como objetivo assegurar que as informações recebam a devida atenção dentro da PSI. As informações devem ser classificadas segundo sua sensibilidade, prioridade, criticidade, acessibilidade, entre outros critérios. Depois de classificá-las, elege-se qual o melhor procedimento a ser adotado. Tais procedimentos precisam levar em consideração a informação na forma física e eletrônica.

4. Elaboração de normas e procedimentos: Nesta etapa, a equipe entra em consenso, elabora normas e procedimentos que devem ser seguidos por todos na organização. Recomenda-se que as normas e procedimentos contenham o maior número de comandos possível, e que enfatize os seguintes pontos: acessos externos; acessos internos; uso da Intranet; uso da Internet; uso de correio eletrônico; política de uso e instalação de softwares; política de senhas; política de backup; uso e atualização de antivírus; acesso físico; acesso lógico; trilhas de auditoria; padrões de configuração de rede, entre outros.

5. Definição de um plano de recuperação e continuidade dos negócios e um plano de contingência: São planos que contêm as diretrizes que a empresa deve seguir em caso de parada de um ou mais processos, decorrente de um desastre ou perda inesperada. Tem como objetivo, auxiliar na recuperação imediata dos processos que dependem das informações, levando em consideração a criticidade, a importância e o impacto, fazendo com que eventuais perdas e prejuízos à organização sejam minimizados.

6. Definição de sanções ou penalidades pelo não cumprimento da PSI: São definidas as punições aplicadas pelo não cumprimento da PSI. Estas sanções balizam-se na cultura e política da organização, sempre respeitando as leis e convenções. O principal objetivo de se estabelecer sanções é incentivar o cumprimento voluntário da PSI.

7. Elaboração de Termo de Sigilo e Confidencialidade: Algumas informações, por sua importância ou valor intrínseco, devem ser conhecidas por poucas pessoas ou mesmo permanecer em sigilo absoluto. A fim de protegê-las, elabora-se um Termo de Sigilo e Confidencialidade, no qual são reforçados os principais pontos da PSI. O termo deve ser parte integrante do contrato de trabalho, especificando a responsabilidade de quem o assina em caso de descumprimento.

8. Comunicado formal da diretoria ou presidência: A diretoria ou presidência deve comunicar formalmente aos colaboradores, usuários e membros da equipe a implantação da PSI. Deve, também, demonstrar-se engajada na política e, através do exemplo de comprometimento, conquistar seus seguidores.

9. Divulgação da Política: Um dos maiores desafios da PSI é conseguir a aderência voluntária dos funcionários. O descumprimento generalizado da PSI pode decorrer da falta de divulgação. Assim, recomenda-se que junto com a PSI seja estruturado um bom planejamento de marketing interno, deixando, dessa forma, sempre vivo o ideal almejado. Os métodos de divulgação da Política variam de acordo com a empresa; a seguir, listamos alguns dos métodos de divulgação mais utilizados: campanhas internas de conscientização; palestras de conscientização; destaque em jornal e folhetos internos; destaque na Intranet da organização; criação de manual em formato compacto e com linguagem acessível aos usuários; disponibilização na Intranet ou na rede, em local comum a todos, a PSI, na íntegra.

10. Implantação e Revisão: A implantação é a etapa final da PSI e consiste na aplicação formal das regras descritas na política e a assinatura do termo de compromisso. Deve ser realizada de forma gradativa e, obrigatoriamente, após o programa de divulgação, capacitação e conscientização dos funcionários. Lembrando que a revisão, além de ocorrer antes da fase de implantação, deve ser cíclica e periódica, para manter a PSI sempre atualizada diante das novas tendências e acontecimentos do mundo moderno.

Imaginando ser a Política de Segurança de Informações uma corrente, seu elo mais fraco pode ser o usuário. Assim, este merece atenção dobrada, ou seja, deve ser bem capacitado, treinado, motivado a colaborar com a PSI.

Finalizando nosso trabalho, agradecemos o interesse, a atenção e convidamos o leitor a aprofundar o assunto, seja pela Internet, seja pela vasta literatura escrita existente, vez que neste espaço, procuramos apenas colocar o tema em pauta, alertar riscos e esboçar soluções, sem maiores pretensões.

"NÃO ASSUMIR RISCOS É O MAIOR RISCO QUE EXISTE"
Jawaharlal Nehru

Parte 5 – Bibliografia Sugerida

Autor	Título	Editora
Barros Jr., Jairo Moreno de	Universidade Espionagem Digital	Digerati
Beal, Adriana	Segurança da Informação	Atlas
Beal, Adriana	Gestão estratégica da informação	
Brasiliano, Antonio C. Ribeiro	A (in) Segurança nas redes empresariais	Sicurezza
Burnett, Steve	Criptografia e segurança	Campus
Campos, André L.	Sistema de Segurança da Informação - Controlando os Riscos	Visual Books
Caruso, Carlos A. A.	Guia Básico para Projetos de Segurança Lógica de Dados	Ibcb
Caruso/Steffen	Segurança em Informática e de Informações	Senac
Dawel, George	A Segurança da Informação nas Empresas	Ciência Moderna
Dias, Cláudia	Segurança e Auditoria da Tecnologia da Informação	Axcel Books
Ferreira, Fernando Nicolau Freitas	Segurança da informação	Ciência Moderna
Fontes, Edison	Vivendo a Segurança da Informação	Sicurezza
Fontes, Edison Luiz Gonçalves	Segurança da Informação	Saraiva
Furtado, Vasco	Tecnologia e Gestão da Informação na Segurança	Garamond
Garfinkel, Simson E Spafford, Gene	Comercio e Segurança na Web	Market Books
Gomes, Elisabeth; Satrec, Cláudio	Gestão estratégica da informação e inteligência competitiva	Saraiva
Horton, Mike; Mugge, Clinton	Hack Notes: segurança de redes	Campus
Martins, José Carlos Cordeiro	Gestão de Projetos de Segurança da Informação	Brasport
Mccarthy, Mary Pat E Campbell, Stuart	Transformação na Segurança Eletrônica	Makron
Menezes, Josué das Chagas	Gestão da Segurança da Informação	J.h. Mizuno
Mitnick, Kevin D. e Simon, William L.	A Arte de Enganar	Pearson Education do Brasil
Paladini, Alexandre Negrão	Você está seguro na Internet?	Simetria
Peixoto, Mário César Pintaudi	Engenharia Social e Segurança da Informação na Gestão Corporativa	Brasport
Plantullo, Vicente Lentini	Estelionato eletrônico: segurança na internet	Juruá
Sêmola, Marcos	Gestão da Segurança da Informação	Campus
Shema, Mike	Hack Notes: segurança na web	Campus
Volpi Neto, Ângelo	Comercio Eletrônico – Direito e Segurança	Juruá

Tácito Augusto Silva Leite, ASE, DSE

MBA em Sistemas de Informação, com ênfase em Segurança de Informações pela Universidade Potiguar – UnP (2004); MBA em Gestão de Segurança Empresarial pela Universidade Anhembi-Morumbi (2005); Pós-Graduação em Segurança Empresarial pela Universidade Pontifícia Comillas de Madrid (2006/2008); Graduação em História - Licenciatura e Bacharelado pela Universidade Federal do Rio Grande do Norte (2000). Certificado DSE (Diretor de Segurança Empresarial) pela Universidade Pontifícia Comillas de Madrid e Certificado ASE (Analista de Segurança Empresarial) pela Associação Brasileira dos Profissionais de Segurança - ABSEG. Possui experiência na área de Gestão Empresarial, com ênfase em Gestão de Empresas de Segurança, Gestão de Riscos Corporativos e Prevenção de Perdas. Diretor da Associação Brasileira dos Profissionais de Segurança - ABSEG e Articulista do Jornal da Segurança - JSEG e Revista SESVESP. Trabalha na área de segurança desde 1994, sempre com foco em gestão estratégica, análise de processos e projetos.

Uma "Nova" Acepção do Termo Inteligência Aplicada ao Ambiente Empresarial

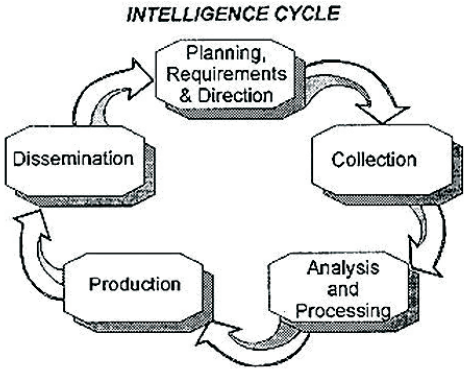
Vinícius Domingues Cavalcante

UMA BREVE INTRODUÇÃO À ATIVIDADE DE INTELIGÊNCIA

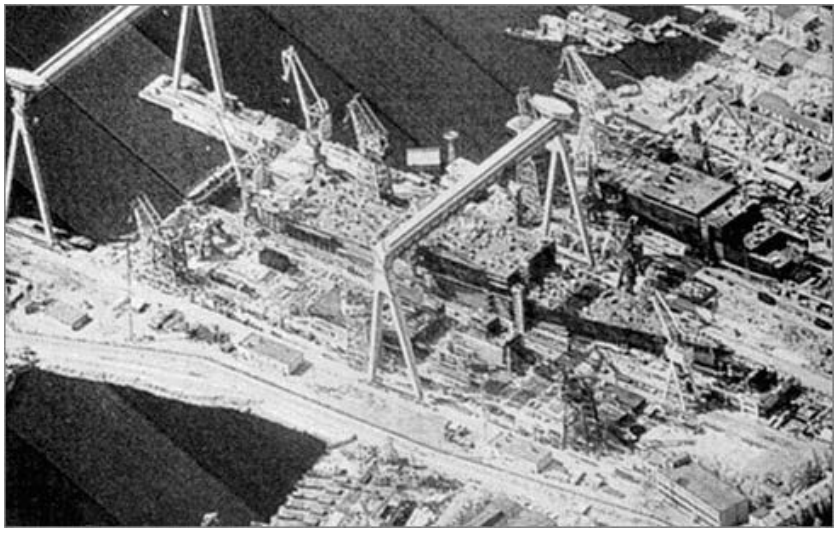
Em qualquer campo da atividade humana haverá sempre uma constante, ou seja, a busca de dados, de elementos, de conhecimentos, em última análise, de informações, a fim de instruir decisões, auxiliar na elaboração de planos e na execução de ações.

Nenhum administrador ou chefe se empenha em projetos, planejamentos, opta por investimentos ou toma decisões sem que haja manipulado e refletido acerca de uma enorme quantidade de dados, detalhes, informações e estudos. Hoje em dia, modernos tratados acadêmicos de administração e marketing enfatizam as informações de que devem estar munidos os profissionais, a fim de poderem manipular, com certo grau de acerto, os problemas de sua instituição ou empresa. A necessidade de dispor de informações faz parte do dia a dia de homens de negócio, administradores e políticos, pois não é possível, hoje, conduzir uma administração modesta, uma empresa ou órgão público, um município, estado ou país, sem que haja um fluxo constante e ordenado de informações de toda a natureza, das mais simples às mais complexas, permitindo um perfeito conhecimento do que se passa ou do que, possível ou provavelmente, virá a suceder no futuro.

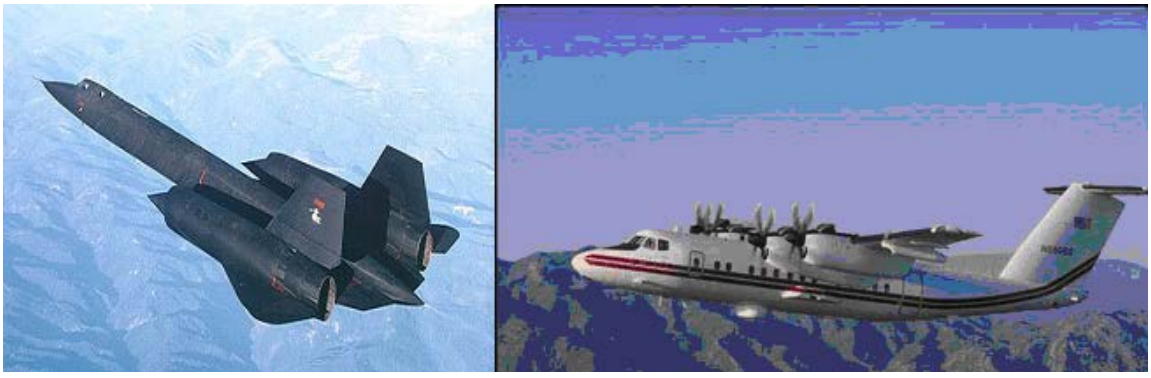
Em se tratando da dependência de informações, não seria demais comparar a direção de uma empresa com a alta administração de uma nação, onde, em relação àquela, obviamente os problemas por solucionar são de alcance bastante mais amplo, mais complexos, envolvendo áreas de atrito e interesses que, se não forem do conhecimento dos seus dirigentes, poderão trazer grandes dificuldades nas áreas interna e externa. Todos os governos, quaisquer que sejam seus matizes ideológicos, necessitam de informações que lhes propiciem, além de segurança física, melhores condições para implementar seus processos decisórios.



Os Estados têm constante necessidade de conhecimentos. Alguns podem ser acessados livremente em enciclopédias, em anuários estatísticos, nas redes de computadores, na livre imprensa, mas outra preciosa gama se compõe de dados confidenciais, sigilosos, os quais são, por natureza, de difícil obtenção. Para a formulação e condução de suas políticas nacionais, os governos precisam saber o que se passa com os demais países, suas ambições, perfis psicológicos, histórico-bibliográfico e mesmo detalhes reservados da vida dos membros da classe política e empresariado, informações sobre a economia, recursos naturais, pesquisa e desenvolvimento tecnológico, extensão do poderio militar, quais os grupos (dentro e fora do país) lhe são simpáticos ou antagônicos, todo um conjunto de informações, importantes em algum momento do processo decisório, que não se encontram disponíveis com facilidade.



A construção do primeiro porta-aviões da antiga União Soviética, em meados dos anos 80 é acompanhada através de fotografias do satélite espião KH-11, tiradas a mais de 500 km de altura. Ressalve-se que a nitidez da imagem certamente foi degradada antes de sua "liberação" pelos americanos, os quais hoje dispõem de meios de coleta fotográfica muito mais espetaculares.



Aviões espiões militares, de grande altitude, são dotados de sensores capazes de coletar imagens, bem como sinais oriundos de equipamentos de radar, radiocomunicação, telefonia etc. Alguns aviões espiões operam descaracterizados, sob matrículas civis.

Para auxiliar na busca e na análise das informações confidenciais de que necessitam, as nações criaram seus serviços secretos ou agências de inteligência. Os serviços de inteligência lançam mão de todos os expedientes ao seu alcance, a fim de coletar ou mesmo subtrair informações sigilosas de seus detentores, sendo a espionagem um recurso bastante utilizado.

Ao mesmo tempo em que se dedicam à coleta dos segredos alheios, os órgãos de inteligência também tem por função detectar e coibir a insidiosa ação da espionagem adversária, negando-lhes o acesso às informações ou segredos que buscam obter e prevenindo as ações de sabotagem. Trata-se de um componente imprescindível da Inteligência, garantindo a segurança em face das ações inimigas. A essa atividade denomina-se "contra-espionagem" e se constitui num ramo bastante especializado e extremamente necessário do universo da Inteligência.

Um bom serviço secreto elabora pesquisas, analisa possibilidades e probabilidades, estima tendências, deduz intenções, adverte os dirigentes sobre a iminência de riscos em face dos indícios coletados. A partir da coleta de informações fragmentárias e/ou em estado bruto (também chamadas de informes), os serviços de inteligência compõem um grande mosaico, encaixando os dados uns aos outros, permitindo-se avaliar e até antever situações com razoável grau de precisão. Os órgãos de inteligência crescem e se sofisticam em razão da importância que o produto de seu trabalho assume para o governo do país e assim se justifica a existência de um verdadeiro "exército" de especialistas (os "analistas"), cuja função é avaliar, relacionar e interpretar todos os dados possíveis, concernentes aos países e governos estrangeiros, à economia, à defesa e à segurança nacional. Dando suporte a um governo que atinge seus objetivos através da otimização de seus recursos, certamente estará um eficiente serviço de inteligência, ainda que uma expressiva parcela da população nacional jamais venha a se dar conta de tal fato, ou de sua crucial importância. Embora alguns historiadores acadêmicos possam torcer o nariz diante dessa afirmação, não seria

equivocado admitir que muito da história recente da humanidade é diariamente "escrita" nos bastidores, pelos ditos "serviços secretos". Os "porquês" de importantes decisões da História e muitos acontecimentos marcantes foram decididamente influenciados pelo aconselhamento (ou mesmo pela participação direta) dos órgãos de inteligência.

As ações de um serviço secreto nem sempre se atém às normas da ética, da honestidade e da humanidade. Na condução de seus processos, a guisa de alcançar os objetivos que se identificariam com os mais legítimos ideais da nação, não faltam exemplos de roubo, furto, trapaças, traições, mentiras, chantagens, campanhas de difamação, sabotagens, sequestros e até assassinatos. No exército alemão de outrora era voz corrente que os serviços secretos não eram exatamente "ofício apropriado para cavalheiros".

A esta altura do texto, o leitor pode estar se perguntando qual a relação que existe entre a estrutura e as ações dos serviços de inteligência (espionagem e contra-espionagem), daqueles que inspiram autores como John Le Carré, Frederick Forsyth e Tom Clancy e a atividade de inteligência aplicada ao âmbito empresarial?

Assim como a espionagem diplomática, político-econômica e militar estendeu seus métodos e seus recursos tecnológicos a outros tipos de espiões, a ideia de um serviço de inteligência como fator essencial no processo de tomada de decisões também encontra ampla aplicação no contexto empresarial.

Elementos contratados por governos ou empresas concorrentes buscam através dos mais diversos ardis, obter segredos industriais ou informações privilegiadas que possibilitem colocar determinada companhia numa posição destacada no mercado. Furtos de plantas, fotografias clandestinas, roubos de protótipos... Empresas de renome perdem, anualmente, milhões com o "vazamento" de informações sigilosas, por meio de espionagem comercial/industrial. Através da interceptação das comunicações de uma diretoria ou da presidência de uma empresa, os concorrentes pretendem saber qual é o passo mais acertado a dar, em meio a uma disputa comercial, ou buscam, com o "grampeamento" dos ambientes e telefones, obter informações para chantagens ou desmoralizações.

Criminosos buscam dados para o planejamento de ações de roubo, furto e sequestro. São incomensuráveis os prejuízos que as informações obtidas de maneira subreptícia podem ocasionar às pessoas ou às instituições privadas e públicas. Infelizmente, no Brasil, não há estatísticas confiáveis sobre o roubo de informações sigilosas e sabotagens no meio empresarial, bem como dos prejuízos ocasionados por tais práticas. Não faltam histórias de escutas clandestinas, fotografias misteriosas e arrombamentos em gabinetes ou salas, de onde, "ao menos aparentemente", nada teria sido subtraído. A espionagem - em suas mais diversas formas - é uma realidade que só pode ser eficazmente enfrentada com ações de inteligência!

A prevenção às ações de sabotagem (e de terrorismo), a segurança física das instalações empresariais (e a prevenção aos roubos, furtos e perdas), a segurança das comunicações, das redes de computadores, bem como a segurança dos altos executivos são extremamente dependentes de informações, que são obtidas por meio de atividades de inteligência. Desde a avaliação de erros e vulnerabilidades até a própria coleta e análise de informações potencialmente significativas para o planejamento e a condução dos negócios. A inteligência se aplica "como uma luva" às necessidades do empresariado, sendo clássicos os exemplos de grandes conglomerados como a Krupp (alemã), a Vickers (britânica), a Du Pont e a Remington (americanas) e a Schneider (francesa) que, desde o início do século, já contavam com autênticas "centrais de inteligência" trabalhando em seu proveito.

A INTELIGÊNCIA NA EMPRESA

A crescente competitividade entre as empresas torna a atividade de inteligência - como produtora de conhecimento e previsão - crítica para a tomada das decisões no âmbito empresarial. Embora as informações e produtos da atividade de inteligência sejam objeto de trabalho das Diretorias e Gerências empresariais, ambas, normalmente, não estão familiarizadas com as técnicas, os processos e os equipamentos dos serviços de inteligência. A simples existência de empresas que se destinam à pesquisa, catalogação e o fornecimento de grandes quantidades de dados (todos relacionados a um campo específico de interesse e sob os mais variados critérios de escolha) não eliminam a necessidade de contar com profissionais habilitados para efetuar a aquisição de informações verdadeiramente precisas e essenciais, analisá-las, reservadamente, à luz dos interesses da empresa e encaminhar relatórios, aconselhando a adoção de medidas, fazendo projeções ou estimativas para os usuários daquele conhecimento útil, o qual se constitui o produto final. Embora sejam, hoje, notórios os casos de agências noticiosas que se anteciparam aos serviços nacionais de inteligência, na informação de diversos governantes, no mundo dos negócios, os empresários não podem esperar pelos indicadores publicados nos jornais, pelo BLOOMBERG, CBS-News ou pela CNN, a fim de dirigir seus negócios, até pelo fato de que muitas das informações de que podem necessitar simplesmente não estão disponíveis nessas fontes. No mundo globalizado de hoje, quando se considera que a "informação" é muitas vezes o bem mais precioso da empresa, a coleta e a análise de informações vem se tornando muito mais necessária aos centros decisórios do

setor privado. Apenas considerando àquelas com propósitos civis e comerciais, podemos constatar que as mesmas excedem em muito o volume dos dados manipulados pelas agências de inteligência governamentais da maioria das nações da Terra. A "Inteligência Empresarial" é uma ferramenta indispensável à realização das metas de uma empresa e, uma vez que os meios e processos para alcançar tais objetivos devam ser mantidos em segredo para os concorrentes, compreendemos que estamos diante de uma atividade que, ao menos em princípio, não deveria ser terceirizada.

Não se discute a necessidade de um profissional com a responsabilidade de assessorar a empresa em técnicas e métodos para uma tomada de decisões inteligente, assegurando sua competitividade no mercado, ao mesmo tempo em que a salvaguarda de todo um leque de ações adversas. O fato é que existe formação específica para o profissional de inteligência na esfera privada. Logo, além da honestidade, boa reputação, educação acadêmica formal e a ampla vivência no ramo de atividade negocial da empresa, seria recomendável deter uma "razoável bagagem" de conhecimentos sobre História, Lógica, Relações Humanas aplicadas, Direito, Espionagem e Contra-espionagem (abrangendo as ações, seus modus operandi e equipamentos utilizados), Investigações e Perícia Criminal, Segurança Física, técnicas e equipamentos de Vigilância e contra-vigilância, Sensoriamento e Alarmes, Informática e Segurança de Redes etc. Em função de sua necessidade e ampla aplicação no meio empresarial, acredito que seria bastante apreciada a criação de uma disciplina acadêmica voltada para ministrar o conceito enunciado de inteligência, no âmbito dos cursos superiores de Administração.

Em 1949, Lorde Louis Mountbatten, então no comando da frota britânica no Mediterrâneo, ao realizar manobras navais em que sua esquadra se opunha à esquadra metropolitana, infiltrou um telegrafista no Quartel-General rival em Gibraltar, o qual lhe radiografava os movimentos da "força adversária". Quando questionado sobre a atitude considerada desleal e anti-britânica, ele defendeu-se, comentando que: "Não se pode esperar que o inimigo jogue sempre obedecendo às regras de Queensberry!" (as regras do Marquês de Queensberry, que norteiam as lutas de boxe). Nos dias de hoje, quando a competição entre as empresas tornou-se global, concorrências comerciais são encaradas como verdadeiras guerras, em que os contendores não costumam muito se preocupar com as "regras".

Elementos egressos dos organismos de inteligência militar ou serviços secretos podem ter excelente emprego na Inteligência Empresarial. Com o fim da bipolaridade e a consequente redução dos orçamentos de defesa, inúmeros profissionais de inteligência, de ambos os blocos, migraram para a iniciativa privada, onde se empregam como especialistas em segurança ou prestam consultoria na área de inteligência. O fim da perspectiva de conflito entre o Ocidente e a antiga URSS não transformou o mundo num lugar mais seguro para as empresas: a competitividade desleal, as máfias, o banditismo e o terrorismo ainda vão, por muito tempo, requerer profissionais capazes de analisar as ameaças e aconselhar os empresários sobre os procedimentos mais acertados. Os ex-especialistas governamentais podem analisar dados que escapariam a um administrador típico e formular um conceito baseado nos fatos e nas suas experiências passadas, as quais certamente envolvem informações obtidas de fontes clandestinas e secretas. A inteligência empresarial tende a lucrar com a formação e a experiência dos profissionais oriundos dos serviços secretos, mas há de se estabelecer, na iniciativa privada, uma conduta mais ética e de observância aos ditames da lei. Já que na inteligência privada não se poderá contar com os recursos e as garantias proporcionadas (ou justificadas) pela soberania e o interesse nacional, o nome e a imagem de uma empresa devem ser prioritariamente preservados e mantidos à margem das ações judiciais e dos noticiários negativos ou sensacionalistas.

Potências como os Estados Unidos da América, cuja posição hegemônica no cenário mundial se assenta no trabalho de uma enorme "comunidade" voltada para as atividades de inteligência, reconhecem a inadequação dos recursos à disposição da iniciativa privada para lidar com as questões de inteligência e espionagem, principalmente quando se considera que diversas das ameaças que pesam contra as empresas modernas (tanto as americanas como, por exemplo, as brasileiras) advêm de agências governamentais ("serviços secretos") estrangeiras e de pessoal altamente especializado (às vezes, até oriundos de tais serviços), trabalhando a soldo de grandes empresas concorrentes. Embora saibamos que inúmeras grandes empresas norte-americanas dispõem de eficazes departamentos inteiramente voltados ao exercício de atividades de inteligência (coleta/análise e proteção dos próprios segredos corporativos), na América, o governo federal instituiu uma agência especialmente voltada para desenvolver atividade de "contrainteligência" - a "National Counterintelligence Center" (NACIC). Trata-se de uma organização composta por especialistas do FBI, CIA, NSA, DIA, Departamento de Estado e Departamento da Defesa, voltada a coordenar, em nível nacional, as atividades de contrainteligência, ou seja, a salvaguarda ante as ações da inteligência adversária. Entre seus objetivos estão:

- Aprofundar o interrelacionamento com as empresas privadas, identificando conjuntamente as vulnerabilidades e necessidades de informação ou segurança das companhias;

- Auxiliar no desenvolvimento de programas de prevenção;

- Promover seminários e conferências;

- Compilar e disseminar informações sobre a atuação clandestina (de potências estrangeiras ou seus agentes) que atente contra a indústria americana, ou qualquer entidade do setor público ou privado, a qual tenha responsabilidade de proteger

informações sensíveis, classificadas, tecnologias e patentes.

A NACIC colabora com a "Inteligência Empresarial", apresentando para as empresas uma resenha atualizada de técnicas, métodos e equipamentos utilizados pelos países estrangeiros, inclusive um completo e elaborado histórico de ameaças contra as atividades empresariais em solo americano e no exterior.

Salvaguardando o sigilo necessário às suas próprias operações, os Estados Unidos, em momento algum, admite claramente a utilização de seu enorme aparato de inteligência para propósitos de espionagem econômica ou comercial. De qualquer forma, agências como a NSA detêm permissão legal para "certas atividades de vigilância eletrônica", coletando informações no estrangeiro, "em benefício dos interesses dos Estados Unidos". Embora os manuais de inteligência voltados ao meio corporativo (sobretudo os de "INTELIGÊNCIA COMPETITIVA") destaquem a necessidade de uma conduta legal e ética, é fato que empresas de toda parte continuam, discretamente, recorrendo aos mesmos recursos, reconhecidamente escusos, os quais julgam condenáveis quando empregados pelos concorrentes.

Nos Estados Unidos, em meados de 2003, um escândalo sacudiu a indústria de defesa, quando veio a público que gerentes da Boeing Company tinham conhecimento de que, por vários anos, seus empregados faziam uso de documentos ilegalmente subtraídos à concorrente Lockheed Martin, no esforço de superar a rival na competição pelos multimilionários contratos de lançamento de satélites do governo. No mais rumoroso escândalo de espionagem industrial doméstica, um engenheiro, ex-funcionário da Lockheed, entre 1997 e 2000, auxiliou na subtração de mais de 37.000 páginas de documentos que permitiram à Boeing ganhar U$1.9 bilhões de dólares em lançamentos de seus foguetes Delta-4. A posse de documentos da companhia rival constituiu-se em uma violação da lei americana, prevista no Procurement Integrity Act. A punição prevista para atos dessa natureza incluiria a rescisão dos atuais contratos e a exclusão de futuras concorrências do Departamento da Defesa; porém, impingir tal punição a uma empresa do porte da Boeing é problemático para os militares americanos, uma vez que a companhia produz desde caças até aeronaves de transporte, helicópteros, satélites e bombas guiadas por satélites, desenvolve integração de sistemas, fabrica foguetes etc.

As ameaças estrangeiras às informações econômicas e tecnológicas das companhias americanas também não advêm exclusivamente das nações consideradas ideológica ou militarmente adversárias; outros países, aliados de longa data, ou tradicionalmente neutros, também buscam apropriar-se de segredos econômicos ou técnicos, independentemente de suas relações amigáveis com os Estados Unidos. É sabido que em países como a França, Israel, Coreia do Sul, Taiwan e Rússia, os serviços secretos nacionais colaboram ativamente com a iniciativa privada, municiando-a com segredos econômicos e industriais coletados (ou subtraídos) de outros países, poupando milhões em pesquisa e desenvolvimento tecnológico e conferindo mais competitividade e rentabilidade às suas respectivas economias nacionais.

Assim como muitos soldados altamente treinados sempre buscaram vender sua experiência profissional a quem quer que lhes pagasse mais, nos dias de hoje, muitos profissionais oriundos de serviços secretos são flagrados em atos ilícitos ou têm seu nome associado à práticas de espionagem, chantagem ou sabotagem. É fato que muitos ex-agentes, de grande know-how, dedicam-se a espionar e a comercializar os segredos obtidos de forma subreptícia e ilegal. Um concorrente, em dúvida acerca de como proceder, sempre poderá lançar mão da espionagem.

Desprovida de um setor (ou mesmo de uns poucos profissionais) voltado para atividades de inteligência e segurança, uma empresa (com todos os seus segredos) se constitui uma atrativa e fácil presa para as ações de seus adversários, concorrentes ou inimigos, os quais não pouparão recursos, esforços, ou "truques sujos", para alcançar seus objetivos. Leon Trotsky disse uma vez: "Você pode não estar interessado na guerra, mas a guerra está interessada em você". Parafraseando-o, podemos afirmar que é profundamente arriscado para um empresário ou diretor de empresa negligenciar com a atividade de inteligência (e todas as suas implicações, lícitas ou não) pelo motivo de que seus "colegas" e concorrentes certamente não estarão dispostos a proceder da mesma forma!

O fato de tradicionalmente não estarmos acostumados a uma "cultura" de sigilo ou mesmo a nossa visão preconceituosa para com todos os que se dedicam ao ramo da inteligência (rotulando-os pejorativamente de "arapongas" ou associando-os à repressão política dos idos do regime militar), fazem com que, no Brasil, não nos apercebamos - a priori - das inegáveis vantagens que a "Inteligência Empresarial" pode trazer para os negócios.

São alguns exemplos de atuações de um Setor de Inteligência Empresarial:

- Estudo das publicações técnicas do respectivo ramo empresarial, no intento de colher informações sobre progressos dos concorrentes, novas técnicas, produtos e tendências mercadológicas;

- Análise dos noticiários das fontes correntes como jornais, rádio, televisão e Internet, coletando informações julgadas relevantes para a empresa e encaminhando-as à direção;

- Estudo das empresas concorrentes (seus talentos, sua estrutura, seus processos, equipamentos, parceiros comerciais, perspectivas de expansão de negócios etc);

- Estudo dos "serviços de inteligência" dos concorrentes, identificando seus integrantes, seus planos, ações de espionagem em curso etc;

- Auditoria das condições de segurança de uma empresa, analisando suas vulnerabilidades frente às ações delituosas de roubo, furto, espionagem, sabotagem e atentados contra a alta direção da instituição;

- Proposição de normas e procedimentos voltados para a salvaguarda da empresa no que tange à segurança;

- Indicação de necessidade e elaboração, em conjunto com os demais departamentos, de planejamentos contingenciais com vista à manutenção (ou a retomada, no mais curto espaço de tempo possível) das atividades normais da empresa, em face de sinistros, catástrofes naturais etc;

- Prevenção de "vazamento de informações", por meio de ações de varredura nas linhas telefônicas, inspeções contra escutas nos diversos ambientes, bem como desenvolvendo campanhas de conscientização;

- Tentativa de detecção e identificação da fonte de qualquer boataria lesiva à imagem da empresa, de seus produtos ou dos seus funcionários;

- Proceder às investigações ou sindicâncias, de nível interno, na empresa, visando detectar atos lesivos ao interesse da companhia - principalmente ações de furto, espionagem e sabotagem;

- Promoção de ações de vigilância e infiltração no âmbito interno, sob ordens estritas da alta direção;

- Auxílio à autoridade policial e acompanhamento das investigações de delitos praticados contra a empresa;

- Auxílio no processo de recrutamento e seleção de funcionários, no sentido de detectar desvios pregressos de conduta, que possam comprometer a atuação do novo funcionário e prejudicar a empresa;

- Identificação das necessidades especiais de treinamento e realização de palestras periódicas sobre temas concernentes à segurança e inteligência, para a conscientização do corpo de funcionários em seus diversos níveis;

- Acompanhamento da atividade do sindicato da categoria, mantendo a alta administração informada quanto aos movimen-

tos reivindicatórios ou às paralisações que possam ser prejudiciais aos interesses da empresa.

A ESPIONAGEM EMPRESARIAL

A espionagem consiste no esforço de desvendar, através de métodos ocultos e não convencionais, os segredos alheios. Os espiões - agentes que agem com o intuito de subtração de segredos - não são profissionais que agem com altruísmo e, para tais elementos, os fins a serem alcançados mais do que justificam os meios empregados. Para compreender mais os processos da espionagem é muito importante que dissociemos a imagem de seus agentes daquela veiculada por Hollywood, com James Bond e seus congêneres. Os verdadeiros profissionais da espionagem "agem incólumes no anonimato e em nada se assemelham a seus aparentados cinematográficos". Podem se apresentar de infinitas formas, como um executivo de sucesso, um colaborador ou correligionário político, uma mulher (ou homem) atraente, um técnico, um digitador, um mecânico, um faxineiro, sempre de forma insuspeita.

A espionagem talvez possa ser definida segundo o que eu chamaria de seu "axioma de nº1": "Não existem regras, ética ou limites; se você dispuser de um segredo (de um dado, de uma informação ou produto) que seja objeto de interesse dos "outros", tenha certeza de que eles realizarão o impossível para acessá-lo, copiá-lo, roubá-lo ou até mesmo destruí-lo". Quando falamos de "outros", estamos querendo nos referir aos concorrentes e seus consultores de inteligência empresarial, adversários, detetives particulares, aos repórteres investigadores e até mesmo às agências de inteligência estrangeiras.

A prevenção contra os riscos da espionagem requer um estudo individualizado para cada caso ou empresa:

a) Procure definir quais são os segredos ou informações acerca da empresa ou negócio que possam despertar a cobiça de concorrentes ou adversários. Quais os segredos do negócio? Fórmulas de produtos? Processos fabris? Processos administrativos revolucionários? Quais informações, se copiadas ou "vazadas" poderiam provocar danos à imagem, prejuízos financeiros ou ameaçar a posição que a empresa ocupa no mercado?

b) À exceção desses segredos ou informações anteriormente mencionados, existiriam outros objetos de interesse para os concorrentes? Quais? Ressalve-se que nem sempre as informações privilegiadas são objeto de cobiça unicamente dos concorrentes. Em dois casos conhecidos de registro de marcas, os próprios representantes e distribuidores se anteciparam ao fabricante e registraram a marca de um produto antes de seu lançamento. Nesses casos específicos, uma delas perdeu a representação, mas conseguiu retirar a marca de uma empresa americana do mercado brasileiro, gerando um processo na justiça brasileira. Curiosamente, a outra empresa não teve êxito por uma casualidade. A onda de fusões e aquisições na economia norte-americana abortou o lançamento do produto, mas se isso não houvesse acontecido, o prejuízo seria bastante grande.

c) Quem são os concorrentes? É empresa nacional ou multinacional? Qual é sua posição no mercado? Quem são seus dirigentes? Tais empresas concorrentes contam com setor devotado à atividade de inteligência? Têm contrato com alguma consultoria de inteligência empresarial?

d) Quem tem acesso às informações ou aos segredos que a empresa precisa manter a salvo da espionagem? Todos teriam realmente a necessidade de ter acesso a tais informações? Qual o grau de confiabilidade desses funcionários e de sua fidelidade à empresa? Há quanto tempo integram os quadros funcionais da instituição? Eles estão satisfeitos com a empresa? Qual a avaliação que se pode fazer de seu caráter? Como eles reagiriam a uma tentativa de cooptação por um concorrente?

e) Existe alguma "compartimentação" das informações que se pretenda preservar? Onde os "segredos" estão "guardados"? Por onde circulam?

f) Quais as "medidas de segurança" existentes na empresa? Elas envolvem efetivamente os segredos comerciais e industriais da atividade? Vale lembrar que a simples existência de fechaduras, alarmes e guardas de vigilância particular, por si só, não constitui em um dissuasor eficaz contra ações de espionagem.

Em seu excelente livro, de 1969, intitulado "ESPIONAGEM INDUSTRIAL", Jean Barral e George Langelaan citam alguns "sintomas básicos", em torno dos quais podem surgir outros indícios (às vezes difíceis de interpretar) da espionagem no meio empresarial:

- Queda inexplicável do volume de vendas em certos setores ou no total do mercado;

- Um novo concorrente lhe "passa uma rasteira";

- Um novo produto, praticamente idêntico ao seu, é lançado no mercado, pouco antes ou ao mesmo tempo que o seu;

- Uma campanha de publicidade de um concorrente precede e prejudica a que estava prestes a ser lançada pela empresa;

- O próximo lançamento de seu novo produto é amplamente difundido e faz cair as vendas do modelo anterior, ainda em estoque nas fábricas ou nos revendedores;

- Solicitam à empresa, com maior frequência que a costumeira, de lados diferentes e sem razão aparente, notícias, prospec-

tos, fotografias e informações de ordem técnica;

- Um ou mais engenheiros, técnicos, chefes, representantes comerciais, laboratoristas, supervisores ou mesmo operários altamente especializados, pede demissão para trabalhar numa firma concorrente;

- Estagiários contratados demonstram exagerado interesse em certos processos da empresa;

- A empresa recebe consultas ou visitas pouco comuns de pesquisadores, especialistas e jornalistas estrangeiros;

- Firmas estrangeiras solicitam estudos minuciosos, tendo em vista a possibilidade de fabricar, eventualmente, seu produto sob licença;

- Ocorrência de furto ou arrombamento que pareça, de alguma forma, curioso, fora do comum ou dificilmente explicável.

Poderíamos relacionar alguns "alvos" (pessoas), dentre os praticamente infinitos e possíveis, para as ações de espionagem empresarial:

- Integrantes da alta direção de empresas e instituições públicas ou privadas;

- Elementos com "funções-chave", porém de escalão inferior, nas áreas de administração, pesquisa e desenvolvimento de projetos, arquivos e mesmo da produção;

- Funcionários demitidos ou descontentes;

- Telefonistas e secretárias;

- Políticos e lobistas ligados às empresas;

- Empregados de copa, zeladoria ou limpeza, que circulem pelas várias áreas, sem despertar suspeitas;

- Técnicos de manutenção, principalmente de empresas terceirizadas.

São alguns locais visados pelos "agentes" da espionagem:

- Gabinetes de diretoria e salas de reunião;

- Salas de recepção onde trabalham secretárias e recepcionistas;

- Gabinetes de políticos que representam interesses da empresa;

- Salas de projeto, arquivos, reprografia ("xerox") e CPD;

- Refeitórios ou Copas, onde normalmente se conversam "assuntos de serviço";

- Centrais telefônicas, armários de distribuição de edifícios e "caixas de passagem";

- Centrais de Segurança;

- Cestas de papéis e depósitos de lixo;

- Quartos de hotéis ou motéis, quando se tratar de "alvos" em viagens.

O que buscam os espiões?

- Informações técnicas sobre processos de produção e novos produtos;

- Plantas, projetos, esquemas, arquivos de computador ou fórmulas de produtos;

- Fotografias detalhadas de instalações ou equipamentos;

- Manuais técnicos ou documentos sigilosos;

- Subtração de amostras de produtos;

- Informações sobre a estrutura administrativa e saúde financeira da empresa-alvo;

- Informações privilegiadas sobre as intenções comerciais, perspectivas de lançamento de produtos ou novos mercados;

- Identificação dos profissionais que trabalham nas empresas-alvo, seus hábitos e vida pessoal, estabelecendo seus perfis, com vista à eventual contratação, cooptação ou chantagem;

- Detalhes da vida privada de empresários e executivos, para campanhas de desmoralização (contra pessoas ou instituições) junto à mídia;

- Detalhes censuráveis da vida pública de políticos e autoridades, provas de desvios de conduta etc.

À medida que a tecnologia avança, o aperfeiçoamento dos "métodos de agressão" dos espiões vem requerer a contraposição de profissionais sempre mais qualificados e competentes. Embora equipamentos cada vez mais sofisticados possam ser facilmente adquiridos no comércio (principalmente no exterior), não se deve esquecer que uma expressiva quantidade de informações pode e ainda continua sendo obtida de maneira simples e tradicional, através da escuta de conversas, da inconfidência dos detentores de segredos, do acesso indevido a anotações, listagens e manuais técnicos etc.

São equipamentos utilizados em espionagem / invasão de privacidade:

- Micro-câmeras de foto e vídeo, normalmente dissimuladas em roupas, chapéus, bolsas, valises ou em objetos de decoração ou mobiliário.

- Câmeras de foto e vídeo que permitem grande aproximação de foco ("zoom"), mesmo em condições de iluminação precária;

- Extensões clandestinas, transmissores de rádio (normalmente FM) ou gravadores acoplados à linha telefônica, todos genericamente conhecidos por "GRAMPOS";

- Microfones/transmissores dissimulados (escondidos sob a roupa ou sob a forma de objetos como canetas, cartões de crédito, calculadoras ou maços de cigarro) ou monitorando compartimentos ("ESCUTAS") disfarçados no interior de tomadas, interruptores, por trás de quadros, sob mesas, em "fundos falsos" de itens de decoração ou mobília;

- Amplificadores de sons, microfones parabólicos e estetoscópios com ventosas;

- Em se tratando de ações levadas a cabo por serviços de inteligência, a sofisticação de meios tende a surpreender. À disposição dos países do "Primeiro-Mundo" existem estações terrestres, embarcações ou aeronaves com dispositivos capazes de receber, processar, analisar, identificar, localizar e armazenar os sinais eletrônicos das comunicações de rádio, telefonia, fax e correio eletrônico.

A Agência de Segurança Nacional dos Estados Unidos (NSA), assim como sua equivalente britânica, o Quartel General de Comunicações do Governo (GCHQ), possui estações de escuta capazes de selecionar dados a partir de palavras chave preestabelecidas, em qualquer tipo de comunicação.

No caso americano, as bases de escuta dispersas por todo o mundo (inclusive na própria Grã-Bretanha) retransmitem as informações coletadas para uma central em Fort Meade, Maryland, onde um contingente de cerca de trinta mil funcionários se dedicam a processar e analisar as informações obtidas, encaminhando-as em seguida aos órgãos governamentais que delas necessitem.

Fotografias de surpreendente qualidade, tiradas por satélites e aeronaves de reconhecimento, completam o quadro e hoje se encontram disponíveis para a iniciativa privada. Países como a Rússia, China, França e Israel também devem fazer uso de recursos análogos de inteligência, embora seja sabido que nada iguala o sistema americano, em sofisticação. Hoje, através de uma tecnologia de captação e análise de emanações de radiação, conhecido pela sigla TEMPEST, pode-se até monitorar, à distância, todos os caracteres digitados na tela de um computador.

São alguns equipamentos utilizados na contra-espionagem:

- Medidor de tensão elétrica para linha telefônica;

- Identificadores de chamadas telefônicas (BINAs);

- Embaralhador de voz ("PHONE SCRAMBLER");

- Detector de câmeras, transmissores e gravadores ("TTRD");

- Detector de circuitos eletrônicos, ligados ou desligados através de microondas ("Vassoura de varredura");

- "SCANNER", para a detecção de frequências de rádio transmissíveis de qualquer natureza;

- Câmeras dissimuladas;

- Sprays e lápis com tinturas invisíveis a olho nu, utilizados para a detecção de pequenos furtos, cujos autores acabam flagrados pelos vestígios deixados por tais marcadores;

- Microfone parabólico, capaz de captar conversas à distância.

Como se percebe, em todos os campos da atividade existe uma necessidade de que sejam preservadas informações e dados que, se tornados públicos, ou levados ao conhecimento de pessoas inescrupulosas, poderão causar irremediáveis danos às instituições, seus processos comerciais ou fabris, às finanças, às reputações pessoais de seus integrantes e/ou à segurança de personalidades ou instituições em seus diversos aspectos.

Para salvaguardar a privacidade ante a espionagem, devemos nos acostumar ao sigilo e observar o princípio da compartimentação das informações, reportando unicamente aos demais, apenas aquilo que lhes caiba tomarem conhecimento. A chave é o autopoliciamento, negando realmente ao adversário o acesso aos nossos segredos. A curiosidade em torno de informações técnicas, industriais ou comerciais pode estar associada à espionagem. Vale estar atento para pessoas que manifestam ou deixam transparecer um excessivo (ou mesmo incomum) conhecimento ou demonstram interesse em torno dos segredos que se queira manter como tal. Hoje é sabido que muitos dos avanços tecnológicos da antiga União Soviética foram alcançados com o benefício do conhecimento obtido gratuitamente no Ocidente, através do estudo sistemático de publicações de caráter técnico/científico, jornais e revistas, brochuras de publicidade, anais de congressos etc. ("OPEN INTELLIGENCE"). Tais recursos permitiram aos russos poupar grande quantidade de dinheiro, normalmente gasto em pesquisa e desenvolvimento.

Em 1951, o Diretor da Agência Central de Inteligência dos Estados Unidos convocou um grupo de universitários e entregou-lhes diversos exemplares de revistas técnicas e militares, comercializadas livremente, solicitando-lhes que, com base nas mesmas publicações, elaborassem um estudo hipotético sobre o poderio militar americano. Eram anos da Guerra Fria e os resultados ficaram tão próximos da realidade, que causaram preocupação. Nunca se deve esquecer de que mesmo fatos que podem parecer sem importância a um homem comum, podem significar muito para um observador bem treinado.

Quem quer que possa se constituir num alvo de espionagem, jamais poderá negligenciar a identificação de pessoal, sendo que especiais cuidados deverão ser tomados com a circulação no interior da empresa e o controle de acessos às áreas que contenham informações ou documentos que se objetive salvaguardar. Imagine quais informações poderiam ser coletadas, ainda que rapidamente, por um "curioso", que tivesse a liberdade de circular pelas áreas internas da empresa.

Cuidado com a guarda de chaves, bem como precauções devem ser tomadas para impedir que as mesmas sejam copiadas indevidamente.

Devem-se estabelecer critérios para a seleção de mão de obra e, sobretudo, avaliar o seu grau de confiabilidade no que tange ao acesso a qualquer tipo de dado reservado.

Extremo cuidado deve ser observado com agendas telefônicas, documentos sobre as mesas e materiais que possam ser subtraídos ou indevidamente fotografados ou copiados. O simples extravio ou duplicação não autorizada de um disquete pode provocar prejuízos de grande monta a uma empresa.

Documentos que representem segredos, quer políticos, quer empresariais, devem ser manuseados com critério. Seu acesso, manuseio e circulação, ainda que apenas no âmbito interno da instituição, deverão obedecer a cuidados. De nada adianta que os mesmos sejam normalmente guardados em cofres ou arquivos fechados, mas permaneçam durante um dia inteiro sobre a mesa de um funcionário (mesmo de confiança), num compartimento por onde circulem diversas pessoas estranhas ou cujo acesso às referidas informações não seja permitido. Da mesma forma, permitir que um mensageiro circule com um documento sigiloso num envelope aberto, em condições de ser copiado na primeira fotocopiadora, não se constitui um procedimento adequado, sob o ponto de vista de segurança contra espionagem.

A retirada de documentos, arquivos ou dados, sob os quais se pretenda manter sigilo, do ambiente físico da empresa deve ser evitada. A retirada de documentos da empresa para um trabalho noturno ou de final de semana, por funcionário autorizado, ainda facilita a tarefa de quem apenas pretenda acessar o conteúdo dos documentos ou copiá-los. Foi amplamente noticiado na mídia, o caso de um funcionário do Serviço de Inteligência Britânico (M.I.6), que após sair de um bar perto de seu trabalho em Londres, esqueceu seu "notebook" num táxi. Sob o ponto de vista do espião, será sempre mais fácil acessar os segredos de uma empresa quando fora do seu local de guarda habitual e a própria apropriação de tal material poderá ser "mascarada", deixando sempre uma aura de dúvida quanto às reais causas da perda. Pastas com documentos reservados podem ser facilmente extraviadas, roubadas ou furtadas, gerando consideráveis prejuízos para as instituições.

Ações de roubo e de furto, aparentemente simples, podem "esconder" uma real motivação de espionagem! Uma simples tigela de metal, manchada e riscada, moldada por um prisioneiro alemão (às escondidas, em sua hora de folga), tão inocente que lhe foi permitido retornar com ela para a Alemanha, revelou aos ocidentais as características avançadas das ligas metálicas utilizadas pela aeronáutica soviética nos críticos anos iniciais da Guerra Fria. Hoje, na Grã-Bretanha, o furto de computadores ou de seus componentes essenciais de memória fomenta o comércio de gabinetes blindados e outros recursos destinados a garantir a segurança física do equipamento e de seus dados.

É importante atentar para quaisquer comentários, anotações ou documentos que possam vir a comprometer os segredos que se pretenda manter. Cuidado com as conversas e, sobretudo, com quem as possa estar escutando. Linhas telefônicas convencionais devem ser submetidas a inspeções periódicas e – em face de grande risco – equipamentos de detecção de escutas clandestinas poderão ser a elas acoplados (admitindo, contudo, sua ineficiência quanto à detecção de grampos instalados nas próprias centrais telefônicas). Telefones, tanto os convencionais quanto os celulares, não deverão ser utilizados para conversas reservadas.

Atualmente, os computadores são um aspecto fundamental das atividades de pessoas e empresas. As mesmas informações e documentos que um dia apenas existiram em estado bruto, "no papel", acondicionadas em pastas e arquivos, hoje circulam também por meios eletrônicos. A proteção das informações existentes no PC é, primariamente, da responsabilidade de seu usuário. O acesso físico ao terminal deve ser controlado, na medida em que bastam poucos instantes para que um elemento treinado possa fazer a substituição de componentes da memória de uma máquina, levando consigo informações de valor. Pesquisas demonstram que uma grande quantidade de ações adversas é praticada por usuários descontentes, mal intencionados ou cooptados por concorrentes. Os terminais devem ser protegidos por senha (de forma a dificultar ao máximo o acesso não autorizado ao conteúdo dos arquivos) e as cópias de segurança obrigatoriamente devem ser mantidas em compartimento seguro e com trancamento adequado. As senhas deverão ser difíceis de serem descobertas e não devem ser compartilhadas,

mesmo entre colegas de trabalho. O temor que as pessoas têm de digitar seus dados pessoais na Internet, bancos ou outros ambientes semelhantes, não se transfere para o ambiente de trabalho. Em princípio, a confiança mútua também é facilitadora das fraudes, não sendo raro ocorrências em que um funcionário comete ato ilícito a partir da utilização indevida da senha de seu companheiro de trabalho. É fato que, ainda hoje, para grande parte das senhas, mesmo profissionais da área de informática e principalmente em sistemas internos, ainda se valham normalmente de nomes próprios (como de filhos, esposas ou namoradas), números de telefone ou datas de aniversário, namoro e outras, facilmente dedutíveis.

No caso de Redes, a simples utilização de programas antivírus ou "Firewall" não garante a incolumidade do PC e seus arquivos. Computadores conectados em rede devem merecer toda a atenção de bons especialistas em segurança lógica, os quais, além de conhecimentos técnicos, devem apresentar um histórico de conduta ilibado. Não se deve economizar na segurança das informações da empresa e os profissionais que a gerenciam devem ser obrigatoriamente confiáveis e bem remunerados. Campanhas de conscientização em torno da segurança devem ser instituídas na empresa e o cumprimento das normativas estabelecidas terá de ser fiscalizado bem de perto. Sempre que possível, deve-se evitar transmitir informações reservadas "online"; caso seja imprescindível fazê-lo, utilize-se de sistemas criptografados, os quais só podem ser acessados e lidos por pessoas que tenham a chave de decodificação. Dados passados via e-mail são, em sua maioria, transmitidos abertos e podem ser vistos inclusive pelo próprio provedor. Vale lembrar que, na atual legislação brasileira, dificilmente se consegue configurar e punir a "espionagem online".

Uma senha escrita num papel de lembrete ou mesmo as páginas seguintes de um bloco de anotações (com os sulcos do lápis ou caneta que possam ser coloridos) revelam muitas informações preciosas para um adversário realmente esperto. Documentos aparentemente sem utilidade, mas que contenham informações de caráter reservado, não deverão ser apenas rasgados ou amassados e jogados no lixo. O lixo "fala" muito sobre os indivíduos e as empresas. Da "arqueologia do inservível" podem surgir peças importantes, que ajudarão a compor o mosaico dos segredos que se pretenda desvendar. Não é incomum se encontrar nas lixeiras listagens completas, com dados reservados de clientes ou produtos, disquetes, fitas de máquina de escrever ou impressoras matriciais, materiais que podem representar informações inestimáveis aos adversários e concorrentes. A "leitura" das fitas pode revelar o teor de todos os textos e documentos impressos, bem como os dados nos disquetes podem, em vários casos, ser "recuperados" por alguém que disponha dos recursos tecnológicos adequados. As cestas de papéis podem se constituir numa inestimável "fonte de informações" e os documentos que possam despertar interesse devem receber especiais cuidados de destruição. Às vezes, o simples fitilhar de um documento numa máquina destruidora de papéis não garante que o teor do documento não possa a ser revelado. Quando da invasão da Embaixada Norte-americana no Irã em 1981, a grande maioria dos documentos capturados, mesmo picotados, pode ser reconstituída mediante um exaustivo e paciente trabalho de dezenas de pessoas. A "sucata" de computadores pode conter informações as quais não se desejaria tornar pública e que poderiam causar alguma forma de prejuízo para a empresa. O próprio autor já teve oportunidade de constatar, numa inspeção em instalações de uma empresa líder do ramo das telecomunicações, inúmeros microcomputadores precariamente estocados e que vinham sendo sistematicamente "depenados" de seus "hard drives" e outros componentes, sem que a segurança local parecesse se importar com isso. Não existia, na referida companhia, um procedimento padrão para "zerar" os arquivos de discos rígidos daquelas máquinas e, se considerarmos que a tecnologia de hoje já permite a reconstituir dados de computadores após acidentes aeronáuticos ou mesmo a imersão em água ou lama, não se poderia descartar que algum tipo de informação de valor tenha acabado por mudar de mãos.

Nada pode favorecer mais ao "Espião" do que a crença generalizada de que não haja segredos por proteger e que os cautelosos se preocupam sem razão, pois estariam apenas "vendo fantasmas".

O espaço das poucas laudas deste trabalho seria claramente insuficiente para apresentar exemplos de espionagem empresarial. Cada executivo, diretor ou gerente de empresa certamente poderá apresentar um bom número de casos (supostos ou comprovados) ocorridos em seu ramo de negócio, alguns dos quais, quem sabe, até vivenciados por eles próprios. Tais fatos são uma pequenina pedra de gelo, da ponta de um iceberg; até pelo fato de que, normalmente, as ações da espionagem empresarial raramente chegam ao conhecimento do público. Ninguém admite publicamente e de bom grado que sofreu espionagem, principalmente se não houver provas suficientes para a condenação, quer do espião ou (o que é ainda mais difícil) de seus mandantes. Vejamos alguns casos conhecidos:

- Uma rede de espionagem do governo soviético, com o roubo de segredos de empresas privadas e instituições governamentais de pesquisa tecnológica, permitiu-lhes "acelerar" a construção da bomba atômica comunista;

- A indústria aeronáutica soviética beneficiou-se da enorme infiltração de espiões na Grã-Bretanha durante as décadas de cinquenta e sessenta. A enorme semelhança entre o Illyushin Il-62 russo e o VC-10 britânico, bem como entre o Tupolev Tu-144 e o supersônico Concorde parecem falar por si. Ambos os aparelhos britânicos eram produzidos pela mesma companhia (inicialmente a Vickers, que em meados dos anos 60 passou a se chamar British Aircraft Corporation). No caso do Concorde, a descoberta, em tempo, pela contra-espionagem ocidental, do vazamento de informações para os espiões a soldo dos sovié-

ticos, motivou a "intoxicação" dos mesmos com dados fraudados, que comprometeram irremediavelmente o desempenho do "Concordsky" (como o "clone" do Tupolev ficou conhecido). A queda de vários Tu-144 (inclusive na apresentação oficial do aparelho, no Salão Aeronáutico de Paris) e o fracasso comercial da aeronave parecem estar associados às falhas de cálculos e defeitos nos planos deliberadamente passados aos agentes soviéticos.

Não dá para esconder a extraordinária semelhança entre o Concorde (esq.) e seu concorrente soviético, o Tupolev TU-144 (dir.), da mesma forma que o VC-10 (esq.) e o Il-62 (dir.) também parecem ter muito em comum.

- Na década de sessenta, Israel conseguiu contrabandear da Suíça as plantas completas do caça francês Mirage III e, assim, fabricou cópias não autorizadas do aparelho. Além de produzir novos aparelhos e sobressalentes em Israel, o contrabando de tecnologia francesa redundou, anos mais tarde, num projeto completamente novo, o caça Kfir, uma combinação (avançada para a época) da aerodinâmica francesa com um motor americano mais poderoso.

O Kfir (esq.) tem motor americano, mas seu projeto foi claramente adaptado do Dassault Mirage III francês.

- Em 1982, a IBM americana reportou que a companhia japonesa HITACHI estaria se utilizando indevidamente de segredos da manufatura de computadores.

- Em 1998, fontes do FBI reportaram ao LOS ANGELES TIMES que Israel figurava entre os principais responsáveis pelas ações de espionagem industrial contra companhias americanas, às quais redundaram em prejuízos orçados em US$300 bilhões, em 1997. Mais de 1.100 casos documentados pela contraespionagem americana apontam como alvos prioritários dos estrangeiros as empresas de informática do Vale do Silício, seguidas pelas indústrias do setor aeroespacial, de defesa, de eletrônica (em particular as ligadas às telecomunicações) e químicas. Por se tratar de matéria politicamente sensível, o FBI não identifica abertamente os governos que patrocinam as ações de espionagem econômica, mas se especula (com razoável chance de acerto) que dentre as nações estariam a França, a Alemanha, a China, a Coreia do Sul, além de Israel e (é claro) da Rússia.

- A indústria de materiais óticos e eletro-eletrônicos é pródiga em exemplos de produtos "copiados" ilegalmente ou "aper-

feiçoados" com base em ações de espionagem. A China, hoje, desponta como o paraíso dos "clones" sem licença e, curiosamente, os americanos revelaram (em 1999) a descoberta de uma vasta rede de espionagem que teria conseguido se apossar de valiosíssimos segredos industriais e militares como, por exemplo, o da "bomba de nêutrons";

- O Iraque, de Saddam Hussein, foi repetidamente acusado de espionagem tecnológica e a rede de defesa aérea do país foi reconstituída, após a primeira Guerra do Golfo (1991), graças a processadores de computador de videogames de última geração, adquiridos no exterior e habilmente contrabandeados para país muçulmano;

- Documentos do Parlamento Europeu apontam que, entre 1994 e 1995, o Brasil teria sido o alvo de uma ação dos serviços de inteligência americanos quando da licitação para compra dos radares do Sistema de Vigilância da Amazônia - SIVAM. A CIA e a NSA, valendo-se de uma enorme gama de recursos, que envolvem desde estações terrestres de monitoramento de comunicações, até aeronaves e satélites militares, teriam "grampeado" as comunicações do governo brasileiro e dos escritórios da companhia francesa Thomson, tida como favorita na concorrência. O contrato de US$1,3 bilhões de dólares, finalmente firmado com a americana RAYTHEON, é mencionado como um dos mais importantes exemplos de espionagem econômica do contexto pós guerra fria. Segundo fontes ligadas à empresa francesa, citadas pela revista brasileira ÉPOCA, a assistência dos órgãos de inteligência americanos teria mudado o rumo da negociação: "Havia algo estranho. Cada vez que os franceses faziam uma proposta, os americanos vinham com outra melhor pouco tempo depois".

A espionagem e a invasão da privacidade são, hoje, uma realidade com a qual profissionais de segurança, sobretudo os encarregados da proteção de empresas, políticos e pessoas de notável projeção, têm de estar preparados. Os empresários e demais profissionais de alta direção ou gerência empresarial também precisam estar conscientes dos riscos que estão correndo. Conquanto a realidade da espionagem lhes parecer distante, ou mesmo "coisa de filme", eles continuarão se constituindo um alvo fácil e compensador, tendo seus negócios prejudicados pelas mesmas "forças ocultas", cuja ação não foram capazes de prevenir, detectar e neutralizar.

Os nossos "detentores de segredos", bem como aqueles a quem lhes caiba proporcionar segurança, devem estar conscientes dos riscos da espionagem, dos diversos modus operandi e dos recursos à disposição de seus agentes.

A SABOTAGEM NO MEIO EMPRESARIAL

O termo "sabotagem" está profundamente ligado a pratica empresarial; origina-se da palavra francesa "sabot" ou, em português, tamanco. O tamanco veio a ser considerado símbolo da revolta de trabalhadores revolucionários que atiravam seus sapatos de madeira dentro das máquinas, nas fábricas, durante as periódicas agitações dos séculos XVIII e XIX. Mais tarde, ao se procurar uma palavra para descrever o ato de deliberada destruição de propriedades para alcançar uma solução desejada, chamou-se ao ato de "sabotagem" e de "sabotadores" os seus agentes.

Por sabotagem poderemos compreender um conjunto de ações de perturbação da ordem, normalmente perpetradas de modo dissimulado ou covarde, no anonimato, e que ocasionam graves danos às instalações, ao que nelas é produzido ou guardado, aos processos ou andamento do serviço etc.

Como uma forma ou ato de guerra a sabotagem se destina a provocar danos à capacidade do adversário: são ações contra a administração, produção industrial, produção de alimentos e bens de consumo, contra as forças armadas e complexo industrial militar, contra os meios de comunicação e suas linhas ou equipamentos de transmissão, contra o moral de uma população etc. A sabotagem, bem como a espionagem, aperfeiçoou-se no meio militar e dos serviços secretos, evoluindo em um número infinito de formas, nem todas necessariamente violentas ou físicas. As empresas, hoje, e as atividades que as mesmas desenvolvem, são diuturnamente alvo de ações de sabotagem. Tais atos condenáveis, moral e legalmente, derivam-se da concorrência extremamente desleal e são um desafio com o qual os profissionais de inteligência e segurança devem - obrigatoriamente - estar capacitados a lidar. No Brasil são recentes os exemplos de explosão de torres de transmissão de energia elétrica, panes no sistema de telefonia, descoberta de peças defeituosas em aviões da EMBRAER e até os sucessivos e misteriosos defeitos que vêm comprometendo o êxito do programa nacional de satélites espaciais. Uma constante nos atos de sabotagem empresarial é a grande dificuldade de proceder à apuração da real autoria das ações, acabando por gerar, além dos prejuízos materiais, uma desconfiança mútua que desarmoniza o meio funcional.

Para melhor compreensão, dividiremos o tema em Sabotagem Ativa, ou "ação direta", que se constitui em atos repentinos e violentos perpetrados contra "alvos-chave". São as ações de destruição ou inutilização temporária de máquinas, equipamentos e instalações, os atentados a bomba, os incêndios criminosos, os envenenamentos dos suprimentos de ar, água ou comida, as panes provocadas nos fornecimentos de energia, cortes de linhas de comunicações, geração de interferência eletrônica, destruição de eletromagnética de arquivos de dados, disseminação de vírus de computador, "Bombas de E-mail" etc.

A extrema dependência da informática faz as empresas padecerem nas mãos de "hackers", os quais, por motivos que vão desde a satisfação da vaidade pessoal à prática de chantagem financeira, buscam penetrar nas redes de computadores de empresas e governos. O próprio Presidente americano e o sistema de comunicações por computador da Casa Branca já foram alvo de um verdadeiro bombardeio de e-mails: dezenas de milhares de mensagens, emitidas, ao que se acredita, por uma única fonte, "congelaram" o sistema de correspondência por sobrecarga. Da mesma forma, ataques que visam à paralisação dos serviços (nos modos "Denial of Service" e "Distributed Denial of Service") já atingiram sites de empresas como o YAHOO, CNN e AMAZON.

Numa outra modalidade de Sabotagem Ativa, funcionários inescrupulosos ou descontentes ("insiders") podem se utilizar do acesso aos computadores da empresa a fim de sabotar as informações neles contidas, cometer fraudes etc. Verdadeira dor de cabeça dos planejadores de segurança de sistemas, os quais tentam se antecipar às ações, bem como, registrando no sistema todos os atos dos usuários, poder apurar posterior autoria. Além disso, para determinadas ações, estabelece-se uma hierarquia de senhas que só permitem que determinados comandos sejam executados por usuários de elevada graduação. Normalmente, no meio empresarial, os problemas enfrentados devem-se a pouca importância que os próprios usuários, detentores dos cargos de chefia, dão à segurança física de seus próprios terminais ou às suas senhas. O acesso quase irrestrito aos terminais, aos seus componentes de memória e, sobretudo, senhas fáceis de deduzir ou anotadas de forma que possam ser copiadas, fazem com que sistemas nos quais se gastou uma fortuna em hardware e softwares de segurança acabem valendo muito pouco. Alguns inquéritos administrativos instaurados contra funcionários do DETRAN/RJ nos últimos anos se deveram a pouca atenção dada às suas próprias senhas, as quais permitiram a realização de uma miríade de fraudes.

São mundialmente famosas as ações de sabotagem (e extorsão) envolvendo envenenamento dos remédios da marca TYLENOL e os chocolates MILKA. Embora nem sempre seja encarada como tal, a "ação direta" pode envolver ações de rapto ou eliminação física de pessoal-chave da administração, pesquisa e desenvolvimento etc. Nos anos sessenta, o Serviço de Inteligência de Israel empenhou-se em "desencorajar" os cientistas alemães que trabalhavam na construção de mísseis balísticos para o governo egípcio: dentre os recursos utilizados figuravam desde as ameaças pessoais, ao envio de cartas-bomba. No Rio de Janeiro, ficou famoso o caso de assassinato do dono da rede de lojas REI DAS TINTAS, por pistoleiros a mando de um concorrente.

Na "ação indireta", ou Sabotagem Passiva, objetiva-se a mesma finalidade de prejudicar o adversário, porém sem fazer uso da violência. Trata-se de encorajar o absenteísmo ou a paralisação no trabalho, retardar ou postergar a execução das atividades cotidianas ("operação tartaruga"), fingir-se de doente, deixar de cumprir rotinas preestabelecidas ou fazê-las displicentemente, ou com atraso. Simulando resfriados, e por isso, afastando-se periodicamente do serviço, o trabalhador mal intencionado pode interferir eficazmente com a produção. Deixar de lubrificar máquinas ou substituir peças desgastadas, próximas do fim de sua vida útil, inevitavelmente, ocasionará avarias no equipamento, reduzindo a produção. A Sabotagem Passiva, mesmo que dispersa, tem um efeito cumulativo enorme.

A Sabotagem Psicológica objetiva causar greves, paralisações, diminuir o ritmo de trabalho dos funcionários da empresa, provocar pânico, motins, disseminar boatos etc. Um exemplo simples desse tipo de sabotagem nas empresas é a prática do "trote telefônico", quando o agente telefona para uma empresa e avisa da existência de uma bomba prestes a explodir. É normal que, ao receberem tais chamadas, as empresas parem a produção e evacuem seus funcionários do prédio, enquanto a segurança e os policiais efetuam a busca ao artefato explosivo. Sem utilizar-se de violência ou recorrer a nenhuma injúria física direta, o sabotador causa a perda de inúmeros homens-hora e reduz a produção de uma determinada empresa.

No contexto da Sabotagem Psicológica a propaganda tem muita importância, e verdadeiras campanhas podem ser planejadas e postas em prática, por concorrentes, com o intuito de denegrir pessoas, companhias ou seus produtos. Todos os mecanismos e técnicas da publicidade podem ser inteligentemente empregados para reverter os hábitos de um público consumidor, ou minar a simpatia para com uma pessoa ou uma instituição.

O emprego dos recursos da moderna computação permite hoje, a qualquer pessoa, adulterar imagens fotográficas. A realidade que Jacques Bergier e Pierre Nord retratavam em seu "ATUAL GUERRA SECRETA", de 1967 ("Pode-se reproduzir qualquer voz humana por meios eletrônicos e produzir uma declaração do Presidente Johnson gritando 'Viva o Vietcong! '") evoluiu de forma quase inimaginável. Steven Spielberg filmou Lyndon Johnson cumprimentando Tom Hanks (em "Forest Gump"); hoje os programas permitem alterar imagens dinâmicas com base em sons e fonemas pré-gravados, os quais são identificados, arquivados e recombinados de maneira que produzam novas palavras e frases. Tais dados são combinados à gravação de imagens da pessoa pronunciando uma frase curta; o computador memoriza expressões da boca, face, do queixo, demarca pontos para a reprodução, processa imagens recombinando os fonemas iniciais, forma outras palavras e exibe a imagem pré-gravada falando frases diferentes das que haviam sido ditas. Embora os programas necessários à produção desses filmes ainda não se encontrem à disposição do público, conjecturamos que não deverá levar muito tempo para que os mesmos se tornem uma ferramenta tão comum nos PCs quanto os programas que hoje nos facultam "compor" fotografias. Com os recursos

adequados, pode-se falsear a realidade, criando "provas" necessárias para emprestar credibilidade à sabotagem psicológica em suas diversas acepções.

A disseminação de boataria também pode ter resultados catastróficos, permitindo a especulação financeira ou marcando pejorativamente a imagem de empresas, pessoas ou produtos. Além do tradicional "boca a boca" e dos canais tradicionais de mídia, hoje a Internet proporciona um propício campo para a divulgação de boataria. Os rumores ou boatos são difíceis de ser enfrentados e desmentidos. O ditado popular, segundo o qual "o povo aumenta, mas não inventa" pode comprometer a reputação de uma instituição, de produtos ou mesmo pessoas, necessitando, para sua reabilitação, de um às vezes caríssimo trabalho de marketing.

Em conjunturas trabalhisticamente adversas como as dispensas de um grande número funcionários, privatizações, redução ou congelamento de salários, que concorrem para um aumento no descontentamento geral, é constatado um aumento na ocorrência de sabotagens.

As possibilidades de sabotagens são praticamente ilimitadas e vêm requerer um estudo prévio e bastante pormenorizado acerca das possibilidades e probabilidades de suas ocorrências.

PEQUENO GLOSSÁRIO DE TERMOS DA ÁREA DE INTELIGÊNCIA

BUSCA: É a operação de obter quaisquer informações que não estão disponibilizadas em fontes ostensivas, que sejam mantidas em sigilo ou sob qualquer esquema especial de proteção. Para obtenção de informações de tal natureza faz-se necessária a adoção de estratagemas, que incluem a observação de pessoas ou locais (vigilância), a infiltração, o "grampeamento" de ambientes, a interceptação telefônica ou postal etc.

CAVALO DE TROIA: Programa altamente destrutivo, que permite o roubo de senhas ou outras informações sigilosas, inserido ou "disfarçado" sob a forma de um programa ou arquivo útil.

CIFRA: É a explicação ou a "chave" para uma escrita secreta. Um documento cifrado necessita ser decifrado para tornar-se inteligível, visto que seu teor não pode ser descoberto através de simples leitura.

CÓDIGO: Trata-se de um sistema de palavras, ou grupo de letras ou símbolos, designados para representar outras palavras. Sob o sistema de código, uma simples palavra pode ter vários significados, representar várias palavras combinadas, ou ser equivalente a uma frase ou mesmo a um parágrafo inteiro, tudo segundo uma determinação prévia.

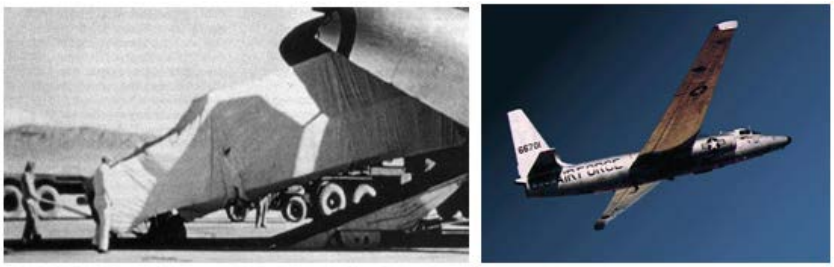
COLETA: Ação de amealhar informações contidas em fontes ostensivas, de fácil acesso. Consiste em acessar informação não reservada, disponível em livros, catálogos, bancos de dados ou sites de Internet etc.

COMPARTIMENTAÇÃO: A necessidade de manutenção do sigilo estabelece que cada pessoa conheça apenas aquilo que precisa ou que lhe é permitido saber acerca de um determinado assunto. Consiste na divisão de trabalho ou de um segredo, de forma que um elemento envolvido ignore a tarefa ou a missão creditada ao outro companheiro. A compartimentação visa minimizar a possibilidade de que as informações sigilosas "vazem" para adversários ou concorrentes e garante que uma traição ou inconfidência apenas acarretará no conhecimento parcial de um assunto e nunca sua totalidade.

CONTRA-ESPIONAGEM: Trata-se da atividade do ramo da contra inteligência que tem por objetivo a detecção, a identificação e a neutralização da espionagem adversária.

CONTRAINTELIGÊNCIA: "A arte do segredo reside em ser tão aberto, em relação à maioria das coisas, que sequer se imagine a existência daqueles poucos segredos realmente críticos, tranquilizando o adversário e retardando-lhe as iniciativas." B.H. Liddel Hart

Responsável pela salvaguarda dos segredos ou das informações, contrapondo-se às ações da inteligência adversária. Desenvolve, dentre outras atividades, o estudo da estrutura e modus operandi dos setores de inteligência adversários, o planejamento da segurança preventiva, a contraespionagem e as ações de desinformação que visam iludir (ou "intoxicar") o adversário.



Na foto de 1955, um protótipo do então secretíssimo avião-espião U-2 (dir.) chega à base em Nevada para testes, envolto em encerados que impedem a percepção de sua forma.

CRACKER: É o "hacker" criminoso. Indivíduo que tenta conseguir ilegalmente ou sem autorização, acesso a outros sistemas de computadores. O "cracker" faz o possível para quebrar os sistemas criptográficos de segurança e, geralmente, age com o intuito de sabotar ou auferir alguma vantagem econômica a partir das informações que subtrai.

CRIPTOGRAFIA: De forma bem simplificada, pode ser definida como a técnica de segurança que converte informações, mensagens, dados ou arquivos de computador em um código complexo de símbolos, ilegível, difícil de ser descoberto. Tal salvaguarda pode ser decodificada por alguém que detiver a tabela ou fórmula de decriptografia específica ("Chave").

DESINFORMAÇÃO: É um precioso recurso da Inteligência que, através da manipulação planejada de conhecimentos ou dados sigilosos, busca deliberadamente iludir, confundir ou induzir o adversário a um erro de avaliação comprometedor. No intuito de ser aceita como verdade, a desinformação combina, em adequadas proporções, informações autênticas e falsas, habilmente inventadas. A desinformação deve ser plausível e capaz de sensibilizar o alvo escolhido. Para ser bem sucedida ela deve, ao menos em parte, corresponder à realidade ou estar em conformidade com a maneira de pensar do seu público alvo.

ENGENHARIA SOCIAL: Termo relativamente recente, muito empregado no âmbito da segurança de sistemas computacionais, é normalmente utilizado para qualificar os tipos de intrusão não técnica, que enfatiza o elemento humano como o alvo mais vulnerável dentro da cadeia de segurança. Trata da obtenção de informações importantes de uma instituição, a partir da colaboração involuntária de seus usuários e colaboradores, os quais são manipulados em sua ingenuidade ou boa fé. Esse mesmo "abuso da boa fé" pode ter por objetivo envolver pessoas para obter informações privilegiadas, roubar-lhes segredos, como senhas bancárias etc. Trata-se de uma terminologia nova para definir uma "arte" muito antiga. O emprego da "Engenharia Social" envolve a capacidade de enganar pessoas, aproveitar-se de sua ingenuidade, fazê-las descuidar de procedimentos de segurança básicos – em última instância – ações que qualquer agente de operações de um serviço de inteligência (ou "espião") já vem praticando há muito tempo.

FONTES: Em inteligência, considera-se fonte a origem de onde provém o informe. A fonte pode ser uma pessoa, organização, publicação, documento, página da WEB etc.

HACKER: Entusiasta do trabalho com computadores, programação ou transmissão de dados. Normalmente dotado de grandes conhecimentos, na realidade é um "problem solver", ou seja, aquele que resolve problemas. Como um desafio às suas capacidades técnicas, alguns se dedicam a penetrar os códigos de comunicação de outros sistemas e, hoje, já é comum encontrar "hackers" prestando consultoria na área de segurança de redes e sistemas.

INFILTRAÇÃO: A infiltração é um dos recursos utilizados pelos órgãos de inteligência para a obtenção de informes. Consiste em introduzir um elemento em contato com pessoas ou grupo de pessoas, com o objetivo de coletar dados. É a infiltração de espiões. Trata-se de uma ação muito elaborada e deve haver um processo delicado de seleção e treinamento do infiltrado. Em seus livros "ESCOLA DE ESPIÕES" e "OS SUBVERSIVOS", Bernard Hutton pormenoriza os cuidados dos soviéticos na escolha e na formação dos agentes que seriam infiltrados no ocidente. Após selecionar os elementos, física, intelectual e psicologicamente mais adequados, seguia-se o confinamento em pequenas cidades-escola, cópias, o mais fiel que se podia reproduzir, de cidades dos Estados Unidos, Grã-Bretanha, Canadá, Escandinávia, França ou Itália. O treinamento era ministrado sob forma de "completa imersão", em que o aluno apenas se comunicava no idioma estrangeiro, aprendia sobre

as respectivas culturas, familiarizava-se com as publicações, alimentava-se, tudo de forma a poder se passar por um cidadão do país onde seria designado para atuar. Na inteligência empresarial utiliza-se a infiltração de pessoal de confiança no seio dos próprios funcionários da empresa, normalmente com o propósito de detectar falhas de segurança, ou como auxiliar em processos investigativos internos.

INFORMAÇÃO: Trata-se do informe que foi devidamente avaliado, apurado e processado, de forma a constituir-se em um conhecimento preciso e válido o suficiente para ser utilizado em um processo decisório. Na Inteligência Empresarial, o termo abrange um grande volume de conhecimentos, que vão facilitar a atividade de gestão.

INFORME: O termo refere-se à "matéria prima" da INFORMAÇÃO. Os informes se constituem numa primeira etapa da elaboração do conhecimento acerca de um determinado assunto. O conhecimento parcial, em estado bruto, contido nos informes, oriundo das mais diversas fontes, é estudado e vai compor um produto mais consistente, completo, voltado para as necessidades de quem detém o processo decisório.

INTELIGÊNCIA COMPETITIVA: Seu objetivo principal é "proporcionar aos executivos uma sistemática de coleta e análise de informações públicas sobre os concorrentes ou sobre o mercado em geral, auxiliando na tomada de decisões". Constitui-se numa atividade de gestão estratégica da informação, a qual tem como objetivo permitir que os gestores, tomadores de decisão, antecipem-se às tendências dos mercados e a evolução da concorrência, detectem e avaliem ameaças e ações ofensivas e defensivas mais adaptadas às estratégias de desenvolvimento da empresa. Trata-se de realizar uma coleta de informações ostensivas sobre os concorrentes, fornecedores e clientes, visando, com a mesma, obter um apoio às necessidades organizacionais, avaliando o resultado desta coleta e fazendo com que tais informações cheguem até quem delas necessite no âmbito da organização, tudo como objetivo alcançar vantagem competitiva. Este ramo de atividade se pretende escrupulosamente ético e não está associado à prática de atividades ilegais, tais como espionagem ou roubo de informações comerciais.

INTOXICAÇÃO: Produto de uma ação de contrainteligência. Por meio da desinformação, consiste em levar o adversário a conclusões falsas. É o emprego judicioso de uma mentira útil, quer nos ouvidos do homem, no espírito do povo ou nas deliberações da empresa ou governo que se pretenda induzir ao erro.

VACINAÇÃO ANTIVÍRUS: Programa de proteção eletrônica contra a introdução de um comando destrutivo no software de uma rede, quer por meio de disquetes, CDs ou mesmo através das linhas de comunicações. Como os vírus variam em formas, padrões e complexidade, existe a necessidade de uma constante atualização dos programas antivírus, assumindo, contudo, que nem a melhor das vacinas pode garantir "100%" de segurança.

VAZAMENTO: Consiste na divulgação indevida (ou não autorizada) de segredo ou um assunto acerca do qual se pretenda manter sigilo.

VIGILÂNCIA: Consiste em manter determinado local, objeto, pessoa ou canal de comunicação sob observação constante. Utiliza-se de recursos humanos (agente) e técnicos (microfones/transmissores, máquinas fotográficas e câmeras dissimuladas de TV). Pode ser fixa ou móvel e é muito utilizada na Inteligência Empresarial com o propósito de detectar falhas na segurança e elucidar delitos ocorridos nas dependências da empresa.

VÍRUS: Programa de software que, quando carregado em um sistema de computador, incorpora-se aos programas existentes, destruindo arquivos, interrompendo ou provocando erros no processamento.

REFERÊNCIAS BIBLIOGRÁFICAS E INDICAÇÕES PARA LEITURA:

1) BARRAL, Jean e LANGELAAN, George. "ESPIONAGEM INDUSTRIAL", Editora Expressão e Cultura, Rio de Janeiro, 1970;
2) BECKET, Henry S.A. "THE DICTIONARY OF ESPIONAGE", Dell Publishing Co. Inc., New York, USA, 1986;
3) BERGIER, Jacques. "A ATUAL GUERRA SECRETA", Editora Expressão e Cultura, Rio de Janeiro, 1969;

4) BERGIER, Jacques. "O ESPIÃO INDUSTRIAL", Editora Nosso Tempo, Rio de Janeiro, 1980;

5) BROWN, Robert. "ESPIONAGEM ELETRÔNICA", Agents Editores Ltda, Rio de Janeiro, 1977;

6) DVIR, Avi. "ESPIONAGEM EMPRESARIAL", Novatec Editora, São Paulo, 2004;

7) FARAGO, Ladilas. "O MUNDO DA ESPIONAGEM", DINAL – Distribuidora Nacional de Livros ltda, Rio de Janeiro, 1966;

8) HUTTON, Bernard J. "ESCOLA DE ESPIÕES", Editora Forense, Rio de Janeiro, 1968;

9) HUTTON, Bernard J. "OS SUBVERSIVOS", Editora Artenova, Rio de Janeiro, 1972;

10) KENT, Sherman. "INFORMAÇÕES ESTRATÉGICAS", Biblioteca do Exército Editora, Rio de Janeiro, 1967;

11) McGARVEY, Patrick J. "C.I.A. – MITO E LOUCURA", Editora Artenova, Rio de Janeiro, 1976;

12) PLATT, Washington. "A PRODUÇÃO DE INFORMAÇÕES ESTRATÉGICAS", Editora Agir , Rio de Janeiro, 1967;

13) PRESCOTT, John E. e MILLER, Stephen H. "INTELIGÊNCIA COMPETITIVA NA PRÁTICA", Editora Campus, Rio de Janeiro, 2002;

14) RAVIV, Dan e MELMAN, Yossi. "TODO ESPIÃO UM PRÍNCIPE – A HISTÓRIA DO SERVIÇO SECRETO DE ISRAEL", Imago Editora, Rio de Janeiro, 1991;

15) SCHÖN, Bernhard Wolfgang. "O UNIVERSO DAS ESCUTAS ELETRÔNICAS", Editora Saber ltda, São Paulo, 1993;

16) SHANNON, M. L. "DON´T BUG ME – THE LATEST HIGH TECH SPY METHODS", Palldin Press, Colorado, USA, 1992;

17) STEVENSON, Wiliam. "UM HOMEM CHAMADO INTRÉPIDO", Editora Record, Rio de Janeiro, 1978;

18) VAITSMAN, Hélio Santiago. "INTELIGÊNCIA EMPRESARIAL", Editora Interciência, Rio de Janeiro, 2001;

19) WRIGHT, Peter. "CAÇADOR DE ESPIÕES", Editora Bertrand Brasil S.A., Rio de Janeiro, 1988;

20) WHIITING, Charles. "GEHLEN, UM GÊNIO DA INFORMAÇÃO", Biblioteca do Exército Editora, Rio de Janeiro, 1986;

VINICIUS DOMINGUES CAVALCANTE, CPP

Consultor em segurança e um dos profissionais internacionalmente certificados pela ASIS no Brasil, em 2004. Desde 1985, integra a Diretoria de Segurança da Câmara Municipal do Rio de Janeiro. Especializado em segurança física de estabelecimentos e em segurança pessoal de dignitários, é estudioso de temas como planejamentos de segurança física, contra-terrorismo e inteligência. Atua na segurança de pessoas de notável projeção bem como treinou efetivos de segurança pessoal de diversas instituições públicas e privadas. Palestrante convidado em cursos na PMERJ, ACADEPOL (RJ), SENASP e Centro Regional das Nações Unidas para a Paz, o Desarmamento e o Desenvolvimento Social na América Latina e Caribe (UN-Lirec). Instrutor nos Cursos de Inteligência, de Operações e de Análise de Inteligência, da Subsecretaria de Inteligência da Secretaria de Segurança Pública do Estado do Rio de Janeiro. Articulista em publicações especializadas em segurança do Brasil e do exterior, como o JORNAL DA SEGURANÇA, as revistas PROTEGER, SECURITY, SEGURANÇA PRIVADA, REVISTA SESVESP, TECNOLOGIA E DEFESA no Brasil, bem como SEGURIDAD LATINA e GLOBAL ENFORCEMENT REVIEW, nos Estados Unidos, e INTERNATIONAL FIRE AND SECURITY REVIEW, na Grã-Bretanha, com mais de 50 textos publicados. É colaborador nos portais "on-line" FIREPOWER, SECURITY GATE, SEGURED.COM, FORO DE SEGURIDAD, DEFESA NET e no Blog DIÁRIO DE UM POLICIAL MILITAR

ABSEG

Associação Brasileira de Profissionais de Segurança
www. abseg.com.br - E-mail: abseg@abseg.com.br -

R. Bernardino Fanganiello, 691 - 3o andar
Casa Verde - SP - CEP: 02512-000
(11)3255.6573

ABSEG
ASSOCIAÇÃO BRASILEIRA DE PROFISSIONAIS DE SEGURANÇA