SEGURANÇA NA INDÚSTRIA

DEBATES SOBRE ESTRATÉGIA E GESTÃO

COMPILAÇÃO DO SEMINÁRIO
DE SEGURANÇA NA INDÚSTRIA
21 e 22 de junho de 2016

FIESP CIESP

Federação das Indústrias do Estado de São Paulo (Fiesp)
Centro das Indústrias do Estado de São Paulo (Ciesp)

SEGURANÇA NA INDÚSTRIA

DEBATES SOBRE ESTRATÉGIA E GESTÃO

COMPILAÇÃO DO SEMINÁRIO
DE SEGURANÇA NA INDÚSTRIA
21 e 22 de junho de 2016

1ª Edição

Federação das Indústrias do Estado de São Paulo (Fiesp)
Centro das Indústrias do Estado de São Paulo (Ciesp)
2017

REALIZAÇÃO

Federação das Indústrias do Estado de São Paulo (Fiesp)

Departamento de Segurança (Deseg-Fiesp)

Diretor Titular (Deseg-Fiesp): Ricardo Lerner

CONCEPÇÃO E DESENVOLVIMENTO

Associação Brasileira dos Profissionais de Segurança (Abseg)

Coordenação Geral: Tatiana Diniz – CPP, ASE

Coordenação Técnica: Marcy José de Campos Verde – CPP, ADS

Coordenação Fiesp: Ricardo Franco Coelho

Redação: Lilian Ferracini

PRODUÇÃO EDITORIAL

Edição, preparação e revisão: Karina Sávio

Projeto gráfico e diagramação: André Tamane

Dados Internacionais de Catalogação na Publicação (CIP)

FIESP,

Segurança na Indústria : debates sobre estratégia e gestão / FIESP. – São Paulo : FIESP, 2017.

118 p. : il. : fotos.

Compilação do Seminário de Segurança na Indústria, 21 e 22 de junho de 2016.

Também disponível em versão eletrônica.

ISBN 978-85-7201-026-9

1. Saúde e Segurança no Trabalho 2. Segurança na Indústria I. Título.

CDD: 331.2554

Bibliotecária responsável: Enisete Malaquias CRB-8 5821

Índice para Catálogo Sistemático

1. Saúde e Segurança no trabalho

2. Segurança na Indústria

O cenário mundial exige que as empresas invistam em uma gestão especializada, com grande produção de conhecimento, buscando superar os obstáculos do mercado. Nesta luta diária por competitividade, as empresas brasileiras encontram uma camada adicional de custos de segurança que as coloca em desvantagem no mercado internacional.

Pensando nesta questão, a Federação das Indústrias do Estado de São Paulo (Fiesp) – por meio de seu Departamento de Segurança (Deseg) – reuniu especialistas com vasta experiência na área de segurança privada para a publicação deste livro, que traz importantes discussões sobre o complexo cenário da segurança no Brasil e os desafios que seus gestores enfrentam nos dias de hoje.

As leis que afetam o planejamento de segurança das empresas, as normas reguladoras, os riscos enfrentados pelos produtores de bens de consumo e a ética que permeia todas essas áreas estão retratadas nesta publicação, com a opinião dos especialistas que estão à frente das operações mais complexas de segurança.

Mais uma vez a Fiesp sai na frente no debate de temas de extrema relevância para o setor industrial e sua cadeia produtiva, reunindo o que há de mais atual e inovador e levando esse conhecimento para toda a sociedade.

Paulo Skaf

Presidente da Federação das Indústrias do Estado de São Paulo (Fiesp) e do Centro das Indústrias do Estado de São Paulo (Ciesp)

Em 2017, a Associação Brasileira de Profissionais de Segurança (Abseg) completará 12 anos de atuação no país, promovendo reconhecimento, capacitação, aperfeiçoamento e desenvolvimento profissional de todos que atuam no segmento de segurança.

A história demonstra que as ações de proteção e segurança se ajustam constantemente, a fim de se tornarem compatíveis à realidade socioeconômica e cultural de cada época. Atualmente, com os avanços tecnológicos em informática e sistemas eletrônicos, gestores e consultores de segurança necessitam de formação contínua. A própria arquitetura tem criado edificações que consideram a segurança, gerando novas demandas de perfil para os profissionais da área. Outra tendência clara é a convergência de segurança física, segurança lógica e gestão de riscos.

Prevenir perdas é um importante fator estratégico para as organizações. Aquelas que melhor controlam suas perdas têm mais competitividade e diminuem incertezas relacionadas a seus objetivos. Cresce no ambiente de negócios a consciência de que a segurança patrimonial deve ser vista como função estratégica. Isso se evidencia com a ascensão das posições do gestor de segurança na estrutura das organizações, baseada na formação e capacitação profissionais. É fundamental que o profissional de segurança esteja preparado para enfrentar os desafios e aproveitar as grandes oportunidades. Formação, capacitação e obtenção de conhecimento são alicerces para a construção de uma carreira sólida e promissora. O Congresso de Segurança na Indústria, em parceria com a Federação das Indústrias do Estado de São Paulo (Fiesp), por meio do Departamento de Segurança (Deseg), é prova de que essa matéria está sendo cada vez mais explorada nas empresas, sobretudo na Indústria. Diferentemente das empresas de serviço, a Indústria possui ativos físicos e estrutura logística que demandam ainda mais os serviços de proteção. Gerenciar riscos passa a ser fator crítico de sucesso nesse segmento de mercado.

A geração de conhecimento na área de segurança tem sido intensa nos últimos anos, em todos os aspectos, da segurança física à segurança da informação, passando pela pública, do trabalho, pessoal, do meio ambiente, gestão de riscos, *compliance*, prevenção de perdas e outras áreas correlatas, e é preciso tornar esse conhecimento disponível para os profissionais que atuam no setor e para empresas e empresários. Por esses motivos, a Abseg agradece à Fiesp pela parceria e ratifica seu interesse em seguir contribuindo com a Indústria e a sociedade brasileira.

Tácito Augusto Silva Leite

Presidente da Associação Brasileira de Profissionais de Segurança (Abseg)

ÍNDICE

APRESENTAÇÃO

Em um momento crítico e decisivo, como é o de crise econômica e política pelo qual passa nosso país, a superação depende de esforços que vão além da produção e da comercialização de seus produtos. O foco volta-se à diminuição das perdas, uma vez que isso permite a maximização dos lucros, fundamentais ao aumento da competitividade e à consequente continuidade da Indústria.

Já houve, por parte das indústrias, uma mobilização no sentido de diminuir custos e gastos, resta ainda trabalhar para a diminuição das perdas ligadas aos furtos, desvios e roubos, às fraudes, ao contrabando/descaminho e à pirataria (contrafação/falsificação); tal esforço encontra certa resistência por exigir a revisão de processos.

Tendo este cenário em vista, a Federação das Indústrias do Estado de São Paulo (Fiesp) promoveu – em parceria com a Associação Brasileira dos Profissionais de Segurança (Abseg) – o **Congresso de Segurança na Indústria**.

Em dois dias de evento, que contou com palestras e mesas redondas com profissionais de notório conhecimento em suas áreas de atuação, o objetivo foi levar ao público informações relevantes sobre a situação atual da Segurança Privada no Brasil, bem como o levantamento de cenários e a proposição de soluções para que a segurança das indústrias seja pensada e implementada de forma a não ser uma fonte de custo, mas sim uma forma de maximização dos lucros, em razão da diminuição das perdas.

Para se chegar a esse formato e poder contar com a participação de grandes profissionais, tanto do Brasil quanto do México, foram realizadas diversas reuniões de planejamento, a fim de trazer profissionais com diferentes focos de atuação. Tal posicionamento foi tomado para que se pudesse apresentar diversos pontos de vista, de modo que o material refletisse a realidade e trouxesse soluções plenamente aplicáveis tanto tática como tecnicamente, com base na legislação vigente e nas melhores práticas mundiais.

De acordo com Ricardo Lerner, vice-presidente da Fiesp e diretor titular do Departamento de Segurança (Deseg-Fiesp), o evento foi "uma oportunidade de avançar nos grandes temas da área de segurança. Trabalhamos para contribuir não só com a indústria, mas com a sociedade, em debater iniciativas que visam à segurança".

O Presidente da Abseg, Tácito Leite, expôs como o tema segurança pode contribuir dentro das organizações com o desenvolvimento e o aumento da lucratividade: "Falar

de segurança de forma isolada é pouco produtivo, mas abordar o tema de gestão de riscos operacionais – entre eles a segurança – de forma estratégica é mais inteligente e mais eficiente e produtivo para a organização. Antigamente, existia um conceito único de segurança; com o desenvolvimento da sociedade, o conceito foi ampliado e hoje temos segurança patrimonial, segurança das informações, segurança do trabalho, prevenção de perdas, gestão de riscos, *compliance* e uma série de subáreas que significam proteção. Todas elas visam proteger as pessoas e a organização, a segurança total ou segurança integral. Se por um lado, a organização tenta a melhor forma de produzir, de desenvolver suas atividades para atingir seus objetivos, por outro lado, ela tem perdas e quebras de processos; e a área de Segurança Empresarial vem exatamente para melhorar a eficiência da Indústria e diminuir perdas e quebras. Com isso, obtém-se mais eficiência, mais produtividade e maior lucratividade".

Em sua fala, o presidente do Fórum Nacional contra a Pirataria e a Ilegalidade (FNCP), Edson Vismona, apontou que "o momento é oportuno para a discussão de como enfrentar as ameaças externas e internas que estão permanentemente atuando em prejuízo dos interesses dessas empresas e dos interesses nacionais. Nós, do FNCP, temos enfrentado há mais de 10 anos uma forte ameaça externa, que é o mercado ilegal, dos contrabandistas, dos que falsificam, dos que perpetuam práticas ilícitas para obter dinheiro fácil em detrimento das empresas legalmente estabelecidas. Precisamos mostrar à sociedade que esses prejuízos são bilionários e afetam diariamente nossa competitividade e que, se nós não defendermos o mercado legal brasileiro, nossas ameaças e desafios serão cada vez maiores".

Com o combate às perdas como norte para as discussões previstas para os dois dias de seminário, o evento foi dividido em três painéis de debate, apresentados a seguir, cujas ideias foram aprofundadas pelas mesas redondas, com o intuito de definir estratégias para a segurança na Indústria focadas em qualidade, melhores práticas, ética, *compliance* e diminuição de custos e burocracias nas mais diversas esferas, inclusive a tributária.

SEGURANÇA PRIVADA NO BRASIL E NO MUNDO

O foco foi a apresentação da realidade atual do mercado de Segurança Privada no Brasil e sua comparação com as boas práticas mundiais. Dentro deste contexto, foram discutidos tópicos relacionados à formação e às atividades do profissional de Segurança Empresarial, aos programas globais de qualidade, aos modelos de negócios, à contratação de recursos humanos, à percepção, à análise e à mitigação de riscos.

Foi ressaltada a diferença entre a segurança reativa e a proativa, bem como a importância desta diferenciação. Na primeira delas, considerada ultrapassada, os esforços são dedicados à melhoria da segurança, ao cumprimento de programas, à análise de dados de fornecedores, ao plano de continuidade, ao treinamento li-

mitado de equipes de segurança e ao pagamento de multas em caso de sinistros. Já a segurança proativa, mais atual, designa um diretor de Segurança Empresarial e faz avaliações amplas e formais de riscos; a proteção da informação é feita de forma avançada e há a participação em comitês setoriais de segurança para analisar problemas constantes.

ASPECTOS TRIBUTÁRIOS DA SEGURANÇA EMPRESARIAL

Tema complexo, que levou a profundas discussões nas mesas redondas, sendo abordados diversos aspectos do assunto, sempre com um enfoque estratégico da Segurança Empresarial.

Foram discutidos temas ligados ao panorama de riscos na cadeia logística: cenários, Lei dos Portos, matriz de transporte de carga, *performance* logística no Brasil, roubo de carga, transporte marítimo e *International Ship and Port Facility Security Code (ISPS Code)*. Demonstrou-se, também, o mapeamento das cadeias produtivas e de distribuição, bem como o papel e os desafios da Segurança Empresarial, dando especial atenção à garantia da integridade em cada ponto da cadeia logística.

O painel foi encerrado com a importância do Operador Econômico Autorizado (OEA), seus benefícios e encargos para as empresas e suas interfaces com a Segurança Privada.

GOVERNANÇA E *COMPLIANCE* EM GESTÃO DE RISCOS

A abertura do painel debateu como se forma um programa de *compliance*, em que se baseia e quais seus princípios, com comparações entre a antiga e a nova Lei Anticorrupção. Tendo isto como ponto de partida, foram discutidos processos de prevenção de perdas, programas internos de apuração de irregularidades, sindicâncias e comissões de apurações éticas, bem como as dez lições de *compliance* para a Segurança Empresarial.

Os debates entre os profissionais convidados – *experts* nos assuntos – geraram conclusões e sugestões, as quais são apresentadas neste livro – como forma de ampliar e perpetuar os conhecimentos gerados no evento – e levarão às indústrias importantes ferramentas para o desenvolvimento e o aprimoramento de seus departamentos de segurança, de forma a torná-los ainda mais estratégicos, os quais, em conjunto com outros departamentos, auxiliarão na diminuição de perdas e no aumento dos lucros da Indústria como um todo em nosso país.

INTRODUÇÃO
CENÁRIO POLÍTICO E ECONÔMICO BRASILEIRO*

* Compilação das falas da Abertura Institucional e Contextualização do Seminário de Segurança na Indústria, realizado no Prédio da Fiesp, em 21 e 22 de junho de 2016.

A palestra inaugural do Congresso teve como pauta a contextualização do cenário político e econômico do Brasil, e foi proferida pelo diretor do Departamento de Pesquisas e Estudos Econômicos da Federação das Indústrias do Estado de São Paulo (Depecon-Fiesp), Paulo Francini, com mediação do jornalista Ricardo Boechat. O diretor fez importante análise da situação econômica da indústria brasileira, fazendo interfaces com a indústria mundial e suas projeções. Em sua fala, demonstrou a queda da participação da indústria brasileira na economia mundial e do país.

No período de 1975 a 1992, a Indústria respondia por 20% do produto interno bruto (PIB) brasileiro. Com a queda iniciada no governo Collor, chegou-se, em 2016, a apenas 11,4% de participação no PIB, ou seja, queda de 40% – o Brasil deixou de ser um país industrializado. Um dos fatores responsáveis por esse processo foi a utilização da taxa de câmbio no combate à inflação.

A questão do emprego na Indústria seguiu a mesma trajetória: de 1985 a 2015, o percentual de pessoal ocupado caiu de 27% para 15%. Portanto, houve redução da dimensão e do peso da Indústria não apenas em termos de geração de riqueza, mas também de emprego.

A participação da Indústria no PIB mundial passou por um período de redução, cujas causas foram maior eficiência, avanço da tecnologia, globalização e o fenômeno China. Assim, a participação da indústria brasileira caiu nacional e internacionalmente ainda mais: em relação ao PIB mundial, a participação da indústria brasileira caiu de 2,5% para 1,5%. Ou seja, o Brasil acumula duas perdas: a própria e a do mundo.

Traçado tal panorama, o Brasil deixou de ser competitivo e uma das causas da desindustrialização, além da questão cambial, foi a perda da competitividade, de tal maneira que produzir um produto no Brasil custa 25% a 30% mais do que em outros lugares. Isso ocorre por haver desajustes em várias áreas: tributação e custo de capital de giro, de energia, de matérias-primas e de infraestrutura. Porém, de acordo com o palestrante, Delfim Neto atribui à taxa de câmbio a causa maior da desindustrialização brasileira. A importação de bens dobrou nos últimos anos com o câmbio desvalorizado, principalmente aqueles de maior valor agregado, como os tecnológicos.

A indústria de transformação é a atividade econômica com maior capacidade de entregar produtos com alto valor agregado. É, ainda, capaz de adicionar alto valor por trabalhador, em especial nos países emergentes em trajetória de desenvolvimento semelhante à do Brasil. Enquanto o valor adicionado médio por trabalhador para o conjunto da economia brasileira é de R$ 37,8 mil, na área de serviços é de R$ 20 mil e na indústria de transformação, de R$ 49,6 mil, em média. Ou seja, com a redução da atividade industrial, tem-se concomitantemente uma redução da produtividade global da economia.

Para o futuro, a perspectiva é de redução no ritmo de queda, um sinal de que a reversão da atividade econômica está se aproximando. O recuo do PIB no primeiro trimestre foi de 0,3%, acima das expectativas de 0,8% de queda. Piorou, porém menos do que se esperava.

A exportação de manufaturados está em crescimento, fruto de uma taxa de câmbio mais razoável. Portanto, 2016 tem o menor resultado negativo comparativo dos últimos anos. Esses são alguns sinais de melhoria e, em 2017, podemos enxergar o início de retomada, de uma variação pequena positiva para a economia como um todo e um pouco mais significativa para a Indústria. Os *drivers* da retomada seriam a redução do risco fiscal, a melhora de confiança de empresários e das famílias, a desaceleração da inflação em curso, a redução da taxa de juros já sinalizada pelo Banco Central e uma recuperação continuada das exportações.

Já o emprego é uma variável complicada, pois em situações de crise é a última a ser impactada, porém também a última a melhorar após a retomada do crescimento. Desse modo, a taxa de desemprego no Brasil, que em 2016 estava em torno de 12,5%, é capaz de chegar a 13,5% em 2017, o que significa termos a terrível situação de 13 milhões de desempregados.

Ao ser questionado sobre o impacto da Justiça do Trabalho na produtividade das empresas, Paulo Francini disse que ela possui uma grande estrutura, e com ela vem também grandes interesses, porque muitas pessoas vivem e trabalham em torno dessa estrutura. No Japão, existem 10 mil ações relacionadas ao trabalho; nos Estados Unidos, 100 mil; e no Brasil, 2,7 milhões, porque é um negócio.

Para complementar os dados, o presidente da Federação Nacional das Empresas de Segurança e Transportes de Valores (Fenavist), Jeferson Nazário, apresentou alguns pontos importantes: “nosso maior problema hoje é a clandestinidade. Muitos se intitulam ‘empresas de segurança’. Com a crise econômica, acabam contratando empresas não autorizadas pela Polícia Federal para exercer segurança, levando insegurança para dentro do seu estabelecimento. A economia afetou muito nosso setor. Sofremos uma perda de 30 mil postos de trabalho de um universo de 700 mil empregos formais só nos últimos 12 meses”.

Ricardo Coelho, diretor do Departamento de Segurança (Deseg-Fiesp), por sua vez, pontuou a existência do "inimigo interno" nas corporações. Segundo ele, o fenômeno já foi estudado por entidades internacionais como a American Society for Industrial Security International (Asis International) e cujo entendimento é um dos requisitos para obtenção de certificações mundiais para profissionais que atuam em segurança e processos antifraude. Tais estudos apontam que nas corporações existem indivíduos que nunca agirão contra a empresa, nunca cometerão fraudes ou ações ilícitas; existem também indivíduos que sempre que tiverem oportunidade agirão contra a empresa e cometerão desvios de conduta; e, no meio desses extremos, existem indivíduos que agirão conforme as circunstâncias. Para esses, o cenário econômico recessivo ou adverso contribuirá como um motivador para o cometimento de atos ilícitos. Por isso, é crível supor que, em um ambiente de adversidade econômica e de iminência de perda de empregos, a probabilidade de surgimento de "inimigos internos", ou seja, pessoas com mais probabilidade de agir contra a corporação a qual pertencem, aumenta consideravelmente.

O presidente do Sindicato das Empresas de Segurança Privada, Segurança Eletrônica e Cursos de Formação do Estado de São Paulo (Sesvesp), João Eliezer Palhuca, fez importante observação sobre o mercado de Segurança Privada no país, estruturando-a em três pilares principais:

- **Setor bancário:** responsável pela contratação de aproximadamente 32% do efetivo legalizado, pois – por ser totalmente regulamentado, normatizado e fiscalizado pela Polícia Federal – não contrata vigilantes não legalizados.
- **Setor público:** responsável pela contratação de cerca de 33% do efetivo total do Brasil, com necessidades de vigilância e segurança nas esferas federal, estadual e distrital/municipal. Por força de normas legais, exceto em prefeituras pequenas e/ou empresas públicas desinformadas, o setor público é obrigado a contratar empresas legalizadas, daí a baixa incidência de contratação não legalizada. Tais órgãos têm conduta alinhada com a legislação vigente e, normalmente, contratam dentro da lei.
- **Setor privado:** com exceção dos bancos, já abordados anteriormente, este setor é responsável pela contratação de aproximadamente 35% do mercado de Segurança Privada. Compreende os três setores da economia, quais sejam: primário (extrativismo, agricultura, pecuária, mineração etc.); secundário (industrial); e terciário (comércio e serviços, como *shoppings*, condomínios, hospitais, hotéis, clubes, escolas etc.).

A Polícia Federal acaba focando sua fiscalização em bancos, órgãos públicos e algumas empresas, quando denunciadas. Todas as demais áreas são terreno fértil para a clandestinidade, principalmente a Indústria, os condomínios, o comércio e os serviços (*shoppings*, lojas, centros de distribuição, hotéis, clubes, hospitais

etc.). É aqui, nesta faixa, que precisamos trabalhar para erradicar a clandestinidade. E nisso a Fiesp pode ajudar, orientando e instruindo seus associados sobre como contratar regularmente e dentro da lei.

Outro problema que afeta negativamente o setor de segurança é a prática de aquisição dos serviços por meio de licitações e pregões eletrônicos. Ricardo Coelho apontou que as licitações deveriam objetivar as aquisições de produtos e serviços com os contratos mais vantajosos para a administração pública, e não simplesmente comprar pelo menor preço, pois este quesito nem sempre é o mais vantajoso. O diretor do Deseg apontou que isso acontece porque o menor preço é o mais fácil e o mais defensável do ponto de vista do pregoeiro, mas que esses agentes deveriam se dispor a analisar melhor as propostas e valorizar os contratos realmente mais vantajosos para o Estado. Igor Pipolo, consultor de segurança e diretor do Deseg, apontou que os editais de licitação deveriam ser mais bem detalhados e explicar como os serviços de segurança devem ser definidos com maior grau de transparência e qualidade.

Com este panorama inicial em mente, foram iniciados os trabalhos com focos temáticos do Seminário de Segurança na Indústria, que serão abordados ao longo dos três capítulos desta obra: Segurança Privada no Brasil e no Mundo; Aspectos Tributários da Segurança Empresarial; e Governança e *Compliance* em Gestão de Risco.

CAPÍTULO 1

SEGURANÇA PRIVADA NO BRASIL E NO MUNDO*

* Compilação dos debates transcorridos durante o painel e a mesa de trabalho de mesmo título do Seminário de Segurança na Indústria, realizado no Prédio da Fiesp, em 21 e 22 de junho de 2016.

CENÁRIO ATUAL

A política de Segurança Pública praticada pelo Estado deve estar pautada na prestação adequada, eficiente e eficaz dos serviços, de modo que os cidadãos e a sociedade tenham seu direito constitucional de sentirem-se protegidos dentro de suas casas e nas ruas garantido.

Por viver um dos piores momentos de insegurança de sua história, o interesse da sociedade brasileira pelo tema da Segurança Privada tem aumentado de forma significativa, muito em decorrência dos números crescentes de crimes cada vez mais graves e requintados em audácia, mostrando o estágio avançado em que se encontra a criminalidade e sua cruel influência na vida da população.

A Segurança Pública e a violência custam ao Brasil cerca de R$ 256 bilhões por ano (o que equivale a 5,4% do produto interno bruto [PIB]), conforme publicado pelo *Anuário Brasileiro de Segurança Pública 2014* (Fórum Brasileiro de Segurança Pública, 2014, p. 7). A perda de aproximadamente 57 mil vidas anuais custa aos cofres R$ 114 bilhões; assim, o governo dispende 1,26% do PIB neste setor, um dos mais altos e ineficientes gastos do mundo. Segundo Igor Pipolo (2016), as informações podem ser provadas por meio de dois pontos-chave: baixo índice de resolução dos crimes (menos de 8% ao ano), o que reflete a impunidade; e taxa de reincidência criminal superior a 70%, segundo o Conselho Nacional de Justiça (CNJ).

A sensação de insegurança afeta todo o país, em especial as cidades mais populosas, colocando a Segurança Pública negativamente em destaque, proporcionando campo fértil para discussões sem fim sobre a solução adequada para o combate à criminalidade, principalmente sobre a eficácia da prevenção de crimes. Por outro lado, enquanto as autoridades não tomam as medidas necessárias para resolver a insegurança, abre-se uma enorme oportunidade para o desenvolvimento e o crescimento do crime em geral.

A criminalidade no Brasil e no mundo tem se modificado e diversificado seu comportamento ao longo dos últimos anos. O crime organizado está cada vez mais estruturado e violento – utilizando-se de tecnologia e muita informação –, parecendo estar sempre à frente das forças de segurança, quer sejam elas públicas ou privadas.

Em um país como o Brasil – com grande desigualdade social, escolaridade, civilidade e cidadania que deixam muito a desejar, fraqueza institucional sistêmica e corrupção endêmica –, a violência só poderia ser epidêmica. É de conhecimento geral que os problemas devem levar em conta alguns passos para sua solução, dentre eles:

- Prioridade para a prevenção (em lugar de repressão).
- Certeza da punição (em lugar de impunidade).
- Qualidade de vida (saúde, lazer, mobilidade, emprego etc.).
- Educação de qualidade.

Na esfera privada, sofremos o impacto direto da falta crônica de Segurança Pública, gerando inúmeras perdas nos setores produtivos, que se tornam menos competitivos sob a ótica da Indústria, refletindo diretamente no bolso do consumidor.

Fraudes, extorsões, corrupção, roubos de carga, explosões de caixas eletrônicos, invasão de *shoppings centers*, assalto a indústrias, condomínios residenciais e/ou comerciais, ônibus, roubos em hotéis, farmácias, hospitais, *shows* e outros tantos crimes em lugares diversos passaram a ser cada vez mais frequentes. Órgãos de inteligência em quase todo mundo são unânimes em indicar que a próxima onda será de ciberataques. Segundo um estudo feito pela Cybersecurity Ventures, os crimes virtuais provocam uma perda anual de US$ 8 bilhões/R$ 28 bilhões às empresas brasileiras, de acordo com informações publicadas em artigo do *Jornal do Brasil* (2016).

A iniciativa privada precisa se adaptar de forma rápida e eficiente à evolução dos crimes, sob pena de impactar diretamente seus negócios. Tal esforço apenas será possível com a ajuda do poder público, pelo fato de haver muito a se fazer e em curto espaço temporal, a fim de que se reverta o *status* atual de criminalidade. Por onde começar? Embora a tarefa seja grande, talvez seja possível delinear algumas reflexões sobre como a Segurança Privada poderá dar sua parcela de contribuição para essa mudança.

A atividade de Segurança Privada tem assumido inegável importância na proteção de pessoas e bens, quer na prevenção, na dissuasão ou na reação aos atos criminosos. Cabe ressaltar que a Segurança Privada e a Segurança Pública não são e nunca foram concorrentes, pois atuam em áreas distintas e complementares. O ideal seria poderem trabalhar de forma integrada, trocando informações e cooperando uma com a outra na prevenção e no combate à criminalidade.

A sociedade reconhece e convive muito bem com a Segurança Privada em aeroportos, eventos, empresas, *shoppings*, escolas e faculdades, transporte de valores, bancos, indústrias, em outros tantos lugares e até mesmo em espaços públicos. Quanto ao papel dos organismos de Segurança Pública, ele é insubstituível, o

qual não se questiona excluir. E o mesmo pode se dizer da Segurança Privada em seu espaço próprio, autorizado por lei, com as prerrogativas e os requisitos que ela define, desenvolvendo uma atividade complementar e igualmente essencial para a proteção da sociedade.

A Segurança Privada no Brasil e no mundo está se organizando por meio de entidades fortes e construindo importantes laços com outras áreas do setor, bem como com o poder público, a fim de oferecer cada vez mais proteção. O amadurecimento do setor passa por iniciativas como a do Seminário de Segurança na Indústria, realizado pela Federação das Indústrias do Estado de São Paulo (Fiesp), que reuniu experientes profissionais para pensar em um amanhã mais seguro e resultou na produção deste material.

Boa parte da defasagem enfrentada pela Segurança Privada se deve à desatualização da Lei nº 7.102/83, que rege o setor. Além disso, o Estado não auxilia a atividade quando impõe pesada burocracia a ser cumprida pelas empresas legalizadas, mas não consegue fiscalizar as empresas ilegais/clandestinas, ou seja, as que vivem à margem desta lei, sem autorização (alvará) do Ministério da Justiça. Aliado a isso, é preciso considerar que segurança é um conceito muito mais amplo do que apenas a atividade de vigilância. Segurança Empresarial é uma expressão que engloba inúmeras atividades, como vigilância patrimonial, prevenção de perdas, segurança da informação, gerenciamento de risco na logística, proteção da marca e *compliance*, para citar alguns exemplos. Quando bem implementada, a segurança deixa de ser custo e se torna investimento, garantindo a continuidade dos negócios e o aumento da lucratividade, em razão das perdas evitadas.

O desafio atual consiste em aperfeiçoar a Segurança Empresarial de forma constante e incansável, para que esteja sempre um passo à frente da criminalidade. No Brasil, a Segurança Privada, em alguns momentos, ainda é reativa. Empresas e executivos não conhecem o potencial de entrega da área de Segurança Empresarial. A segurança é hoje vista como custo, pois o profissional, em geral, não aplica o gerenciamento de risco em sua atividade; assim como a segurança patrimonial, atualmente, representa uma *commodity*[1], cabendo ao prestador ter diferenciais e um preço competitivo.

A área de segurança deve ter poder decisório no processo de contratação e estabelecer critérios técnicos na solicitação de proposta técnica/comercial (RFP, *request for proposal*) aos fornecedores, por meio de um processo de concorrência

[1] Do inglês, produtos de qualidade e características uniformes, não diferenciados de acordo com quem os produziu ou sua origem, sendo seu preço determinado pela oferta e procura internacional. Fonte: *Commodity*. In: **Wikipedia**. Disponível em: https://pt.wikipedia.org/wiki/Commodity. Acesso em: 02/03/2017.

para aquisição de algum produto ou serviço, com o intuito de filtrar empresas que não reúnem capacidade técnica e operacional para o atendimento da solicitação com excelência (por exemplo, solicitar atestados técnicos, de escopo similar, na pré-qualificação de fornecedores).

O risco trabalhista é subsidiário; se o prestador de serviço não pagar seus funcionários, a indústria terá que pagar. É preciso contratar a empresa correta para não pagar duas vezes, sendo de extrema importância que o gestor de segurança faça um gerenciamento/acompanhamento das responsabilidades trabalhistas e previdenciárias em relação ao efetivo terceirizado da respectiva empresa de prestação de serviço de vigilância patrimonial.

A contratação dos serviços de segurança precisa evoluir da contratação de posto de segurança para soluções em segurança. Para isso, é preciso ter uma especificação técnica detalhada, com base na análise de riscos e no planejamento de segurança. A responsabilidade tem que ser compartilhada com o prestador de serviços.

RECOMENDAÇÕES DE BOAS PRÁTICAS

O mercado de segurança no Brasil está em um grande momento de adaptação e aprimoramento. Novas ferramentas e tecnologias estão sendo implantadas. A formação do profissional gestor/administrador dos departamentos de segurança é razoavelmente recente e está se tornando cada vez mais importante para a diminuição dos custos e para o aumento da produtividade da empresa. Há a passagem de um tempo de empirismo para um tempo de mais qualificação e fundamentação teórica, com planejamento, aprimoramento e gestão.

Até pouco tempo atrás, o profissional e os departamentos de segurança eram vistos como “fazem tudo”. Hoje, esses profissionais estão conseguindo definir um escopo mais claro de trabalho, para poderem se dedicar ao que realmente é estratégico. A melhor formação do profissional e a adoção de metodologias reconhecidas internacionalmente, incluindo algumas elencadas neste capítulo, também têm lhes permitido transitar entre os setores estratégicos e táticos com maior profissionalismo.

PLANO DIRETOR DE SEGURANÇA

É muito importante e eficiente elaborar um plano diretor de segurança, pois ele será responsável pela gestão de diferentes pontos, a saber:

- Política de segurança.
- Plano de segurança:

  - Levantamento do local.
  - Fatores críticos de sucesso da organização.
  - Inventário de recursos.
  - Análise de risco.
  - Ocorrências internas e policiais.
  - Plano de melhorias (custo *versus* benefício).
  - Orçamentos comerciais.
- Procedimentos.
- Padronização.
- Programa de capacitação continuada.
- Auditoria de segurança.

STANDARDS E CERTIFICAÇÕES

Há uma tendência no mercado mundial para a busca de formação acadêmica (graduação e pós-graduação e MBA específicos na área de Segurança Empresarial), certificações internacionais e nacionais, *guidelines* (diretrizes) e *standards* (procedimentos). Tais ferramentas permitem a uniformização de processos e a padronização de atividades, aumentando a produtividade das equipes e o nível de segurança como um todo. O Brasil está começando a ter um contingente mínimo de profissionais certificados e conhecedores das ferramentas de gestão. Todos os profissionais devem ser incentivados e amparados para que se certifiquem e conheçam tais ferramentas, já que, dessa forma, trarão às empresas maior profissionalização à gestão da Segurança Empresarial, com ganhos diretos à produtividade, à redução de perdas e à proteção dos fatores críticos de sucesso, o que, vale dizer, é de fundamental importância em épocas de comunicação via *web*, em que as informações positivas, mas principalmente as negativas, correm o mundo em questão de minutos.

Standards, termos e certificações citados ao longo do texto são elencadas a seguir, em ordem alfabética, com dados sobre sua criação:

- **American Society for Industrial Security International (Asis International):** associação criada nos Estados Unidos, em 1955, com 39 mil associados no mundo. Mantém três certificações: desde 1977, certificação com foco em gerenciamento de segurança (CPP, *Certified Protection Professional*); desde 2002, certificações com foco em segurança física (PSP, *Physical Security Professional*) e em investigação (PCI, *Professional Certified Investigator*). Mantém um MBA Wharton/Asis na Philadelphia, PA. Há dois escritórios no Brasil, em São Paulo e no Rio de Janeiro. Para mais informações, acesse: www.asisonline.org.
- **Association of Certified Fraud Examiners (ACFE):** criada nos Estados Unidos, mantém a certificação *Certified Fraud Examiner* (CFE), com foco em fraudes.

- ***Balanced Scorecard* (BSC):** metodologia de medição e gestão de desempenho desenvolvida pelos professores da Harvard Business School (HBS), Robert Kaplan e David Norton, em 1992.
- ***Bribery Act 2010*:** legislação britânica antissuborno.
- ***Budget*:** orçamento.
- ***Business Continuation Planning* (BCP):** plano de continuidade de negócios.
- ***Business Impact Analysis* (BIA):** análise de impacto nos negócios.
- ***Business plan*:** plano de negócios.
- ***Chief executive officer* (CEO):** é o cargo mais alto da empresa ou presidente.
- **Ciclo PDCA:** processo contínuo de *plan* (planejar/estabelecer), *do* (fazer/implementar e operar), *check* (checar/monitorar e analisar criticamente), *act* (agir/manter e melhorar).
- ***Core business*:** negócio principal da empresa.
- ***Due dilligence*:** diligência prévia.
- ***Foreign Corrupt Practices Act* (FCPA):** é uma lei federal norte-americana, promulgada em 1977, que visa combater a corrupção transnacional por determinadas pessoas ou entidades relacionadas aos Estados Unidos. Possui duas disposições principais: contábeis e antissuborno.
- **Gestão de continuidade dos negócios (GCN)**.
- **Information System Audit and Control Association (Isaca):** associação americana com foco na segurança da informação, fundada em 1969, sem fins lucrativos, com 140.000 profissionais em 180 países, com escritório no Brasil. Mantém quatro certificações: *Certified Information Security Manager* (Cism), *Certified Information Systems Auditor* (Cisa), *Certified in the Governance of Enterprise IT* (CGEIT) e *Certified in Risk and Information Systems Control* (Crisc).
- **International Information System Security Certification Consortium (ISC)^2:** associação americana com foco na segurança da informação. Mantém quatro certificações: *Certified Information System Security Professional* (CISSP), *System Security Certified Practitioner* (SSCP), *Certified Cloud Security Professional* (CCSP) e *Health Care Information Security and Privacy Practitioner* (HCISSP).
- **ISO 9.000:** grupo de normas técnicas padronizadas mundialmente, que estabelece um modelo de gestão da segurança das informações para organizações em geral. A International Organization for Standardization (ISO) é uma organização não governamental, fundada em 1947, em Genebra, presente em cerca de 189 países.
- **ISO 22.301:** grupo de normas técnicas padronizadas mundialmente, que estabelece um modelo de gestão da continuidade de negócios para organizações em geral; foram publicadas em junho de 2013.
- **ISO 27.000:** grupo de normas técnicas padronizadas mundialmente, que estabelece um modelo de gestão da segurança da informação para organizações em geral; foram publicadas em outubro de 2005.
- **ISO 28.000:** grupo de normas técnicas padronizadas mundialmente, que estabelece um modelo de gestão da segurança nas cadeias de suprimentos para organizações em geral; foram publicadas em junho de 2009.

- **ISO 31.000:** grupo de normas técnicas padronizadas mundialmente, que estabelece um modelo de gestão de risco para organizações em geral; foram publicadas em novembro de 2009.
- **ISO 37.000:** grupo de normas técnicas padronizadas mundialmente, que estabelece um modelo de gestão anticorrupção para organizações em geral, com previsão de publicação em 2017.
- **Lei Sarbanes-Oxley (SOX, *Sarbanes-Oxley Act*):** é uma lei estadunidense, assinada em 30 de julho de 2002, pelo senador Paul Sarbanes (democrata de Maryland) e pelo deputado Michael Oxley (republicano de Ohio). Foi criada para evitar a fuga de investimentos oriunda da insegurança relativa à governança das empresas; visa à criação de mecanismo de auditoria e segurança adequado[2].
- **Leilão reverso:** uma empresa ou agência do governo, por meio de sua área de compras ou suprimentos, a qual deseja comprar itens, faz uma solicitação de cotação; fornecedores pré-aprovados submetem propostas eletronicamente. Esclarecimentos são feitos por *e-mail* e o vendedor é notificado eletronicamente. Este tipo de leilão é o modelo mais comum de leilão para grandes quantidades de pedidos ou itens de alto custo. O menor lance único vence o leilão.
- **Matriz análise Swot:** forças (*strengths*), fraquezas (*weaknesses*), oportunidades (*opportunities*) e ameaças (*threats*).
- **Project Management Institute (PMI):** associação para profissionais de gerenciamento de projetos. Mantém oito certificações: certificado em gerenciamento de projetos (CAPM, *Certified Associate in Project Management*), profissional de gerenciamento de portfolio (PfMP®, *Portfolio Management Professional*), profissional em análise de negócios do PMI (PMI-PBA®, *PMI Professional in Business Analysis*), profissional de gerenciamento de projetos (PMI-PMP, *PMI's Project Management Professional Certification*), profissional em gerenciamento de cronograma de PMI (PMI-SP, *PMI's Schedule Professional*), profissional em gerenciamento de riscos de PMI (PMI-RMP, *PMI's Risk Management Professional*), profissional de gerenciamento de programas e certificação (PgMP, PMI's *Program Management Professional*) e profissional certificado em métodos ágeis de PMI (PMI-ACP, *PMI's Agile Certified Practitioner*).
- **Retorno sobre investimento (ROI, *return on investment*):** também chamado de taxa de retorno (ROR, *rate of return*) ou tempo necessário para o retorno do investimento.
- **Six Sigma:** metodologia criada pela Motorola, com foco na gestão, a fim de aumentar a qualidade e os lucros, com base em controles estatísticos.
- **Solicitação de proposta técnica/comercial (RFP, *request for proposal*):** solicitação de proposta aos fornecedores, por meio de um processo de concorrência para aquisição de algum produto ou serviço.
- ***Stakeholders*:** partes que estão diretamente interessadas na atividade da empresa – clientes, acionistas, governo, empregados, fornecedores e sociedade.

---

[2] Lei Sarbannes-Oxley. In: **Wikipedia**. Disponível em: https://pt.wikipedia.org/wiki/Lei_Sarbanes-Oxley. Acesso em: 30/03/2017.

SLA/MÉTRICAS/SLM

O setor de segurança possui uma carência de sistemas de medição e metodologias de contratação, o que acarreta a ausência de dados confiáveis e oficiais, bem como uma falta de sintonia entre o que o cliente espera receber e o que o prestador de serviços pode efetivamente entregar, ou seja, em relação ao serviço pretendido e o efetivamente contratado. Há desconhecimento também sobre o que o prestador de serviços de segurança pode fornecer, havendo, muitas vezes, confusão entre os serviços de Segurança Pública e Segurança Privada.

Nos Estados Unidos, são comumente usados o acordo de nível de serviço (SLA, *service level agreement*), com definição de métricas específicas para diferentes casos, e o gerenciamento do nível de serviço (SLM, *service level management*), para o acompanhamento da entrega do serviço. Lá a empresa é punida se não entregar aquilo que foi acordado, mas também é premiada se atingir níveis pré-estabelecidos no contrato. No Brasil, não é comum o uso do SLA nem do SLM como ferramentas para estabelecer e gerenciar o nível de *performance* a partir de indicadores de desempenho e acordados entre as partes (contratante e contratado). O objetivo desta ferramenta é estabelecer e gerenciar a qualidade do serviço prestado.

A grande função do SLA é servir como um balizador entre o que foi contratado e o que deverá ser fornecido, sendo uma ferramenta de gestão, que, em conjunto com o SLM, permite constante análise e aprimoramento dos serviços. Não deve ser apenas uma ferramenta de punição, mas também uma forma de reconhecimento da qualidade dos serviços entregues.

TECNOLOGIA E INTEGRAÇÃO

Os investimentos em sistemas e segurança precisam ser justificados com estudos de viabilidade e de impacto econômico para a Indústria, ou seja, a implantação de um Sistema Integrado de Segurança precisa estar atrelada à análise e ao gerenciamento de riscos (ABNT NBR ISO 31.000, 2009). Para essas análises serem feitas é preciso conhecer o negócio, as perdas, os impactos e os números que englobam toda a empresa. Para isso, devem ser feitas as seguintes perguntas: em qual local da indústria é mais necessário esse tipo de investimento? Em que área, caso peças ou projetos sejam roubados ou furtados, a produção pode parar? As análises precisam vincular o investimento ao impacto total que causam ao negócio.

Atualmente, nenhum investimento em segurança é aprovado se não tiver um ROI bem justificado, principalmente no atual cenário econômico desfavorável.

O caminho do profissional de segurança é se aprimorar para assumir novas funções dentro da segurança moderna, a qual utiliza recursos tecnológicos para a excelência de sua execução, sabendo justificar o investimento de forma precisa e bem fundamentada. Desta forma, têm-se:

- Sistemas de controle de acesso:
  - Bloqueios baixos (catracas e baias óticas).
  - Bloqueios altos (torniquetes e portas giratórias).
  - Integração ao antecipador de chamadas do elevador.
  - Integração ao sistema de incêndio.
  - Portas giratórias e eclusas com detector de metal.
  - Portal detector de metal ou detector de metal portátil: sorteador aleatório.
  - Máquina de raio X e *scanner* corporal.
  - Leitores de proximidade (*wiegand*, *smart*, comunicação por campo de proximidade [NFC, *near field communication*] e identificação por radiofrequência [RFID, *radiofrequency identification*]);
  - Leitores biométricos (entre outras):
    - Impressão digital.
    - Geometria de mão.
    - Mapa vascular da mão (palma ou costas).
    - Geometria facial.
    - Íris.
  - Leitor *QR-Code*.
- Sistemas de alarme perimetral:
  - Sensores externos de infravermelho passivo (IVP).
  - Sensores de infravermelho ativo (IVA).
  - Cerca eletrificada industrial (6 ou 20 fios).
  - Cabo microfônico.
  - Sensores de impacto/vibração.
- Sistemas de circuito fechado de televisão (CFTV):
  - Câmeras com saída analógica, de alta definição (HD, *high definition*), *Internet Protocol* (IP), 4K ou 8K.
  - Sistemas de gravação.
  - Sistemas de alarme com videoanálise (*video analytics*), análise inteligente de vídeo ou CFTV inteligente, no qual um *software* faz uma análise com parâmetros previamente estabelecidos e aciona alarmes quando esta situação é detectada.
  - Câmeras com reconhecimento ótico de caracteres (ROC), que identifica e armazena placas.
  - Câmeras termais.
  - *Videowall*.
  - *Software* de gestão de vídeo (VMS, *video management system*), que faz o monitoramento em vídeo com várias câmaras diferentes, criando diversos mosaicos de visualização.

- Sistemas de alarme de ambientes:
  - Sensores internos de IVP.
  - Sensores de abertura.
  - Alarme com gerador de neblina (fumaça).
- Sistemas de barreiras:
  - *Bollards*/postes (fixos, removíveis ou hidráulicos).
  - Cancelas.
  - Portões rápidos.
  - Barricadas.
- Sistemas de gerenciamento:
  - Ronda eletrônica *on-line*.
  - *Software* corporativo para viagens nacionais e internacionais, de forma que seja possível acompanhar colaboradores em regiões críticas, adiar ou suspender uma viagem e até mesmo passar recomendações específicas (preventivas e reativas) de segurança.
  - *Softwares* projetados para evidenciar, medir e gerenciar o desempenho das atividades rotineiras de segurança, operados a partir de dispositivos móveis (*smartphones*, *tablets*, *laptops*).
  - Metodologias e sistemas com métricas e indicadores para expressar em números a entrega dos serviços de segurança, propiciando, inclusive, inferências estatísticas sobre tais atividades.
  - Claviculários eletrônicos.
  - Sistemas de rastreamento, bloqueio veicular ou de materiais/carga (serviços gerais de pacote por rádio [GPRS, *general packet radio services*], rádio ou sistema de posicionamento global [GPS, *global positioning system*]).
- Sistemas de *software* que integram subsistemas de segurança eletrônica:
  - Plataforma de segurança integrada (PSIM, *physical security information management*), que agrega *software* de acesso, CFTV, alarmes, incêndio, automação etc.
- Armas não letais:
  - *Spray* de gás pimenta – oleorresina *capsicum* (OC).
  - *Spray* de gás lacrimogênio – clorobenzilideno malononitrilo (CS).
  - Projétil de borracha/munição de elastômero.
  - Armas de energia eletroconduzida de dardos (choques elétricos).
  - Tonfa.
  - Bastão retrátil.
- Centrais de monitoramento:
  - Local.
  - Remota.

PRESTADOR E CONTRATANTE DE SERVIÇOS

Segurança terceirizada, segurança orgânica ou equipes mistas de segurança privada? A decisão sobre a formação das equipes de Segurança Empresarial deve ser discutida e analisada levando-se em conta o porte da indústria, as característica dos produtos manipulados, entre outras variantes.

Deve haver também distinção entre gestão e operação, estando claro que a integração entre ambas é fundamental. Formatos em que a operação se faz por equipes terceirizadas e a gestão por equipes mistas costumam ser os mais eficientes.

Outro ponto bastante útil é o plano de auxílio mútuo (PAM), uma cooperação entre empresas, por meio dos gestores de segurança de determinada localidade. Deste modo, as empresas precisam dimensionar, por meio de seus planos de segurança e de contingência, os recursos próprios e compartilhados/terceirizados, qualificando fornecedores que possam atender às suas demandas.

Deve-se exigir o treinamento constante do corpo de vigilância, bem como a obrigatoriedade de treinamento prevista em contrato. É importante também que se elabore a descrição dos cargos dos agentes de segurança, principalmente terceirizados, a fim de se evitar a confusão de atividades entre os colaboradores.

CULTURA DE PREVENÇÃO DE PERDAS

A segurança deve ser encarada e tratada como um projeto (PMI), por meio do qual as metas e os objetivos sejam definidos de forma clara. Tal projeto deve ser avaliado com base no ROI, ou seja, o investimento somente deve ser feito se valer a pena; aliás, o projeto deve ser feito de forma a fazer o investimento valer a pena.

A participação da alta gerência/direção é fundamental para a implantação de projetos de segurança. Muitas vezes, a implantação desses processos só funciona depois que a diretoria passa a acompanhar e cobrar sua eficácia e resultados e a se sujeitar aos mesmos processos.

SENSO DE RESPONSABILIDADE (*ACCOUNTABILITY*)

O senso de responsabilidade deve ser desenvolvido entre os empregados de todas as áreas, por meio de treinamentos, campanhas de conscientização e cobranças/punições. Os colaboradores devem se acostumar a ter responsabilidade pelos bens da empresa e do posto de trabalho. Se a empresa delegou ao colaborador um recurso, como um *tablet*, um *laptop* ou um *smartphone*, o funcionário tem o dever de cuidar dele como se fosse seu. Se não tiver o mínimo de diligência, ele será responsabilizado e poderá pagar por eventual dano ou perda. Ao se ter este tipo de cuidado, o nível de segurança sobe automaticamente. Deve-se ainda ampliar este senso de responsabilidade a tudo que envolve a empresa; todos de-

vem estar instruídos a informar o responsável sobre atitudes suspeitas, desvios, furto interno e quaisquer outros delitos envolvendo a empresa. Além disso, deve haver a definição formal das responsabilidades de cada um.

SEGURANÇA E ARQUITETURA

É importante que os projetos arquitetônicos das instalações já prevejam as estruturas adequadas para equipamentos e processos de segurança, a fim de assegurar seu melhor desempenho.

Além da participação da segurança nas estruturas físicas das corporações, deve haver a participação em projetos de novas plantas e produtos desde o início de sua concepção, bem como em questões mais complexas, como fusões e aquisições. Assim, parte dos processos de *due dilligence*, por exemplo, podem ficar a cargo dos gestores de segurança, a fim de evitar despesas não previstas.

O PROFISSIONAL

Atualmente, há pessoas atuando na área que estão se profissionalizando, com perfil colaborativo e interativo com as demais áreas da empresa. Os gestores de segurança já ocupam altos cargos de segurança, inclusive como vice-presidentes ou diretores de Segurança Empresarial para um país ou uma região, como a América Latina.

Dentro das corporações, o gestor de segurança é encarado como especialista na função, consultor ou assessor da companhia, e passou a falar a linguagem dos negócios (conceitos como *budget*, ROI, BSC, *risk analysis* etc. fazem agora parte de seu dia a dia). Além disso, sua atuação é multidisciplinar, cuidando da segurança de forma integral (Figura 1.1).

Figura 1.1. Riscos e competências profissionais associados ao profissional de segurança. Adaptado de: UNIVERSITY OF PHOENIX; ASIS INTERNATIONAL. **Security Industry Survey of Risks and Professional Competences**. Disponível em: http://cdn.assets-phoenix.net/content/dam/altcloud/doc/industry/ASIS-Security-report-WEB.pdf. Acesso em: 24/03/2017.

Apesar disso, em alguns setores, o gerente de segurança médio ainda atua focado em gerir equipes de vigilância, em vez de atuar estrategicamente. É necessário atentar para o fato de que o profissional de segurança deve desenhar um modelo de segurança voltado/customizado ao negócio, inserindo-o no planejamento estratégico da organização, o qual atenda a sua missão, visão e valores. Assim, toda a cadeia de serviços de segurança deve ser moldada para atender a esta expectativa. Para tanto, os profissionais de segurança devem buscar mais capacitação, por meio de cursos universitários na área de segurança e MBA de negócios, além de participar de cursos e congressos (nacionais e internacionais) e feiras (nacionais e internacionais).

Ainda existe a ideia de que militares e policiais estão preparados para gerenciar a Segurança Privada. A formação militar e/ou policial pode ajudar, mas é preciso muito mais, tanto que a American Society for Industrial Security International (Asis International) tem um comitê dedicado à preparação dos profissionais em transição da Segurança Pública para a Segurança Privada.

Education (educação) e *Awareness* (consciência) são as únicas ferramentas capazes de ajudar os profissionais de segurança a disseminar seu potencial e alavancar o negócio. As empresas devem se preocupar em criar e manter um plano de carreira para o vigilante, que representa o nível mais básico da segurança, mas que é fundamental ao processo. Geralmente, ele começa como vigilante e termina sua carreira como vigilante.

Os profissionais de segurança terão que trabalhar ainda mais para permanecerem atualizados diante dos fatores sociais, econômicos e políticos, bem como do avanço tecnológico. Criatividade e pensamento estratégico serão fundamentais para antecipar e mitigar as ameaças cada vez mais dinâmicas. Além disso, conhecer os números, os dados da segurança ou a falta deles é o idioma mais eficiente na linguagem dos negócios das empresas.

AMPLIAÇÃO DA ATIVIDADE

Em algumas grandes empresas, a segurança da informação não está mais atrelada à tecnologia da informação (TI), mas à área de gestão de riscos, que trata de forma mais estruturada e holística os riscos da atividade empresarial, como questões atreladas à marca e à reputação, ou seja, como gestão de marca de maneira geral.

Em gestão de riscos, um dos pontos-chave é que o profissional de segurança não deve ser o dono do risco. Muitas vezes, tem-se a tendência de transformá-lo no guardião do potencial problema, responsabilizando-o por ele. Quando se faz isso, mantém-se ou fomenta-se o isolamento e a falta de responsabilidade do negócio.

É necessário inverter essa lógica, compartilhando a responsabilidade com o dono do negócio/departamento, pois quando há risco e não se investe em sua redução ou mitigação, este é transferido a um terceiro (por exemplo, a seguradora). Deve haver um acordo entre o gestor do risco e o dono do negócio/departamento, em que a ocorrência do risco não ocasionará culpa a seu gestor, pois ele foi assumido por ambas as partes. Ao fazer isso, o gestor faz o *business* se preocupar com a segurança também. Muitas vezes, esse compartilhamento de responsabilidade (conforme prevê a metodologia da ISO 31.000, 2009) não acontece.

MEDO, INCERTEZA E DÚVIDA (FUD, *FEAR, UNCERTAINTY AND DOUBT*) *VERSUS* ROI

Antigamente, os gestores de segurança avançavam em seus programas de proteção através da cultura da paranoia, vendendo a sensação de medo. Pode ser que isso aconteça algumas vezes, mas a longo prazo tal atitude não sobrevive. O que sobrevive é o ROI, que justifica o investimento com os retornos recebidos.

REQUISITOS PARA O FUTURO

- É importante que o profissional de segurança seja certificado (por associações reconhecidas nacional e internacionalmente), fale outro idioma e aprenda a linguagem da empresa (dos negócios) e da alta gestão.
- Atualização da nomenclatura: o termo "segurança" associa-se a uma atividade muito operacional, o que não deve ocorrer. Gestor de riscos – apesar de ser muito usado apenas no setor de transporte de cargas – é o que mais se assemelha globalmente às atividades de um profissional de segurança, que hoje se tornou gestor de riscos, devido às diversas facetas da profissão.
- Trabalhar estrategicamente.
- Agir como um líder de negócios.
- Antecipar as necessidades do seu cliente.
- Apoiar sua cultura organizacional, valores e missão, bem como adaptar seu programa de segurança a eles, na medida do possível.
- Ajudar a construir programas de funções inter-relacionadas e não "territoriais". A segurança pode ser um facilitador de ponte.
- PDCA/Matriz Swot: diga, mostre, faça, evidencie e meça. Diferenciar com métricas, indicadores e excelência operacional.
- Encontrar uma maneira de mitigar o risco sem afetar negativamente os objetivos de negócio.
- Falar regularmente com a alta administração sobre seus problemas de segurança e como pode contribuir, mostrando seu valor para a organização.
- Sempre se comunicar em linguagem usada em ambientes de negócios, não utilizar somente termos de segurança.

- Metas de segurança com base em objetivos de negócios: estar pronto para mudar os planos se a organização mudar de direção, e fazê-lo de forma ágil.
- Não permitir que a área de segurança seja invisível ao resto da organização; posicionar-se.
- Segurança gerida como uma empresa: o gestor deve ser responsável por aquilo que tem a oferecer e deve medir a eficácia.
- Desenvolver equipes de alta *performance* e sucessores.
- Lembrar sempre que o principal "elemento operacional" da economia é o recurso humano, devendo-se dispender especial atenção a este.

ISO 31.000

O mercado de segurança ainda não utiliza comumente a ISO 31.000 (2009). Têm-se processos e modelos corporativos que possuem pontos comuns, mas não consideram a ISO 31.000 como modelo. Ainda assim, quando uma empresa usa a ISO 31.000 como suporte para análise de riscos de um cliente, estes são mais bem encarados e assimilados por ter como base uma norma internacional.

O conjunto das normas ainda não é exigido nas empresas e há dúvidas se será amplamente adotado. Em algumas empresas, suas regras internacionais recomendam mais condutas que as próprias normas de qualidade. Porém, no caso das empresas que não possuem nenhuma política de administração de riscos, a ISO 31.000 é um forte ponto de partida.

Conclui-se que a gestão de riscos evoluiu muito nos últimos anos, permitindo sua atuação nas corporações para agregar valor a outros departamentos, principalmente nas empresas multinacionais, chegando a colaborar com o cumprimento de legislações, como SOX e FCPA, que impõem uma série de restrições e observações a empresas que possuem ações em bolsas de valores nos Estados Unidos.

CAPÍTULO 2

ASPECTOS TRIBUTÁRIOS DA SEGURANÇA EMPRESARIAL*

* Compilação dos debates transcorridos durante o painel e a mesa de trabalho de mesmo título do Seminário de Segurança na Indústria, realizado no Prédio da Fiesp, em 21 e 22 de junho de 2016.

A Segurança Empresarial envolve a gestão de todos os riscos que lhe são inerentes, independentemente de sua origem, porque, no limite, eles se tocam e se correlacionam. Eles podem também ser financeiros, podem decorrer da falta de conformidade (*compliance*) nos negócios da empresa ou mesmo da falta de atualização tecnológica e, ainda assim, gerar eventos que parecem ser, num primeiro exame, simplesmente decorrentes da segurança perimetral da planta.

Com este enfoque estratégico, o Congresso abordou o tema Aspectos Tributários da Segurança Empresarial. Os especialistas concentraram-se na cadeia logística do comércio exterior, a qual envolve uma parcela significativa da Indústria e exibe a interface na relação de vários *players* dentro e fora do país, expondo os riscos empresariais e as medidas de segurança adotadas, inclusive alfandegárias.

Dentro da sequência do tema abordado, inicialmente foi apresentado o panorama de riscos na cadeia logística, concepções, cenários e programas de segurança, sempre comparando a situação brasileira ao que é praticado no mundo, seja em gerenciamento dos portos, matriz de transporte da carga, roubos de carga, nos reflexos da corrupção e demais ameaças, incluindo o terror. Tratou-se também do diferencial competitivo da cadeia logística bem administrada, proporcionando rapidez, redução de estoques e de custos, melhor disposição e armazenamento de produtos, garantia de suporte em cada elo e interação com agentes preparados e que garantam a segurança do conjunto.

Em seguida, foi apresentado o mapeamento das cadeias produtiva e de distribuição, bem como o papel e os desafios da segurança. Em face da complexidade da cadeia é absolutamente necessária a implementação das bases para sua proteção, através do controle das unidades de carga, do acesso físico aos produtos em comercialização, da segurança e do seu treinamento para garantir a integridade das cargas e das instalações que a acondicionam. Na implementação e gestão dessas bases de proteção ocorre a interface direta com os agentes do Estado e com as diversas empresas ligadas à cadeia, ocasião em que emanam os entraves ao seu bom funcionamento. É também o momento em que deve ser contratada a interveniência de empresas de segurança, transporte, armazenagem, escolta, fornecedores de partes e peças etc. até o atendimento aos clientes finais. No fim das contas, com qualquer destes intervenientes, o foco sempre é na segurança dos negócios, pois o objetivo é a integridade da cadeia logística e do produto final em

si, cuja necessidade de comercialização é a fonte que gera a existência do próprio encadeamento das ações.

E, por fim, como parte de uma solução global a ser buscada incessantemente para os problemas gerados pelo funcionamento de uma cadeia logística de comércio exterior, o painel da mesa 2 apresentou o Programa da Receita Federal do Brasil denominado operador econômico autorizado (OEA). O OEA é um interveniente em operações do comércio exterior que cumpre com determinados requisitos obrigatórios de segurança e *compliance* previamente definidos e que, por tal razão, recebe uma espécie de chancela ou "selo de qualidade" na condição de OEA, ou seja, é certificado pela Receita Federal do Brasil como tal.

Uma vez certificado, muitos procedimentos de checagem de conformidades aduaneiras podem ser simplificados ou até mesmo dispensados para o interveniente OEA, tornando a operação logística mais célere, eficaz e segura. Todos os intervenientes da cadeia logística podem se habilitar à certificação OEA, tais como: importador, fabricante exportador, despachante aduaneiro, transportador, agentes de carga, depositário, operador portuário etc. Quanto maior o número de agentes da cadeia que possuem o certificado, mais segura é a cadeia logística.

A seguir, mais detalhes sobre cada abordagem da pauta temática oferecida pela mesa.

PANORAMA DOS RISCOS DA CADEIA LOGÍSTICA

O bom funcionamento da cadeia logística possui uma interferência positiva na competitividade da Indústria e, por consequência, do país, pois atua diretamente na velocidade da execução do processo de transferência dos produtos com segurança e manutenção de sua integridade.

Todavia, a cadeia logística sempre oferece riscos em potencial, e no Brasil, particularmente, ainda enfrenta graves problemas prospectivos relativos a estes riscos, tanto decorrentes de má gestão quanto do atraso da legislação em vários aspectos, os quais serão relatados a seguir.

INFRAESTRUTURA PORTUÁRIA INADEQUADA

Tão logo houve a promulgação da Lei Federal nº 12.815/2013, a chamada Lei dos Portos, esperava-se que ocorressem medidas de modernização dos portos brasileiros em geral, ganhos de competitividade e redução do chamado custo Brasil. Contudo, ao menos até agora, o que se constatou foi uma retração do volume de movimentação portuária e um aumento no custo Brasil em face a mudanças

trabalhistas e a uma série de efeitos decorrentes que atravancaram os negócios. O argumento do governo para mudar totalmente a lei foi evitar uma colcha de retalhos para a área. Para vários especialistas, porém, o objetivo seria criar uma estrutura que permitisse centralizar as decisões em Brasília, ao mesmo tempo em que as autoridades portuárias (as companhias e docas), os conselhos deliberativos (Conselho de Autoridade Portuária) e a agência reguladora do setor (Agência Nacional de Transportes Aquaviários [Antaq]) fossem esvaziadas, encurtando o caminho das decisões. Fato concreto é que a lei permitiu a criação de terminais privados que podem movimentar suas cargas e de terceiros – o que não existia até então – e também tornou legais terminais privados de uso público em portos organizados administrados por uma autoridade portuária.

Ao mesmo tempo que aumentou a competição, a mudança na lei criou novas incertezas. Os arrendatários que já tinham contratos de arrendamento de terminais dentro dos portos públicos passaram a competir com terminais privados, tanto em portos privados como em portos públicos, com legislações trabalhistas diferentes, fato que feriu o princípio da isonomia. Nos terminais privatizados dentro dos portos públicos, a novidade mais incômoda foi a manutenção da regulação do trabalho com os trabalhadores portuários avulsos (TPA), o que, na prática, aumentou o custo Brasil. Os arrendatários de terminais dentro dos portos públicos são obrigados a contratar trabalhadores (estiva e categorias correlatas) por meio do Órgão Gestor de Mão de Obra (OGMO) vinculado ao porto público, cujo objetivo era fazer com que trabalhadores avulsos fossem priorizados na contratação. Contudo, esta meta mostrou-se inexequível, tanto que o governo autorizou um acordo entre empresas e sindicatos para vinculação de apenas 50% da mão de obra ao OGMO, previsto até fevereiro de 2015, o qual foi prorrogado, trazendo um cenário de desajuste operacional, instabilidade jurídica e aumento do custo Brasil. Assim, o Brasil continua entre os piores países (posição 131 de 148) em termos de qualidade de infraestrutura portuária, segundo o *ranking* do Fórum Econômico Mundial, atrás de países como Iêmen, Costa Rica, Camarões etc. Um balanço da gestão da Secretaria dos Portos (SEP), elaborado há três meses, mostrava que quase todas as metas estabelecidas não haviam sido cumpridas ou foram cumpridas apenas parcialmente. Há ainda os vários problemas das empresas: estruturas precárias, terminais que só operam graças a medidas judiciais, problemas ambientais variados e, finalmente, tão impressionante quanto tudo já exposto, alguns bilhões de reais em investimentos parados.

MATRIZ DE TRANSPORTE DE CARGA CONCENTRADA

O transporte de carga no país está absolutamente concentrado em rodovias, que transportam 61% do volume; seguidas pelas ferrovias, com 21%; pelas aquavias, com 14%; e, finalmente, pelos dutos, com 4%. Estima-se para 2025 uma transformação significativa, alterando a distribuição do transporte para:

rodovias, com 30%; ferrovias, com 35%; aquavias, com 29%; dutos, com 5%; e, finalmente, o transporte aéreo, com 1%. A matriz atual é ultrapassada e condiciona a problemas históricos, como grande frequência de roubo de cargas e greves de caminhoneiros.

ROUBO DE CARGAS

O Brasil é um dos três países de maior risco no mundo para o transporte rodoviário de mercadorias, ao lado de México e África do Sul, com taxas de roubo em ascensão, o que eleva os custos para produtores, consumidores, seguradoras, contribuintes e governo. De acordo com as estatísticas dos governos estaduais, o roubo de carga nas estradas paulistas aumentou 12% em 2014 e 9% em 2015, em relação ao período de 2013. O estado representa mais de 50% de todos os roubos de cargas no Brasil.

O número de impacto econômico de perda para os produtores não é conhecido com precisão por autoridades, analistas e comentaristas, mas as estimativas ficam na casa de dezenas de bilhões ao ano. O Departamento de Polícia Judiciária de São Paulo Interior (Deinter 6 – Santos) registrou no ano de 2014 um total de 272 ocorrências de roubo de cargas no porto de Santos, enquanto somente no primeiro trimestre de 2015 foram registradas 58 ocorrências. O principal alvo das quadrilhas são os veículos transportando cargas de alto valor agregado ou outros com produto atrativo (desde eletrônicos até aparelhos de barbear) nas estradas de acesso ao Porto de Santos. Contudo, os terminais portuários e do retroporto também são alvos. O principal *modus operandi* destas quadrilhas é a fraude documental *versus* física, aproveitando-se de vulnerabilidades nos processos de registro, controles internos e controle de acessos com aliciamento de funcionários, por exemplo. Contudo, casos de invasões a terminais no retroporto com uso da força também foram registrados nos últimos anos.

PIRATARIA NOS PORTOS

A pirataria é hoje um dos grandes problemas encontrados nas atividades de cargas dos portos brasileiros. De episódios isolados, passou a ser uma constante, com eventos regulares e cada vez mais graves. Chegou-se a tal ponto que alguns armadores estão analisando a mudança do porto de descarga no Brasil. Tais eventos têm ocorrido, inclusive, à luz do dia, principalmente nos terminais de contêineres de uso público. Busca-se subtrair todo tipo de mercadoria, com foco em produtos eletrônicos e perfumes, mercadorias de fácil circulação no mercado negro. Essas ações causam grande prejuízo financeiro, prejudicando a imagem do país e aumentando custos de seguros. A fiscalização insipiente nas embarcações de pequeno porte, aliada ao policiamento marítimo insuficiente dos órgãos

de segurança intervenientes – tais como Departamento de Polícia Federal (DPF), Marinha do Brasil (MB) e autoridades portuárias –, propicia um caminho livre para estes criminosos.

CORRUPÇÃO

Segundo o relatório anual para assuntos de governança publicado pelo Banco Mundial desde 1996, há uma curva ascendente no índice que mediu a eficiência no combate à corrupção no Brasil. O índice avaliou 212 países e territórios, e registrou queda descontínua do Brasil desde 2003, tendo o pior índice em 2006, atingindo a pontuação de 47,1, em uma escala de 0 a 100 (em que 100 é a mais positiva), em comparação com alguns países da América Latina, como Chile, Costa Rica e Uruguai, que obtiveram nota 89,8 (BBC Brasil, 2007). Um estudo realizado pela Federação das Indústrias do Estado de São Paulo (Fiesp) apontou que o custo anual da corrupção no país gira em torno de 41,5 e 69,1 bilhões de reais (Fiesp, 2010, p.26).

Outro aspecto importante nesta questão refere-se à impunidade, que dificulta o combate à corrupção. A justiça morosa e privilégios classistas contribuem para a manutenção da impunidade, tendo os portos brasileiros significativa participação neste contexto de corrupção política, assim como as forças públicas de segurança e a população local, influenciadas pela ausência do estado constituído. Prova disso é o caso de corrupção na Petrobras, a maior empresa brasileira, que teve um prejuízo de bilhões de dólares entre desvios e outras perdas financeiras. Diante de todo o cenário de corrupção, diversas manifestações populares ocorreram em todo o território nacional. Assim, o governo federal, pressionado pelo apelo popular, apresentou em março de 2015 ao Congresso Nacional um pacote de medidas de combate à corrupção.

Contudo, a medida mais importante já tomada foi a recente regulamentação da Lei Federal nº 12.846/2013, conhecida como Lei Anticorrupção. Em vigor desde janeiro de 2014, a Lei Anticorrupção destina-se a punir empresas envolvidas em corrupção.

TRÁFICO DE DROGAS

Há uma expansão crescente do tráfico de drogas em todo o território nacional, a despeito da Constituição de 1988 ter classificado a prática como crime inafiançável e sem anistia. É também um dos mais recorrentes crimes a ocorrer entre nações distintas, sendo o Brasil um dos mais importantes entrepostos da rota do tráfico de cocaína para a América do Sul e para a Europa.

Mesmo com o aumento do investimento em tecnologia e a elevação da fiscalização em contêineres, registrou-se um aumento geométrico do número de apreensões. Ou seja, as medidas de combate e de inibição ao tráfico, por enquanto, permitem maior apreensão, mas ainda estão longe de serem suficientes para sanar o problema, pois o crime continua sendo cada vez mais praticado, com a participação efetiva de facções criminosas, principalmente pelo retorno financeiro que proporciona.

ARMAS ILEGAIS

A fragilidade das fronteiras brasileiras favorece a entrada de armas que abastecem o crime organizado no país. Os investimentos do governo federal na reestruturação e priorização de ações de combate ao crime nas fronteiras são insuficientes. Para se ter uma ideia, o porto de Santos constitui-se, atualmente, como a segunda maior porta de entrada de armas ilegais, vindas principalmente dos Estados Unidos e da Europa, estando atrás apenas das áreas de fronteiras.

De 2013 em diante, com a implantação de escaneamento de contêineres, houve queda considerável na apreensão de armas no Porto de Santos. Hoje, cem por cento (100%) do tráfego de importação e exportação para a Europa pelo porto e pelos aeroportos deve passar por *scanner*.

A cadeia logística ao longo da história sempre foi alvo de diversos riscos de fraude, descaminhos, furtos e roubos, entre outros. O fator adicional e crucial em comparação aos expostos anteriormente é a sua atratividade potencial para fins da prática de atos terroristas. Tal situação foi percebida pelos governos em particular e também por organizações não governamentais, e tem recebido especial atenção, particularmente após os eventos terroristas ocorridos em 11 de setembro de 2001, nos Estados Unidos. Desde então, uma série de iniciativas no âmbito da melhoria da segurança da cadeia logística tem sido adotada no mundo todo, principalmente nos Estados Unidos e na Europa. Estes programas podem abranger toda ou parte da cadeia logística. Desta forma, para as empresas, é importante avaliá-los tanto na sua aplicabilidade, como no retorno de investimento de acordo com o modal logístico. Os governos dos países que possuem capítulos destes programas os aliam aos seus planos de segurança na esfera nacional, tratando este tópico como questão estratégica da defesa do país, de maneira que as garantias ou tratativas diferenciadas dadas pelos governos aos participantes dos programas garantam um fluxo logístico adequado, ou seja, com vazão condizente e ainda certificado por processos de segurança dos programas. Para tanto, existem diversos programas, dentre os quais destacam-se: Container Security Initiative (CSI) e Customs-Trade Partnership Against Terrorism (C-TPAT) na América do Norte; operador econômico autorizado (OEA), como definido na Organização Mundial das Aduanas (OMA); certificação ISO 28.000 (2009) – Sistemas de Gestão

de Segurança para a Cadeia Logística. No Brasil, a mais recente demonstração da preocupação do país com a segurança da cadeia logística foi a publicação da Instrução Normativa (IN) RFB nº 1.521/2014, substituída pela IN-RFB nº 1.598/2015, que instituiu o programa brasileiro da OEA, o qual, aliado a outros mecanismos internacionais, apresenta princípios para o fiel controle nas atividades de segurança na cadeia logística.

Enquanto o programa OEA não se consolida e remanescem os demais fatores de risco elencados, a cadeia logística vivenciada na entrada e saída de produtos do país continuará contribuindo para a baixa competitividade e mantendo os níveis de investimento muito abaixo do nível esperado para um país continental como o Brasil.

MAPEAMENTO E SEGURANÇA DA CADEIA LOGÍSTICA

MAPEAMENTO DA CADEIA (FATOS GERADORES DE TRIBUTOS)

Serão elencados os elos da cadeia logística em que a preocupação com a segurança, a integridade da carga e, consequentemente, com o produto final a ser entregue sofrem a interferência direta do panorama de riscos da cadeia de risco até aqui descrita.

Como exemplo, há a importação em que o ciclo se inicia com a identificação do fornecedor e os cuidados nesse processo e na forma de contratação. Adquirido o produto, tem-se o primeiro transporte até o porto de origem, envolvendo empresas transportadoras e seguradoras.

Na sequência inicial, temos o transporte internacional do porto de origem ao porto de chegada. Aqui, a integridade do produto em transação é o aspecto relevante da operação. As ocorrências como danos (avarias), sumiços, desvios, extravios, furtos, inclusão de elemento estranho etc. constituem as possibilidades frequentes nesse trajeto. Por esta razão, podem ser utilizados lacres com sensores que permitem o rastreamento do produto. O transporte pode se dar por via aérea, marítima ou terrestre.

No ponto de chegada no território brasileiro incidem Impostos de Importação (II), sobre Produtos Industrializados (IPI), Programa de Integração Social (PIS), Contribuição para o Financiamento da Seguridade Social (Cofins), sobre Circulação de Mercadorias e Serviços (ICMS) e despesas para a liberação aduaneira de incidentes, inclusive sobre o custo de transporte e do seguro, que também compõem a base de cálculo desses tributos.

Neste rito de passagem pelo ponto de chegada, evidenciam-se vantagens do importador certificado como OEA, já comentado no capítulo anterior. Em face

à celeridade dos desembaraços, ele terá custos de logística menores no Brasil. Aqui, o produto poderá permanecer por um período, onde se acumulam custos de armazenagem e aumento da probabilidade de afetação da sua integridade, tanto por deterioração quanto por ataques de criminosos, por vezes em vista de vazamento de informações.

Havendo a opção do importador para a guarda transitória em um porto seco, insere-se o custo do transporte adicional e da respectiva segurança. Na sequência tanto do porto de chegada quanto do porto seco transitório, haverá novo transporte até o importador e possível armazenamento temporário nas dependências do importador e/ou em um de seus centros de distribuição e, finalmente, o transporte destes para o cliente final. Em todas as fases, há a seleção de parceiros para transporte, para o seguro e para seu armazenamento.

A segurança em seu conceito amplo deve nortear toda a operação do exemplo anterior, o que também se aplica à cadeia exportadora.

SEGURANÇA DOS PRINCIPAIS ELOS DA CADEIA

Quando se fala em segurança em logística, para muitos isso significa pensar na segurança da carga em trânsito, referente, na maioria das vezes, à fase de distribuição com todos os aspectos do gerenciamento de risco envolvidos. Obviamente, nesta fase da logística repousa grande parte das perdas experimentadas pelas empresas, mas infelizmente há outros pontos em que as perdas também são grandes dentro dos processos de logística e, de forma ampla, também de toda a cadeia de suprimento (*supply chain*). A falta de observação do todo pode levar a perdas ainda maiores.

A logística serve de plataforma para o conceito moderno de gerenciamento da cadeia de suprimento, que significa combinar as ações desde o fornecedor de matéria-prima ou peças até o consumidor final, obtendo melhor custo e velocidade na operação, em que a logística é uma fase ou parte do processo. O gerenciamento da cadeia de suprimento vem sendo adotado pela grande maioria das empresas como resposta ou meio de otimizar e diminuir gastos, pois os processos integrados e bem gerenciados podem vir a baixar o custo de produção e trazer outras vantagens, como a diminuição do tempo de produção, armazenagem e distribuição.

As áreas envolvidas necessitam cumprir suas metas de tempo, qualidade, quantidade etc., e certamente não vão cumpri-las sem considerar o fator segurança em todos os processos de recebimento, armazenagem, produção, embalagem e distribuição. Como exemplo, se uma empresa ou seu departamento de logística tem como meta 97% de entregas dentro do prazo, e esta mesma empresa

é assolada por uma série de eventos como roubo em trânsito ou furto interno, dificilmente ela conseguirá entregar no prazo e, por consequência, não cumprirá as metas estabelecidas.

TRANSPORTE DA CARGA

Todos os anos, registram-se perdas de centenas de milhões de reais nos estados brasileiros, e a projeção dos números para este ano indicam mais ou menos as mesmas tendências. Comparando-se o crescimento do número de casos de roubo de 14% no estado de São Paulo com o índice de crescimento da indústria paulista, que fechou 2015 com um recuo de 10,5%, é possível verificar que o aumento dos casos de roubo não se relaciona ao aquecimento de mercado.

O que não fica claro nas pesquisas de roubo de carga verificadas é em que ponto da operação a carga foi roubada. Este tipo de informação é vital para estabelecer quais medidas deverão ser tomadas para proteger não só a área mais afetada, mas também toda a operação de logística. A combinação de dados pode fornecer muito sobre qual a área mais suscetível ao vazamento de informações, voluntário ou não, que precede 100% dos casos planejados de roubo de carga.

Cada fase da logística aplicada ao gerenciamento da cadeia demanda processos e medidas preventivas diferentes. Em algumas, o cliente deve ser parte integrante do processo, em conjunto com o transportador; em outras, o sigilo poderá ser a base do sucesso. O fato é que as medidas adotadas não devem ser estáticas, deve-se variar algum item sempre, pois a rotina é a maior aliada da atividade criminosa, em especial dos informantes de plantão.

ARMAZENAGEM, EMBALAGEM E DISTRIBUIÇÃO DO EMBARCADOR

Pode parecer estranho achar que o furto interno venha influenciar na qualidade e na pontualidade em relação ao cliente. O fato é que se há furto interno, provavelmente há falhas nos processos de controle. Se tais falhas estiverem ocorrendo em áreas pós-produção, como embalagem e estoque, e só forem detectadas quando o cliente receber uma caixa com metade das unidades que deveria receber, isto vai influenciar nas metas de qualidade.

Piores consequências podem trazer os grandes roubos feitos por quadrilhas aos armazéns da fábrica ou de fornecedores de serviços de logística, quando não conseguem ou não querem pegar a carga em trânsito. Normalmente, grande quantidade de mercadoria é roubada e o trabalho para nova produção e atendimento ao cliente em tempo hábil nem sempre é possível.

Estes e outros argumentos devem ser utilizados pela área de segurança para conseguir a colaboração e participação das diversas áreas envolvidas na cadeia de suprimento no que diz respeito à execução e também à divisão do financiamento das ações. E o mais importante: deve-se reconhecer a participação da segurança no atingimento das metas de outras áreas, incluindo o "lucro" obtido na prevenção de perdas. O conhecimento do processo em cada ponto distinto é fundamental para iniciar as discussões sobre qualquer mudança necessária. Normalmente, tal conhecimento é adquirido por normas escritas que quase nunca abordam questões de segurança como fator determinante, e sim alguns poucos itens de controles internos.

A segurança deve participar de todo o planejamento da atividade dentro da cadeia logística, reportando-se diretamente e fazendo parte da alta direção. Deve-se diferenciar se não há processo relativo à segurança ou se há e este não está sendo cumprido. Medidas como controle de acesso, contagem cíclica nas trocas de turno, conferência e pesagem na paletização, entrega ao transportador e prova da entrega, procedimentos de lacres e travas de baú via satélite devem estar previstas por escrito e ser de amplo conhecimento dos envolvidos na operação.

Outras medidas deverão ser adotadas para garantir que a carga chegue ao cliente da mesma forma que deixou a empresa. Quando se trata de entrega porta a porta, consegue-se bons resultados com os processos de lacres numerados, trava baú via satélite e o próprio relatório de rastreamento. O problema aparece quando a carga passa por um ou mais pontos para consolidação ou qualquer outro procedimento. Nesses casos, a participação conjunta das áreas de logística, segurança, transportador e cliente é essencial, como visto mais à frente.

CONTRATAÇÃO DE FORNECEDORES – AUDITORIA PRÉ-CONTRATUAL

Na visão moderna do gerenciamento da cadeia de suprimento são desenvolvidas parcerias que garantem a velocidade e o custo demandado pelo mercado. São identificadas empresas que possam atuar em todas áreas, desde a matéria-prima até a chegada do produto ao cliente. Cada fornecedor deve ser minimamente qualificado tanto no aspecto técnico quando no aspecto de segurança. Por isso, a segurança é solicitada a verificar as condições mínimas de funcionamento, aplicando formulário pertinente de auditoria, se for o caso.

Outra vez se faz presente a importância do trabalho conjunto entre negócio e segurança. Para facilitar as coisas, as auditorias prévias de segurança, bem como as anuais, devem estar previstas no processo de contratação de compras ou logística. Uma boa prática é apresentar às empresas interessadas no serviço e aos participantes do processo de cotação os padrões técnicos e de segurança requeridos pela empresa. Desta forma, quem oferecer a proposta já o fará tendo em vista o investimento a ser feito, se necessário.

A auditoria prévia não deve ser por si só eliminatória, a não ser que os problemas encontrados sejam tão graves que não compensem financeiramente a apresentação de um plano de ações corretivas; a ideia é que ela se torne uma parceria. O que pode ser feito é a visita utilizando padrões mínimos de segurança para cada tipo de empresa. No caso do setor de logística, o formulário mais comum é o padrão da Transported Asset Protection Association (padrão Tapa). No formulário, verifica-se a existência de itens marcados em amarelo; tais itens são mandatórios e devem estar em utilização ou ser implementados a curto prazo. Podem servir de parâmetro para auditoria pré-contratual e emissão de um plano de ação com prazos e responsáveis determinados. Em um futuro próximo, a própria certificação Tapa ou similar, inclusive o certificado OEA da Receita Federal do Brasil (RFB), poderá funcionar como condição para contratação dos serviços.

PROGRAMAS INTERNACIONAIS DE CERTIFICAÇÃO

Algumas práticas no mundo constituem o que há de mais avançado (*benchmarks*) no controle da qualidade e segurança da cadeia logística, principalmente nos aspectos do armazenamento e transporte. A seguir, algumas delas serão descritas sucintamente.

TRANSPORTED ASSET PROTECTION ASSOCIATION (TAPA)

A Tapa nasceu nos anos 1990, com a necessidade das empresas de alta tecnologia dos Estados Unidos em proteger a movimentação e armazenagem de seus valiosos e pequenos componentes. Além das empresas produtoras, hoje também conta com fornecedores da área de logística e outros.

Em sua *home page* (www.tapaonline.org/index.php), é possível encontrar os formulários de auditoria (em inglês) divididos em nove áreas, cada uma delas contendo seus vários subitens, conforme segue:

- **Segurança perimetral:** cobertura por circuito fechado de televisão (CFTV), iluminação, alarme perimetral, janelas, portas e outras aberturas, cercas e portões.
- **Controle de acesso nas áreas de escritório:** controle de acesso entre as instalações e os depósitos.
- **Instalações docas/armazéns:** controle de acesso, acesso limitado à área de docas, área para estocagem de carga de alto valor, área externa próxima das docas e armazém, cobertura por CFTV, alarmes de intrusão, revista de bolsas e outros recipientes, detectores de metal.
- **Sistemas de segurança:** monitoramento do sistema, sistema de alarme, sistema de CFTV, sistema eletrônico de controle de acesso, manutenção do sistema de segurança.

- **Procedimentos de segurança:** procedimentos documentados adequadamente, normas gerais e particulares de cada operação, histórico de antecedentes, processo de demissão (*check list*).
- **Padrões de segurança dos caminhões:** dispositivos adequados de segurança instalados nos caminhões, itinerários e rotas, processo de carga e descarga.
- **Pré-alertas:** avisos de provedor para provedor.
- **Segurança adicional:** treinamento de motoristas, escoltas e respectivo treinamento, rastreamento do veículo (integração homem/equipamento).

Os itens anteriores são avaliados conforme a existência da medida e seu nível de utilização (0 para medida não existente, 1 para a medida geralmente presente, 2 para a medida existente e adotada com a melhor prática e X para subitem não aplicável).

A certificação normalmente é feita por órgão emissor de certificação da International Organization for Standardization (ISO), como o Bureau Veritas Quality international (BVQI), nos Estados Unidos, e a Société Générale de Surveillance (SGS), na Europa, que têm seus auditores treinados pela equipe da Tapa para aplicação do formulário.

BUSINESS ALLIANCE FOR SECURE COMMERCE (BASC)

A coalisão empresarial anticontrabando, também criada nos anos 1990, só que para facilitar o trânsito de mercadorias na fronteira México/Estados Unidos, já está se expandindo para outras partes do mundo. As empresas, assim como na Tapa, pagam por esta certificação, que se foca em contrabando e tráfico internacional de drogas.

A empresa certificada conta com passagem mais rápida de suas mercadorias nas fronteiras e aduanas participantes ou signatárias do acordo de Cartagena, Colômbia. A Basc tem a política e os padrões para implantação de um programa de segurança e suas futuras verificações e recertificações, além de formulário para verificação dos padrões mínimos. A segurança deve ser robusta, não permitindo a entrada de produtos ilegais, utilizando-se, para tanto, de embalagens e caminhões de empresas legais.

Os padrões de segurança são divididos em oito grandes áreas e suas várias subdivisões, a saber:

- **Programa de segurança:** medidas adotadas para proteger uma organização, seus ativos, propriedades, empregados e clientes.
- **Políticas de segurança:** padrões definidos, procedimentos para seleção de pessoal, verificações civil e criminal, relações com autoridades, processos de

registro de irregularidades ou ocorrência suspeitas. As políticas devem estar em local visível para as áreas comuns e detalhadas em cada departamento ou unidade de negócio. Pôsteres e boletins descrevendo a política de segurança devem estar em local visível para os clientes (similar ao processo de certificação ISO).

- **Segurança dos funcionários:** proteger os funcionários em relação ao assédio de grupos organizados para que cooperem com suas atividades ilegais, utilizando seleção adequada, verificação dos dados fornecidos, técnicas de entrevista, integração nas políticas, programas antidroga em local visível, visita bianual à residência de funcionários para acompanhamento de estilo de vida e programas de incentivo para comunicação de atividades suspeitas.
- **Segurança física:** áreas de permanência ou tráfego de cargas, segurança de perímetro, portas, iluminação, controle de chaves e armários, treinamento e perfil do pessoal de segurança, sistema de identificação, conscientização de segurança e treinamento, procedimentos escritos, recebimento e expedição de contêineres vazios e cheios, recebimento e expedição de mercadorias em geral, inspeção de veículos não pertencentes à companhia, guaritas, estacionamentos, comunicações e controles de acesso.
- **Sistemas eletrônicos de segurança:** alarmes antifurto, controle eletrônico de acesso, CFTV.
- **Segurança de dados e documentos:** documentos relativos à carga, políticas de verificação de assinaturas e autorizações, segurança da rede de computadores (senhas, *backup*, segurança física do local etc.).
- **Selos e lacres:** fitas customizadas nas embalagens, lacres numerados e controlados por uma pessoa, tratamento de embalagens vazias, vários *check points* para verificar a integridade dos lacres (incluindo o do caminhão).
- **Alianças estratégicas de segurança:** com fornecedores e clientes em toda a cadeia para verificação dos lacres, políticas, assinaturas, controle de *cicle time*, nomes de responsáveis, processo de comunicação. Deve incluir alianças com órgãos governamentais que também conheçam o processo.

A aliança internacional até agora constituída é formada por:

- Basc Colômbia.
- Basc Costa Rica.
- Basc Equador.
- Basc México.
- Basc Miami.
- Basc Peru.
- Basc Venezuela.
- Aduana da Espanha.
- Aduana da Colômbia.
- Aduana do Equador.

- Serviço de Aduanas dos Estados Unidos.
- Aduana da França.
- Organização Mundial de Aduanas.
- Cámara de Comércio Internacional.
- Organização dos Estados Americanos.

O processo de certificação Basc tem os seguintes passos:

- Solicitação com autoavaliação ou não.
- *Chapter* da Basc decide se continua o processo.
- Auditoria e verificação de requisitos mínimos.
- Classificação *in process* ou ínterim (não atingiram os requisitos mínimos).
- Classificação *certified* (aprovada para se juntar à coalizão).
- Implementação das políticas e recomendações.
- Reavaliação anual.

CUSTOMS-TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

É um programa do governo americano, criado após o evento de 11 de setembro de 2001, com a finalidade de proteger as fronteiras americanas contra a entrada de produtos e materiais ligados ao terrorismo.

O programa é operado e administrado pelo governo dos Estados Unidos através do U. S. Bureau of Customs and Border Protection (CBP) e supõe a participação de cada empresa isoladamente em tratado bilateral (empresa x CBP). O C-TPAT não conta com políticas e padrões de segurança padronizados, como no caso da Basc, fundando-se apenas nos formulários e questionários de autoauditoria. A participação é voluntária e gratuita.

O processo de certificação C-TPAT tem os seguintes passos:

- Contrato de participação (*agreement to voluntarily participate*): assinado pela alta gerência e pelo diretor de operações CBP.
- Empresa apresenta perfil de segurança: questionário de autoavaliação (*supply chain security profile*) em até 60 (sessenta) dias após assinatura do contrato.
- Recomendações CBP segundo o perfil apresentado (*CBP security recommendations*).
- Auditorias internas feitas pela própria empresa.
- Visita de validação CBP, de acordo com o seguinte processo de validação:
  - Sua administração é via internet.
  - Supõe visitas de validação CBP posteriores.
  - Cobre todas as plantas e empresas no mundo da mesma razão social.
  - Integra toda a cadeia de suprimentos da corporação.

A vantagem para a empresa certificada é similar às vantagens da Basc, com fluxo mais rápido de mercadorias exportadas para os Estados Unidos, contando com canais exclusivos na alfândega, as chamadas *fast lines*. Para o Canadá, a combinação de certificações é Partner in Protection (PIP), na mesma linha da Basc + C-TPAT, é igual ao Free and Secure Trade (Fast Canadá). Para o México, utiliza-se a combinação Basc + C-TPAT = Fast México.

Essa combinação de programas e certificações sem dúvida traz benefícios para os Estados Unidos, na medida em que foca seus esforços e atenção na verificação de empresas não certificadas, pois as que possuem certificado já foram verificadas em relação aos processos e são constantemente autoauditadas.

Para as empresas, não restam dúvidas em relação aos benefícios, não apenas em relação ao tempo de ciclo nas exportações, mas também por tornarem muito mais profissionais e robustos seus processos de segurança e logística.

Mesmo quem não é certificado ou não tem interesse em ser pode tirar vantagens seguindo de alguma forma as cartilhas disponíveis na *web*, como as políticas da Basc: http://www.wbasco.org/english/certification.htm.

PROTEÇÃO DA CARGA EM TRÂNSITO, PROTEÇÃO DE INFORMAÇÕES E TEMPO DE RESPOSTA AOS INCIDENTES

Pela inevitável necessidade de emissão de ordens do departamento de vendas, notas fiscais, romaneios, conhecimento de transporte, conhecimento aéreo etc., a proteção de informações em logística integrada à cadeia de suprimento é um tanto quanto difícil e, às vezes, impossível. Outro problema que assola a maioria das empresas é o fechamento mensal, ou seja, a maioria das vendas é faturada na última semana de cada mês, tornando o processo previsível, concentrado e de alto risco. A solução para estes casos não é fácil, depende de entendimentos entre vendas, cliente, logística, finanças e segurança, para que, ao menos, seja diminuída a concentração de entregas em uma mesma semana.

Para diminuir os riscos, o fluxo das informações deve estar estabelecido e nomes devem ser dados aos responsáveis em cada fase: pedido, embalagem, emissão de documentos, responsáveis na transportadora, responsáveis na central de monitoramento, escolta e sua central, expedição da mercadoria, seja diretamente do embarcador, via centro de distribuição ou cargas para consolidação.

A surpresa durante o carregamento do caminhão e antes da liberação ajuda a diminuir o tempo de ação de quadrilhas que aguardam informações. As informações devem estar concentradas em uma ou duas pessoas, as quais informarão aos motoristas qual o destino apenas após o carregamento do caminhão, fazen-

do o mesmo com a escolta. Esta mesma pessoa se encarregará de verificar, através de *check list*, se todas as medidas de segurança privada foram tomadas antes do início da viagem, por exemplo:

- Escolta.
- Comunicação da escolta com sua base.
- Comunicação da escolta com o caminhão.
- Coletes e armamento.
- Comunicação do caminhão com a central da transportadora.
- Telefones de emergência da escolta e do motorista.
- Correto acionamento dos dispositivos de proteção e alarme via satélite.
- Verificação das regras estabelecidas entre empresa e transportadora, considerando o limite de valores por caminhão, horários, número de veículos de escolta etc.

TEMPO DE RESPOSTA AO INCIDENTE EM TRÂNSITO: O CALCANHAR DE AQUILES DA SEGURANÇA

A base do gerenciamento de risco da carga em trânsito se funda basicamente em escolta armada e nas proteções via satélite aliadas às condições da seguradora, ou seja, limites de valores por caminhão, comboios, avaliação dos locais de armazenagem, etc. A legislação pertinente pode ser encontrada nos *sites* do Sindicato das Empresas de Segurança Privada, Segurança Eletrônica e Cursos de Formação do Estado de São Paulo (Sesvesp) e no *site* do Sindicato das Empresas de Escolta do Estado de São Paulo (Semeesp).

Principais falhas encontradas em escoltas:

- Erros de procedimento (em parada, dormindo, posicionamento dentro da viatura, forma de ação em paradas sem revezamento etc.).
- Procedimentos não documentados e auditáveis.
- Falta de documentação para trânsito (interestadual, documento do armamento).
- Falta de plano de ação e resposta claros e treinados (incidentes, quebra, troca de pneu, roubo, procedimentos em paradas etc.).
- Conflito motorista *versus* escolta.
- Falta de centro de gerenciamento de crises/monitoramento dos veículos.
- Ilegalidade/clandestinidade.
- Falta de treinamento específico extra.
- Equipamentos incompletos ou inexistentes (comunicação, coletes, rádios, armamento etc.).
- Falta de supervisão/apoio às escoltas no trajeto.

Exemplos positivos encontrados no mercado:

- Escolta rastreada (via sistema de posicionamento global [GPS, *global positioning system*], serviços gerais de pacote por rádio [GPRS, *general packet radio services*] ou rádio – se possível, por mais de uma dessas tecnologias).

- Central de controle na empresa.
- Acompanhamento via rádio, celular, pontos de controle.
- Postos credenciados para paradas.
- Informação/contrainformação junto ao cliente para coleta de dados.
- Orientações escritas aos vigilantes e motoristas: manuais, legislação, documentos, planos etc.
- Centro de treinamento próprio (mínimo e extras).
- Convênios com helicópteros (com condições de identificação do veículo pelo teto).
- Carro supervisor sem logotipo para apoio, coleta de dados e fiscalização: a legislação prevê que o veículo de escolta deva ser identificado, porém a supervisão não necessariamente precisa. A escolta deve ter com quem contar, pelo menos regionalmente.
- Verificação de novas rotas, fotografia e credenciamento de pontos de parada em conjunto com a transportadora.
- Utilização de dois estepes pela escolta.
- Não há operação de uma mesma equipe na mesma área por muito tempo, e a indicação da rota deve ser dada apenas minutos antes da partida.

EQUIPAMENTOS GERENCIADOS VIA SATÉLITE

Além de utilizar a escolta (às vezes mais de uma), um caminhão pode sair da empresa tomadora sendo monitorado por GPS, com os limites de custo de se pedir o posicionamento a cada 10 minutos ou menos, se necessário. Em alguns casos, esta exigência está registrada em contrato, porém a fiscalização demanda análise dos relatórios de rastreamento. Um dos pontos causadores de problemas para o tempo de resposta é o tipo de transmissão utilizada pela empresa de transporte para receber informações da estação terrena da empresa de monitoramento; deve-se procurar conhecer e saber qual o retardo e os problemas de cada tipo.

Esse mesmo caminhão pode contar ainda com vários dispositivos, a chamada inteligência embarcada, para emitir sinais de abertura das portas, parada não autorizada, sensor no banco do carona, sistema de bloqueio de freios da carreta, trava de baú, trava do pino rei, câmeras, alarmes etc. Tais dispositivos podem e devem funcionar mesmo quando a antena do caminhão perde a visada do satélite, por isso seu conjunto é chamado de inteligência.

Somado a isso tudo há ainda o famoso e quase nunca utilizado botão de pânico. Este botão deveria mudar de nome para “botão de ameaça”, pois a palavra tem força e os motoristas acham que devem utilizá-lo só na hora do pânico, quando já é tarde – o dedo trava e não se aperta mais. Se a escolta tem comunicação com o caminhão e está atenta, sua função é perceber o perigo que os ameaça e acionar o dispositivo ou solicitar ao motorista que o faça, caso ele não tenha percebido algo errado. Depois que a arma está apontada para cada um deles, é provável que

não façam movimento algum para acioná-lo. Outra boa prática é o treinamento, talvez convencimento dos motoristas, de que o caminhão não vai simplesmente travar bem na hora em que se aperta o botão (pelo menos não deveria).

Com todo este aparato, a carga ainda corre risco de ser levada devido ao simples fato de que toda esta tecnologia está ligada à ação do ser humano, além das limitações e deficiências do próprio sistema.

OPERAÇÕES DE CONSOLIDAÇÃO – UTILIZAÇÃO DE MAIS DE UM GALPÃO

Grande parte das operações envolvendo transporte, considerando as dimensões do país, são feitas com base na retirada da carga no embarcador, cuja quantidade não permite a utilização de um caminhão fechado até o cliente final, e posterior consolidação em um depósito. Esta operação nada mais é do que consolidar no mesmo depósito por certo período várias cargas com destino ao mesmo Estado ou itinerário, o que é feito normalmente por um caminhão que faz aquele trajeto todo dia ou duas vezes por semana.

Esta é uma operação que baixa o custo do transporte, porém aumenta o risco, uma vez que expõe o produto a mais uma parada, mais pessoas em contato e mais chances de vazamento de informações. É um tipo de operação que não pode ser evitada, tendo em vista a concorrência do mercado e a pressão por melhores preços, mas ela deve ser bem gerenciada nos seus diversos estágios.

A primeira ação será a auditoria de segurança nas filiais em que vão ocorrer as consolidações, começando pela auditoria pré-contratual, solicitando um plano de ação e fazendo a manutenção com as auditorias semestrais ou anuais. A segunda será estabelecer formas de controle e de conferências em todos os pontos do processo. Deve constar no conhecimento de transporte rodoviário de cargas (CTRC) o número do lacre (mesmo se existir a trava de baú) que estava no caminhão ao deixar a doca do embarcador. Já na filial, deve haver um processo de conferência do lacre e da mercadoria e emissão de documento atestando o estado em que foram recebidos. Deve-se continuar as checagens e assinaturas em cada ponto até a chegada no cliente, o qual deverá ter sido informado pelo embarcador sobre detalhes, sobre fitas-lacre, verificação de violações, informações de suspeitas em tempo real etc. Também deve-se estabelecer por escrito (nome, sobrenome, RG, filiação etc.) quem recebe e libera a carga em cada estágio e ainda quem tem acesso a tais informações.

A operação toda deverá ser repetida quantos forem o número de galpões ou pontos de parada para troca de motorista etc. Se houver necessidade de a carga pernoitar ou passar certo período em algum dos galpões, uma auditoria mais

profunda deverá ser aplicada, utilizando-se o padrão Tapa para segurança física. Dependendo da forma e do contrato de seguro, esta operação não será admitida sem que haja a vistoria do seguro no galpão e sua aprovação. Algum sistema de proteção deve estar disponível mesmo em locais distantes, pois nunca se sabe quando o cliente não receberá a carga por um problema qualquer. Aliás, isso deve ser discutido e planejado com antecedência.

Além da consolidação, o caminhão pode passar pela empresa de transporte para a emissão do CTRC, mesmo que seja uma carga fechada (o seguro considera carga em trânsito). Os riscos aí são os mesmos do caso anterior, senão maiores, pois a carga já está carregada com certo valor, o que já compensaria um ataque. Algumas empresas de transporte têm infraestrutura suficiente para emitir este documento ainda na doca do embarcador; sendo assim, a carga pode seguir direto para o destino.

CARGA AÉREA E COMBINAÇÃO DE DOIS OU MAIS MODAIS

Tanto no transporte para o mercado interno quanto para exportação, a empresa pode ou não se utilizar de mais de um modal, depende de cada caso e dos termos da venda. Uma carga pode seguir apenas no modal rodoviário, inclusive para exportação, se o acesso assim o permitir, como é o caso da maioria dos países limítrofes com o Brasil. Neste caso, o gerenciamento de risco será o mesmo do mercado interno, com os controles adicionais e o processo de relacração do caminhão na fronteira após inspeção da aduana, repetindo-se os passos e processos de conferência em cada ponto de parada.

O que se deve ter em mente é que em nosso país o transporte é essencialmente rodoviário, conforme já explorado neste texto. Mais de 60% das cargas trafegam em nossas rodovias com falhas estruturais e predomínio de pistas simples, na maioria dos casos, sem nenhum apoio. Os pedágios vêm mudando algumas poucas situações, mas, em compensação, aumentam o valor do frete ou estrangulam o lucro das empresas transportadoras.

A malha ferroviária brasileira (28.000 Km) é menor que a da Argentina (35.000 Km) e muito menor que a norte-americana (mais de 170.000 Km), país em que 47% do transporte é ferroviário, perdendo apenas para a Polônia, que transporta mais de 56% das cargas via ferrovia. Os transportes ferroviário e hidroviário tendem a crescer no Brasil, mesmo porque, se for diferente, com o estado da malha rodoviária e outros fatores como congestionamentos, roubo de carga etc., haverá um completo estrangulamento do transporte rodoviário no país.

Números à parte, não há muitas diferenças em termos de processo para controle e segurança da carga ao se utilizar mais de um modal; o conceito de checagem

em cada estágio, em cada parada para troca de modal e auditorias em cada ponto é o mesmo. A diferença é que, quando se trata de monitorar a carga durante sua passagem por portos ou aeroportos, esbarram-se em alguns entraves que as autarquias responsáveis pelo manuseio e armazenagem da carga propiciam. Normalmente, estas áreas são de acesso restrito, principalmente quando se trata de exportação ou importação envolvendo a Receita Federal. Apesar de as transportadoras serem clientes destas autarquias e pagarem caro pelo tratamento dado à carga, nem sempre é possível e fácil acompanhá-la de perto quando sob responsabilidade deles.

O fornecedor de transporte, o despachante aduaneiro e o agente de carga devem estar sincronizados quanto aos métodos de verificação, antes de receber a carga em portos ou aeroportos. Padrões de avarias e/ou indícios de furto devem ser estabelecidos para evitar a retirada de carga suspeita e, se for o caso, solicitação de vistoria oficial para fins de seguro. No caso de importação de peças e insumos, o problema maior é o tempo. Normalmente, toda carga "era para ontem" para não parar a produção, distribuição etc. Em muitos casos, as empresas abrem mão de "pequenas" perdas, considerando uma franquia de cinco mil dólares, para não atrasar a produção. Porém, se somadas, tais perdas no final do ano poderão significar uma considerável quantia.

Outro fator a se considerar em transportes são os *incoterms* – termos internacionais de comércio, mas que também são utilizados como parâmetro no mercado interno. Os *incoterms* regulam a medida da responsabilidade por frete, seguro e risco de cada integrante da relação comercial de transporte. Os *incoterms* são divididos em quatro grupos:

- **Grupo E (*Ex Works* [EXW]):** vendedor somente coloca as mercadorias disponíveis ao comprador na propriedade do próprio vendedor.
- **Grupo F (*Free Carrier* [FCA], *Free Alongside Ship* [FAS], *Free on Board* [FOB]):** vendedor entrega as mercadorias a um transportador indicado pelo comprador.
- **Grupo C (*Cost and Freight* [CFR]; *Cost, Insurance and Freight* [CIF]; *Carriage Paid to* [CPT]; *Carriage and Insurance Paid to* [CIP]):** vendedor tem que contratar o transporte, mas sem assumir o risco de perda ou dano às mercadorias.
- **Grupo D (*Delivered at Frontier* [DAF], *Delivered Ex Ship* [DES], *Delivered Ex Quay* [DEQ], *Delivered Duty Unpaid* [DDU], *Delivered Duty Paid* [DDP]):** vendedor arca com todos os custos e riscos necessários para levar as mercadorias ao local de destino.

Independentemente de quem é responsável, quem paga o seguro etc., o fato é que se algo acontecer, dependendo do termo, alguma perda sempre vai ficar para

a empresa embarcadora, quer seja pelo derrame de produto irregular no mercado e consequente concorrência, quer seja pela perda financeira direta. Mesmo quando o transporte e as responsabilidades ficam por conta do cliente, alguma conversa e medidas deveriam ser tomadas para proteger o produto em si.

INTEGRAÇÃO DO PLANO DE SEGURANÇA EM LOGÍSTICA – RESPONSABILIDADES DO EMBARCADOR, DO TRANSPORTADOR, DAS EMPRESAS DE SEGURANÇA E DOS CLIENTES

As responsabilidades de cada integrante são definidas em contrato ou pelos termos da venda. Independentemente do que diz o papel, a responsabilidade de cada parte deve ser com a proteção da carga, a fim de evitar que algo aconteça, pois não importa quem vai pagar ou responder, o fato é que, se houver falha, será mais um número para as estatísticas e mais um impacto para o produto e a empresa.

A ideia principal é conectar os processos internos do embarcador, para garantir a integridade da carga que sai, aos processos do transportador e aos de recebimento do cliente. Tudo isso monitorado e conectado com as áreas de segurança de cada interessado.

Os clientes podem colaborar muito no processo de proteção da carga, principalmente quando envolver casos de agendamento de entrega. Às vezes, há falha na comunicação e a carga não é recebida, gerando duas novas oportunidades de roubo/furto, já que ela faz o caminho de volta e será entregue novamente outro dia. Muitas vezes, não há local para que o caminhão aguarde carregado e nem o seguro permite que pernoite em determinados galpões. A situação chega a ponto de o risco ser assumido e uma operação de segurança especial ser montada, gerando custos que poderiam ser evitados se as partes trabalhassem em maior harmonia.

VISÃO DO FUTURO

A tecnologia fornece e continuará fornecendo boas ferramentas – com equipamentos menores, maior autonomia de bateria, via rádio frequência, celular ou satélite –, a fim de que sejam inseridas nas cargas para posterior rastreamento em caso de roubo.

Conforme mencionado, a maior distribuição do volume de carga nos modais ferroviário e hidroviário deve ser uma busca constante, não só em relação aos custos, mas também em relação à segurança. É muito provável que no futuro tenhamos que criar os barcos-escolta (existentes em alguns pontos), escolta para

acompanhar trens etc. se não resolvermos um problema básico e crucial: a receptação. Ninguém vende se não há quem compre e, em muitos casos, a carga já é comprada antes mesmo de ser roubada.

Veja como o *Código Penal* (Brasil, 1940) trata do assunto:

> Receptação
>
> Art. 180 – Adquirir, receber, transportar, conduzir ou ocultar, em proveito próprio ou alheio, coisa que sabe ser produto de crime, ou influir para que terceiro, de boa-fé, a adquira, receba ou oculte: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> Receptação qualificada
>
> § 1º – Adquirir, receber, transportar, conduzir, ocultar, ter em depósito, desmontar, montar, remontar, vender, expor à venda, ou de qualquer forma utilizar, em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, coisa que deve saber ser produto de crime: Pena – reclusão, de 3 (três) a 8 (oito) anos, e multa.
>
> § 2º – Equipara-se à atividade comercial, para efeito do parágrafo anterior, qualquer forma de comércio irregular ou clandestino, inclusive o exercício em residência.
>
> § 3º – Adquirir ou receber coisa que, por sua natureza ou pela desproporção entre o valor e o preço, ou pela condição de quem a oferece, deve presumir-se obtida por meio criminoso: Pena – detenção, de 1 (um) mês a 1 (um) ano, ou multa, ou ambas as penas.
>
> § 4º – A receptação é punível, ainda que desconhecido ou isento de pena o autor do crime de que proveio a coisa.
>
> § 5º – Na hipótese do § 3º, se o criminoso é primário, pode o juiz, tendo em consideração as circunstâncias, deixar de aplicar a pena. Na receptação dolosa aplica-se o disposto no § 2º do Art. 155 (acrescentado pela Lei nº 9.426/1996).

Não se pode afirmar que as penas são pequenas, somente que não são aplicadas e existem muitas formas de abrandamento, como no caso do art. 5º. O receptador na maioria das vezes é quem fez a encomenda e deveria ser tratado como membro do bando ou quadrilha pela forma reiterada e planejada de agir.

Há muito que se considerar antes de pensar em um futuro protegido por tecnologia, antes deveria haver uma evolução ética e moral do ser humano, agindo de forma a não prejudicar ninguém. Nem seria o caso de se fazer mais leis ou leis mais duras, melhor seria, primeiramente, cumprir as existentes.

Outro ponto é que quanto mais a iniciativa privada toma medidas externas, faz investimentos em escoltas, rastreamentos, tecnologia etc., mais o Estado se afasta da sua função de prover o serviço de policiamento. Existem relatos de caminhoneiros que rodam quilômetros sem cruzar com uma única viatura policial, estando realmente entregues e protegidos apenas pelo seu equipamento e escolta. Mas como ficam as pessoas que não podem investir?

O aparelho investigativo também merece investimento futuro, pois existem casos de comunicação de roubo de carga em que nunca foram abertos inquéritos para investigação do fato. De acordo com matéria do jornal *O Estado de São Paulo*, a pessoa que comete um crime tem apenas uma chance em 20 de responder à

Justiça; e caso não seja pega em flagrante, esse índice sobe para 1 em cada 40 casos (Manso e Brancatelli, 2010). O crime organizado tem muito dinheiro e, por mais que a tecnologia avance, não há sistema no mundo que consiga desfazer a ideia do ganho fácil.

A solução é impor danos financeiros vultosos ao bolso de quem financia o crime. Toda vez que houver um roubo de carga, a empresa ou as empresas vítimas devem nomear um assistente da promotoria e, assim que identificado o receptador e finalizado o processo, entrar com ação cível contra o receptador, pleiteando o recebimento de indenização por perdas e danos diretos e indiretos que puderem ser especificados.

Há no mercado diversos meios e métodos para se proteger contra o crime, basta ter como investir. Câmeras podem ser instaladas em caminhões, transmissores podem ser inseridos nas cargas, escoltas com mais treinamento e equipamento podem ser encontradas e outras possibilidades.

Chegará também o dia em que as empresas trabalharão em conjunto para manter, por exemplo, pontos de controle e vigilância fixos no decorrer das principais e mais arriscadas rotas. Um *pool* de empresas financiando o bem de todas, aliando postos fixos e móveis. Isso pode parecer caro para uma só, mas talvez não seja para todas as empresas que utilizam a rota; por exemplo, somente na região de algumas estradas de São Paulo, o movimento é de 54 mil caminhões/dia.

EMPRESAS DE SEGURANÇA PATRIMONIAL E DE ESCOLTA DENTRO DA CADEIA LOGÍSTICA

As empresas de segurança patrimonial privada e de escolta são as prestadoras de serviço que mais integram o elo da cadeia logística; embora, sob o aspecto tributário, tenham permanecido em regime cumulativo e figurado como exceção às regras da não cumulatividade do Programa de Integração Social (PIS) e da Contribuição para o Financiamento da Seguridade Social (Cofins), de acordo com as Leis nº 10.637/2002 e nº 10.833/2003. Porém, tais empresas esbarram em grandes dificuldades em função da legislação trabalhista brasileira.

A legislação trabalhista em vigor no Brasil é muito antiga e merece uma modernização, com a inserção de ideias criativas, mediante ampla discussão com as partes envolvidas: empresários, trabalhadores e governo.

No segmento da Segurança Privada, tem-se o emprego intensivo de mão de obra, e isto invariavelmente traz à tona diversas polêmicas ainda não resolvidas plenamente pela Justiça do Trabalho. É o caso do intervalo de repouso e alimentação, quotas de deficientes, quotas de aprendizes, trabalho em domingos e feriados, da condenação à ilegalidade de escalas de trabalho que usualmente são as melho-

res etc. Sabidamente, pela Lei nº 7.102/1983, que regula a atividade da Segurança Privada no Brasil, exige-se que o profissional de segurança tenha plena capacidade física e mental. No entanto, as empresas são demandadas a cumprir a quota de deficientes e de aprendizes, tal como ocorre com empresas de qualquer outro segmento. Ou seja, as empresas para cumprirem com todos os requisitos legais, obrigam-se a incorporar custos desnecessários e que efetivamente não contribuem com o desempenho operacional propriamente dito.

Como o custo da mão de obra direta representa 80% ou mais do custo total, se tais problemas caminharem para uma solução, permitirão um fôlego às empresas, propiciando inclusive que transfiram mais recursos ao treinamento e à capacitação profissional. Desta forma, elas integrarão o elo da cadeia logística muito mais preparadas ao acompanhamento, à prevenção e à solução dos problemas até aqui levantados.

Cabe ainda ao contratante a consciência de que precisa pagar pela qualidade do serviço. Baixo custo normalmente significa baixa qualidade dos serviços prestados ou falta de pagamento correto das obrigações trabalhistas.

Os encargos apontados representam, dentro de uma contextualização ampla de encargos, aspectos tributários relevantes dos principais agentes de segurança que atuam junto à indústria e, portanto, merecem especial atenção das medidas governamentais a serem adotadas nos próximos anos.

OPERADOR ECONÔMICO AUTORIZADO (OEA)

Conforme já inicialmente explorado neste capítulo, o certificado de OEA – conferido a determinados agentes da cadeia logística – representou grande avanço na celeridade e segurança das operações globais de comércio. É concedido pelas aduanas de diversos países signatários da Organização Mundial das Aduanas (OMA) e conecta-se com os aspectos tributários dos processos, enquadrando-se perfeitamente na temática abordada no seminário.

O OEA no Brasil é uma certificação concedida pela Receita Federal a importadores, exportadores, agentes de carga, portos, aeroportos, recintos sob controle aduaneiro, transportadores e outros atores da cadeia de suprimentos na logística de comércio exterior, a qual lhes confere o *status* de empresa segura e confiável em suas operações.

No Brasil, como em todos os programas OEA sob as diretrizes da OMA, a adesão das empresas é voluntária. O OEA é uma parte envolvida no movimento de cargas de comércio internacional, que se insere no contexto desse programa de segu-

rança. Sua implementação objetiva maior segurança no comércio internacional e traz vantagens ao fluxo da cadeia logística.

Para que tais fatores sejam intrínsecos às práticas de comércio exterior, não basta apenas implementar procedimentos e normas para o setor como um todo. É preciso focar nos atores da cadeia logística que cuidam da movimentação da carga, pois são eles que garantem que as mercadorias não sejam violadas ou danificadas, mas também, e principalmente, adicionadas de produtos ilícitos, como armas e drogas. Daí a importância de atores que sejam OEA.

Para as autoridades aduaneiras certificarem as empresas nacionais como um OEA, previamente verificam se elas atendem aos padrões mínimos de segurança estabelecidos pelo programa OEA de seu país. Nos certificados de todos os programas OEA dos países signatários da OMA, as empresas comprovaram sua confiabilidade e, por isso, as aduanas irão excluí-las do universo de risco, deixando de fiscalizá-las com frequência, podendo, assim, focar seus esforços nas empresas que não têm o *status* OEA, por não optarem pela sua participação no programa ou, talvez, por não atenderem às normas e regras mínimas de segurança. De qualquer modo, estas últimas são as que representam riscos maiores para suas cargas e operações.

Os requisitos para se tornar um OEA são rigorosos e exigem alto grau de comprometimento da empresa com o estabelecimento de normas de segurança em vários setores, seja no manuseio da carga, seja no procedimento ou documentação de interesse aduaneiro.

No programa brasileiro de OEA, seguindo diretrizes e critérios estabelecidos pela OMA, são exigidos das empresas pretendentes a obtenção do certificado, o atendimento a requisitos de admissibilidade do pedido e de elegibilidade ao *status* de empresa segura. Dentre os últimos, destacam-se:

- Ações para a confiabilidade da parceria empresa *versus* aduana, que representa esse certificado.
- Existência e exercício da atividade na logística de comércio exterior há mais de dois anos.
- Escrituração contábil digital e adesão ao programa da Receita Federal do Brasil denominado Domicílio Tributário Eletrônico (DTE).
- Regularidade fiscal comprovada por certidão da Receita Federal e apresentação do pedido mediante dossiê eletrônico.
- Conformidade com as obrigações aduaneiras: a aduana checará os antecedentes da empresa, isto é, o histórico de autuações e processos de eventuais irregularidades cometidas nos últimos cinco anos.

- Existência de sistemas eletrônicos satisfatórios para controle e gestão dos registros comerciais, fiscais e operacionais.
- Viabilidade financeira: mostra a capacidade que o OEA terá de se adaptar e aperfeiçoar as operações de comércio exterior.
- Cooperação e comunicação: tanto a empresa quanto a aduana devem ter acesso às informações que precisarem em tempo real, de forma a promoverem a segurança de maneira preventiva.
- Conscientização de todo o pessoal sobre a segurança do OEA: como resultado de política de treinamentos para promover e desenvolver meios de capacitação do pessoal para o funcionamento correto e seguro da cadeia logística.
- Segurança dos sistemas informatizados para a garantia da confiabilidade dos dados e acesso às informações apenas por pessoas credenciadas, prevenindo seu uso indevido ou sua alteração por pessoas sem autorização.
- Cuidados na seleção e aceitação de parceiros comerciais: a empresa deve ter política de seleção de seus parceiros comerciais, que podem ser seus prestadores de serviço e, inclusive, seus clientes, para que sejam considerados seguros, ou seja, para que adotem os mesmos padrões de segurança exigidos para sua certificação OEA.
- Segurança das instalações: as instalações em que há movimentação ou manuseio de carga de comércio exterior devem apresentar barreiras em todo o perímetro e estar em condições que ofereçam total segurança contra o acesso de pessoas não autorizadas.
- Segurança da carga: a empresa OEA deve se preocupar em implementar constantemente medidas que garantam a integridade da carga sob sua responsabilidade e que assegurem alto nível de controle sobre ela.
- Segurança do transporte: é necessário que os transportes estejam sob controles eficazes, garantindo sua conservação, segurança e rastreabilidade.

Cumpridas essas exigências de admissibilidade e elegibilidade, a Receita Federal designará uma equipe para a validação e confirmação das informações apresentadas no dossiê; uma vez que a empresa seja aprovada, emite-se o certificado de OEA.

A aduana do país pode, então, oferecer benefícios procedimentais à empresa certificada, tais como agilização de verificação e liberação das mercadorias submetidas a despacho aduaneiro. Isso significa que o OEA terá prioridade nos processos de desembaraço e checagem pela autoridade aduaneira, diminuindo o tempo desses despachos e gerando economia de custos.

Quanto maior o número de empresas nacionais atuantes nas diversas atividades da logística de comércio exterior que obtiverem sua certificação como OEA, melhor para o Brasil promover os acordos de reconhecimento mútuo (MRA, *mutual recognition agreement*) com os países que mantém comércio. Desta forma, o país se compromete com a confiabilidade das informações e a segurança de não exis-

tência de tráfico de armas e drogas nas mercadorias originárias e manipuladas por empresas OEA, permitindo que as exportações tenham um tratamento agilizado no processo de desembaraço aduaneiro no destino.

Para Antonio Russo, a padronização quanto à autorização dos OEA abre campo para o desenvolvimento de sistemas internacionais de reconhecimento mútuo do OEA em níveis bilateral, sub-regional e, a longo prazo, mundial. Através desse reconhecimento mútuo é possível evitar duplicidade de controle de segurança, contribuindo para a facilitação da verificação de mercadorias que circulam na cadeia logística nacional e internacional.

No Brasil, podem requerer a certificação OEA junto à Receita Federal os intervenientes da cadeia logística internacional constantes do art. 4º da Instrução Normativa da RFB nº 1.598/2015:

- Importador.
- Exportador.
- Transportador.
- Agente de carga.
- Depositário de mercadoria sob controle aduaneiro.
- Operador portuário ou aeroportuário.
- Despachante aduaneiro.

A adesão ao programa brasileiro de OEA é voluntária, ou seja, os operadores que optarem pela não certificação continuarão normalmente suas operações no comércio exterior, porém não usufruirão dos benefícios a que fazem jus os operadores certificados.

O art. 4º citado anteriormente traz um rol taxativo das categorias de operadores econômicos que podem ser certificadas pelo programa. Desta forma, se a atividade desenvolvida pela sua empresa não estiver contida dentre as citadas nos incisos deste artigo, neste primeiro momento, sua participação no Programa OEA não será permitida.

Por outro lado, o § 3º deste mesmo artigo traz a possibilidade de, ao longo do tempo, serem introduzidas novas categorias de intervenientes no rol das certificáveis no programa brasileiro de OEA, como se lê: "A Coordenação-Geral de Administração Aduaneira (Coana) poderá estender a certificação a outros intervenientes da cadeia logística no fluxo do comércio exterior".

BENEFÍCIOS DA CERTIFICAÇÃO OEA

Aos operadores certificados no Programa Brasileiro de OEA – conforme determinado no art. 8º da Instrução Normativa RFB nº 1.598/2015, alterada pela Instrução Normativa RFB nº 1.624/2016 – serão concedidos benefícios que se relacionem com a facilitação dos procedimentos aduaneiros tanto no país quanto no exterior. Estes benefícios podem ser de caráter geral ou concedidos de acordo com a modalidade de certificação (Segurança, Conformidade nível 1, Conformidade nível 2 ou Pleno), a função do operador na cadeia logística ou o grau de conformidade aferido.

É importante ressaltar que os benefícios concedidos aos operadores certificados como OEA serão usufruídos em qualquer unidade aduaneira da Receita Federal do Brasil e a Coana poderá conceder outros benefícios além dos descritos a seguir.

CERTIFICAÇÃO OEA – BENEFÍCIOS DE CARÁTER GERAL

O art. 9º da Instrução Normativa RFB nº 1.598/2015 traz os benefícios de caráter geral, os quais são extensivos a todas as modalidades de certificação (OEA-Segurança, OEA-Conformidade e OEA-Pleno):

- **Divulgação no sítio da RFB:** o Centro OEA divulgará o nome do operador no sítio da RFB, após a publicação do respectivo Ato Declaratório Executivo (ADE), caso o OEA assim o solicite no Requerimento de Certificação (Anexo I da Instrução Normativa RFB nº 1.598/2015).
- **Utilização da logomarca AEO (*Authorized Economic Operator*):** fica permitida a utilização da logomarca do Programa Brasileiro de OEA, conforme especificações contidas na Portaria RFB nº 768/2015 – Manual da Marca AEO.
- **Ponto de contato:** o Coordenador Nacional do Centro OEA designará um servidor como ponto de contato para a comunicação entre a RFB e o OEA para esclarecimento de dúvidas relacionadas ao Programa Brasileiro de OEA e a procedimentos aduaneiros.
- **Prioridade de análise em outra modalidade OEA:** o Centro OEA dará prioridade na análise do pedido de certificação de operador que já tenha sido certificado em outra modalidade ou nível do Programa Brasileiro de OEA.
- **Benefícios concedidos pelas aduanas estrangeiras:** será facultado ao OEA usufruir dos benefícios e vantagens dos Acordos de Reconhecimento Mútuo (ARM) que a RFB venha a assinar com as aduanas de outros países.
- **Participação no fórum consultivo:** o OEA poderá participar da formulação de propostas para alteração da legislação e dos procedimentos aduaneiros que visem ao aperfeiçoamento do Programa Brasileiro de OEA, por meio do Fórum Consultivo.

- **Dispensa de exigências já cumpridas no OEA:** as unidades de despacho aduaneiro da RFB dispensarão o OEA de exigências formalizadas na habilitação a regimes aduaneiros especiais ou aplicados em áreas especiais que já tenham sido cumpridas no procedimento de certificação no Programa Brasileiro de OEA.
- **Participação em seminários e treinamentos:** os OEA poderão participar de seminários e treinamentos organizados conjuntamente com o Centro OEA.

BENEFÍCIOS ESPECÍFICOS DO OEA-SEGURANÇA E DO OEA-PLENO

O art. 10 da Instrução Normativa RFB nº 1.598/2015 traz os benefícios especificamente oferecidos aos operadores certificados na modalidade OEA-Segurança e OEA-Pleno:

- **Reduzido percentual de canais de conferência na exportação:** a seleção para canais de conferência dos despachos de exportação do exportador OEA terá seu percentual reduzido em relação aos demais.
- **Parametrização imediata das Declarações de Exportação (DE):** a parametrização das declarações aduaneiras do exportador OEA será executada de forma imediata, após o envio para despacho da DE.
- **Prioridade de conferência das DE selecionadas:** a DE do exportador OEA selecionada para conferência será processada pelas unidades da RFB de forma prioritária, permitido seu disciplinamento por meio de ato específico emitido pela Coana.
- **Dispensa de garantia no trânsito aduaneiro:** será dispensada a apresentação de garantia no trânsito aduaneiro cujo beneficiário seja transportador OEA.

BENEFÍCIOS ESPECÍFICOS DO OEA-CONFORMIDADE (NÍVEIS 1 E 2) E DO OEA-PLENO

O art. 11 da Instrução Normativa RFB nº 1.598/15 traz os benefícios específicos para os operadores certificados na modalidade OEA-conformidade (níveis 1 e 2) e para o OEA-pleno:

- **Reposta à consulta de classificação fiscal em até 40 dias:** a consulta sobre classificação fiscal de mercadorias formulada pelos operadores OEA-Conformidade e OEA-Pleno, formulada nos termos da Instrução Normativa RFB nº 1.464/14, desde que atendidos os quesitos de que tratam os arts. 5º e 6º da referida Instrução Normativa, terá solução proferida em até 40 dias, a contar da protocolização da consulta ou de seu saneamento, quando necessário.
- **Dispensa de garantia na admissão temporária para utilização econômica:** será dispensada a apresentação de garantia para o importador OEA-Conformidade ou OEA-Pleno na concessão do regime de admissão temporária para utilização econômica.

BENEFÍCIOS ESPECÍFICOS DO OEA-CONFORMIDADE NÍVEL 2 E DO OEA-PLENO

O art. 12 da Instrução Normativa RFB nº 1.598/2015 traz os benefícios específicos para os operadores certificados na modalidade OEA-Conformidade nível 2 e para o OEA-Pleno:

- **Reduzido percentual de canais de seleção na importação:** a seleção para canais de conferência dos despachos de importação do importador OEA terá seu percentual reduzido em relação aos demais.
- **Parametrização imediata das Declarações de Importação (DI):** a parametrização das declarações aduaneiras do importador OEA será executada de forma imediata após o registro da DI.
- **Prioridade de conferência das DI selecionadas:** a DI do importador OEA selecionada para conferência será processada pelas unidades da RFB de forma prioritária, permitindo seu disciplinamento por meio de ato específico emitido pela Coana.
- **Registro antecipado da DI no modal marítimo:** será permitido ao importador OEA registrar a DI antes da chegada da carga ao território aduaneiro, com aplicação de seleção parametrizada imediata.
- **Canal verde na admissão temporária:** a DI registrada por importador OEA para o regime aduaneiro de admissão temporária poderá ser selecionada para o canal verde de conferência aduaneira, dispensados o exame documental e a verificação da mercadoria.

OEA – ACORDOS DE RECONHECIMENTO MÚTUO

Os acordos de reconhecimento mútuo (MRA, *mutual recognition agreement*) são acordos bilaterais celebrados entre aduanas de países ou blocos que possuam programas de OEA compatíveis entre si. Isso significa que tanto os critérios adotados quanto os procedimentos de validação devem ser iguais ou semelhantes entre si.

Os principais objetivos de um MRA são:

- Reconhecimento das certificações OEA emitidas pela aduana do outro país.
- Tratamento prioritário das cargas e consequente redução de custos associados à armazenagem.
- Comprometimento recíproco da oferta de benefícios comparáveis.
- Previsibilidade das transações.
- Melhora na competitividade das empresas OEA no comércio internacional.

Os MRA são uma meta a ser alcançada a médio ou longo prazo. Isso se deve porque, primeiramente, os programas de OEA de ambos os países devem estar ma-

duros quanto aos procedimentos de certificação dos operadores adotados e também porque deve haver um número considerável de operadores já certificados e usufruindo dos benefícios em ambos os países interessados no aludido acordo.

Os MRA das certificações OEA entre dois países ou blocos agilizam as transações de comércio exterior, pois permitem uma recíproca elevação da confiança e da segurança nas operações, e o Brasil está negociando tais acordos com os principais países com os quais mantém e/ou pretende incrementar seu comércio internacional.

DIAGNÓSTICO FINAL

Após a apresentação remissiva dos aspectos tributários da Segurança Empresarial, com enfoque na segurança da cadeia logística do comércio exterior, o Congresso de Segurança na Indústria Fiesp permitiu um debate mais amplo no segundo dia do evento, ocasião em que a mesa 2 debateu os conteúdos que foram expostos nas apresentações iniciais e aqui reproduzidos. Finalmente, avaliado o quadro geral dentro do atual contexto macroeconômico do país e, ainda, considerada a experiência de cada profissional em suas carreiras, pôde-se concluir pelo seguinte diagnóstico:

- A segurança é considerada pela Indústria um custo fixo e não um investimento. Consequentemente, o produto oferecido pelo mercado prestador é uma *commodity*, cuja única diferenciação mais palpável é o preço praticado.
- Tal prática torna a *performance* da segurança patrimonial, por exemplo, a mais preponderante no segmento hoje, bastante suscetível a elevações do custo direto da mão de obra, particularmente onerado pelos elevados encargos no Brasil nos últimos anos.
- Mesmo para os tomadores de serviço em que o aspecto operacional é relevante, o aspecto tributário é negligenciado.
- No Brasil, a falta de integração dos agentes de segurança do Estado, em qualquer esfera de poder ou entre elas, obriga as empresas a atender aos requisitos legais mediante diligência burocrática dispersa e onerosa junto a vários organismos diferentes para obtenção de suas autorizações e outras providências que dependem dos órgãos públicos.
- Outra consequência do mesmo fato é que a Segurança Pública desarticulada não provê a parcela de segurança que lhe cabe, obrigando as empresas a adotarem por si mesmas soluções muito mais custosas para prover esta falta.
- No caso da cadeia logística do comércio exterior, esses problemas interferem até mesmo nas decisões do investimento estrangeiro no país, com reflexos diretos no desempenho econômico.

Por outro lado, a experiência do grupo formado na mesa 2 identificou práticas avançadas em outros países que devem servir de *benchmarks* para os estudos brasileiros nessa área, que, resumidamente, são as seguintes:

- Nos Estados Unidos, como também em alguns países europeus, nota-se uma integração maior das forças de Segurança Pública, pela centralização de decisões em um único departamento de Estado, subordinado diretamente ao Gabinete Presidencial, como é o caso do U. S. Department of Homeland Security (DHS). Isto converge para uma facilidade maior dos agentes privados em obter autorizações e discernir até onde vai a segurança do Estado e onde começa sua Segurança Privada interna.
- Como consequência, tome-se como exemplo que, em alguns destes países, o governo sequer autoriza a escolta armada, pois eventos dessa natureza são de responsabilidade do Estado.
- O programa de segurança no comércio exterior norte-americano C-TPAT é outra *benchmark* relevante a ser considerada. Trata-se de associação estratégica entre a aduana e a Indústria contra o terrorismo. É uma iniciativa conjunta do governo dos Estados Unidos e das classes empresariais, cujo objetivo é construir relações de cooperação comercial que reforcem e melhorem segurança e *compliance* na cadeia logística de comércio internacional.
- O programa AEO, semelhante ao C-TPAT, desenvolvido pela Organização Mundial das Aduanas, é outra *benchmark* importante, ressalvado que esse programa já é adotado pelo Brasil desde dezembro de 2014, aqui denominado OEA. O programa ainda está em fase inicial, mas, reforçado pelos acordos internacionais de reconhecimento mútuo entre dois ou mais países, traz agilidade e segurança à cadeia logística mundial.
- Ambos C-TPAT e OEA, além de darem celeridade aos processos e diminuírem os custos da cadeia, aumentam de tal forma a relação de confiança e segurança que representam atrativo de investimentos aos países que os adotam.
- Grandes empresas multinacionais já estão adotando o enfoque integrado da segurança e transferindo-a para a rubrica investimento, fazendo, na verdade, a gestão de riscos do negócio como um todo (ISO 31.000, 2009).

PROPOSTAS DE CONDUÇÃO DE MELHORIAS

Em face do diagnóstico apresentado, foram formuladas propostas que convergem para a melhoria dos aspectos tributários da Segurança Empresarial, conforme descritas a seguir:

- Maior integração das forças de segurança do estado brasileiro, de tal forma a propiciar o exercício da efetiva segurança de competência pública, bem como a desburocratização das atividades privadas delas dependentes.
- Unificação tributária das atividades que envolvem a prestação de serviços

de segurança dentro da cadeia logística, simplificando tarefas de rotina e controle, aumentando assim a competividade brasileira em comparação aos demais países.

- Aceitação pela Receita Federal do Brasil do custo da segurança como crédito tributário dos impostos não cumulativos, independentemente desse custo estar ou não inserido diretamente no processo produtivo. A proposta está em convergência com o enfoque do tratamento da segurança como investimento e não como despesa, estimulando as tomadoras do serviço a adotarem tal prática de forma generalizada.
- Incluir as empresas de segurança como intervenientes da cadeia logística do comércio exterior, de tal forma que elas possam se habilitar (eleger) para a certificação OEA. Isto permitiria uma seleção mais rigorosa e apurada das empresas de segurança e a Receita Federal poderia, além dos requisitos convencionais e legais exigidos no processo, indicar como boa prática a utilização de empresas de segurança certificadas OEA, como fator positivo na determinação do nível de risco na cadeia logística de comércio exterior.
- Edição de legislação prevendo objetivamente a devolução de tributos incidentes em mercadorias roubadas em trânsito por vias públicas.
- Realização de debates ampliados com a representação de governo, classe empresarial e classe trabalhadora, com vistas ao estudo de mudanças criativas na legislação trabalhista, pois, mesmo que totalmente dentro do enfoque da segurança integral, o custo da mão de obra direta ainda remanescerá um item preponderantemente elevado dentro do custo total da segurança na Indústria.

CAPÍTULO 3

GOVERNANÇA E *COMPLIANCE* EM GESTÃO DE RISCO*

* Compilação dos debates transcorridos durante o painel e a mesa de trabalho de mesmo título do Seminário de Segurança na Indústria, realizado no Prédio da Fiesp, em 21 e 22 de junho de 2016.

DEFINIÇÃO

Compliance "é um conjunto de regras, padrões, procedimentos éticos e legais, que, uma vez definido e implantado, será a linha mestra que orientará o comportamento da instituição no mercado em que atua, bem como as atitudes de seus funcionários" (Candeloro *et al*., 2012, p. 30).

Em síntese, o termo *compliance* tem origem no verbo *to comply*, que significa agir de acordo com a lei, uma instrução interna, um comando ou um pedido, ou seja, estar em *compliance* é estar em conformidade com as regras e as normas jurídicas (Bertocceli, 2016).

Governança e *compliance* são temas de grande relevância para as empresas, na medida em que vêm transformando o ambiente de negócios e estabelecendo vinculações mandatórias nas diversas cadeias produtivas, integrando fornecedores e clientes muito além dos aspectos contratação-entrega-pagamento. Prevenção de lavagem de dinheiro, prevenção de corrupção, continuidade de negócios, proteção do conhecimento empresarial sensível, segurança de sistemas de informação e comunicação, ética, sustentabilidade, proteção de pessoas e de ativos (tangíveis e intangíveis), canais de denúncia, responsabilidade social e prevenção de delitos internos são temas que, a despeito de diferentes motivações e aspectos históricos, estão todos imbricados em governança e *compliance* e têm forte interdependência.

Seu gerenciamento integrado aumenta sobremaneira a segurança do negócio, protegendo inovação, estratégia, diferenciais e outros de seus fatores críticos de sucesso em um ambiente de múltiplos riscos, especialmente os riscos operacionais, aqui conceituados a partir de trecho da Resolução nº 3.380/2006 do Banco Central do Brasil, aplicável às organizações de maneira geral:

> Art. 2º – Para os efeitos desta Resolução, define-se como risco operacional a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.
>
> § 1º – A definição de que trata o *caput* inclui o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanções em razão de descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

§ 2º – Entre os eventos de risco operacional, incluem-se:
I – Fraudes internas;
II – Fraudes externas;
III – Demandas trabalhistas e segurança deficiente do local de trabalho;
IV – Práticas inadequadas relativas a clientes, produtos e serviços;
V – Danos a ativos físicos próprios ou em uso pela instituição;
VI – Aqueles que acarretem a interrupção das atividades da instituição;
VII – Falhas em sistemas de tecnologia da informação;
VIII – Falhas na execução, cumprimento de prazos e gerenciamento das atividades na instituição.

O marco regulatório e normativo dos temas mencionados é diversificado. Parte é conduzida não em face de dispositivos legais, mas de Normas Técnicas como as "famílias" ISO 27.000, 31.000, 37.001 e outras, bem como a partir de orientações de instituições internacionais como a American Society for Industrial Security International (Asis International), cujas indicações também subsidiam procedimentos adotados pelo Department of Homeland Security (DHS) dos Estados Unidos.

Frequentemente, as organizações se veem diante de situações que revelam desconhecimento da realidade de seus riscos operacionais, com perdas importantes. As medidas de prevenção à lavagem de dinheiro e à corrupção são antigas para nossos padrões. Tais medidas já têm 40 anos. Há um aperfeiçoamento crescente, em especial da legislação internacional e, bem mais recentemente, da legislação brasileira. Mais do que praticar medidas relativas à integridade e à ética, as organizações precisam comprovar suas ações e espraiar essas mesmas exigências na sua cadeia de fornecedores e clientes. Elas devem agir em conformidade, ou em *compliance* ao quanto é exigido e recomendado para proteção dos negócios das partes interessadas e da sociedade como um todo.

PRINCIPAIS CARACTERÍSTICAS DAS ANTIGAS LEIS ANTICORRUPÇÃO BRASILEIRAS

- Somente pessoas físicas podem ser condenadas pelo crime de corrupção no Brasil.
- Empresas não podem ser condenadas criminalmente por atos de corrupção, ainda que a empresa seja a beneficiária da vantagem.
- Penalidades para corrupção são basicamente pena de reclusão.
- Foco nos agentes públicos. Falta de leis anticorrupção aplicáveis ao setor privado.
- Falta de leis anticorrupção punindo a pessoa jurídica (Lei de Licitações [Lei nº 8.666/1993]; Lei de Improbidade Administrativa [Lei nº 8.429/1992]) até agora.

ASPECTOS IMPORTANTES DA NOVA LEI ANTICORRUPÇÃO

A nova lei introduz a responsabilidade objetiva da pessoa jurídica nos âmbitos civil e administrativo pelos atos de corrupção cometidos em seu interesse ou benefício:

- Responsabilização da pessoa jurídica não exclui a responsabilidade individual de seus dirigentes ou administradores ou de qualquer pessoa que participe do ato ilícito. Tais indivíduos poderão ser responsabilizados na medida de sua culpabilidade.
- Responsabilidade solidária do grupo econômico, limitada ao pagamento da multa administrativa.
- Possibilidade de acordos de leniência, se presentes os requisitos previstos na nova Lei.
- Importante incentivo ao *compliance*. Nova lei prevê que será levada em consideração na aplicação das sanções a adoção efetiva de códigos de ética/conduta, bem como de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades, ou seja, a existência de programas de *compliance*.

PRINCIPAIS SANÇÕES PREVISTAS NA NOVA LEI ANTICORRUPÇÃO

- Sanções administrativas – Empresa:
  - Multas de 0,1% até 20% do faturamento bruto da empresa no exercício anterior ao da instauração do processo administrativo ou no valor de até R$ 60 milhões, quando não for possível tal cálculo.
  - Publicação extraordinária da decisão condenatória em meios de comunicação de grande circulação.
- Sanções judiciais – Empresa:
  - Perda de bens, direitos ou valores auferidos pela infração.
  - Suspensão ou interdição parcial de suas atividades.
  - Proibição de receber incentivos, subsídios, subvenções, doações ou empréstimos de órgãos ou entidades públicas pelo prazo de 1 a 5 anos.
  - Dissolução compulsória da pessoa jurídica nos casos mais graves.

LEI ANTICORRUPÇÃO (DECORRÊNCIAS PENAIS)	
CORRUPÇÃO ATIVA	"Oferecer ou prometer vantagem indevida a funcionário público, para determiná-lo a praticar, omitir ou retardar ato de ofício". **Pena:** De 2 a 12 anos e multa.
CORRUPÇÃO ATIVA EM TRANSAÇÃO INTERNACIONAL	"Prometer, oferecer e dar, direta ou indiretamente, vantagem indevida a funcionário público estrangeiro, ou terceira pessoa...". **Pena:** De 1 a 8 anos e multa.
LAVAGEM DE DINHEIRO	"Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes... de infração penal". **Pena:** De 3 a 10 anos de multa.

Figura 3.1. Definições de tipos de corrupção com suas respectivas penas, de acordo com a nova Lei Anticorrupção.

CENÁRIO ATUAL

A história brasileira é permeada por escândalos envolvendo corrupção. A realização de obras públicas com denúncias de influência ilícita no processo de contratação é até considerada natural.

Nos últimos anos, entretanto, essa situação ficou dramática, pois foram escancarados para toda a sociedade os múltiplos descalabros, envolvendo bilhões de reais. Tais fatos surpreendem mesmo a nós, brasileiros, pois as empresas envolvidas são as maiores, tanto as controladas pelo erário, como as privadas. Todas com conselhos de administração, auditorias internacionais, regras de *compliance*, gestão de riscos, enfim, formalmente capacitadas para coibir desvios brutais de recursos. Em regra, faltou a eficácia da governança. Ou seja, formalmente, muitos dos padrões de procedimentos estavam definidos, mas não foram exercidos na prática.

NECESSIDADE DE DIMINUIR O ESPAÇO DA AÇÃO ILÍCITA

Toda a ação ilícita que envolve questões econômicas e financeiras visa ao lucro. Assim, seguem a mesma lógica de qualquer atividade empresarial, procuram a melhor relação custo-benefício: menor risco, menor investimento e maior margem. Ao encontrarem um ambiente propício, ampliam suas iniciativas.

No Brasil, foi identificado um ambiente favorável a essa lógica aplicada ao crime: baixo investimento, lucros vultosos e impunidade – eis o tripé do sucesso dos criminosos.

Em muitas iniciativas desenvolvidas empresarialmente, há o favorecimento de propostas que envolvem não as melhores práticas e tampouco os menores preços, mas sim o favorecimento da decisão motivada pelo pagamento de altas somas em propina. Pouco importa o interesse do erário e mesmo a permanência das empresas, os objetivos são a curto e médio prazos, ainda que no futuro a própria existência da empresa seja colocada em risco. Os bônus serão pagos de forma imediata, independentemente da sustentabilidade do negócio. Altos ganhos imediatos – sem respeitar princípios, valores e continuidade de resultados – constituem o mantra da irresponsabilidade empresarial.

Este quadro deve ser enfrentado, procurando aumentar o risco das atividades ilícitas, diminuindo a sensação de impunidade, aperfeiçoando os controles internos, desenvolvendo o denominado programa de integridade nas instituições e fortalecendo um comportamento que no Brasil não é muito praticado: a prevenção.

A lição da Dinamarca, considerado o país menos corrupto do mundo, conforme índice da organização Transparência Internacional, aponta para as seguintes iniciativas que auxiliam no combate à corrupção (Milhorance, 2016):

- Menos regalias para os políticos.
- Pouco espaço para indicação de cargos.
- Transparência ampla.
- Polícia confiável.
- Baixa impunidade.
- Confiança social.
- Ouvidoria forte.

DEFESA DAS INSTITUIÇÕES

As instituições públicas e privadas devem instituir os chamados programas de integridade, viabilizando as ações de *compliance*, identificando os riscos nas diversas operações e as áreas mais sensíveis. Não basta a elaboração dos códigos de

ética e manuais de procedimentos, há que se formar uma cultura da integridade. Esse processo deve ser *top-down*. A liderança deve assumir esse compromisso e gerenciar sua aplicação. A Lei Anticorrupção contempla essa necessidade; não basta existir formalmente todo o arcabouço documental, é necessário demonstrar a efetiva aplicação e a eficácia dos processos criados.

A ação sistêmica e sistemática é a expectativa de um efetivo programa de integridade, e isso vale para as empresas privadas e também para a administração pública. Com esse compromisso, os instrumentos de "conheça seu cliente" (KYC, *know your customer*) para a análise de transações e desenvolvimento de atividades, treinamentos de todas as equipes, avaliação da legislação e verificação dos processos internos para enquadramento às exigências legais, definição dos padrões de conduta e seu gerenciamento, recepção de denúncias com a implementação de ouvidorias (organizacionais e externas) são algumas das iniciativas que estimulam a obtenção de resultados para as instituições e permitem a criação de uma rede de proteção e prevenção de riscos.

Respeitadas tais diretrizes, as instituições estarão mais preparadas para enfrentar as ameaças internas e externas que acarretem desvios de conduta, os quais podem afetar sua credibilidade e a própria continuidade da empresa.

CANAIS DE COMUNICAÇÃO

Toda política de integridade necessita de canais de informação e comunicação. Deve-se informar sobre os procedimentos que devem ser adotados, perpassando toda a instituição, bem como ter capacidade de receber dados e denúncias sobre eventuais desvios que necessitem ser apurados. Ou seja, informar e se comunicar é essencial.

Especialmente com relação aos canais de comunicação, é fato que, muitas vezes, procedimentos incompatíveis com programas de integridade, seja em âmbito privado ou público, só são identificados por meio de denúncias que podem ter origem no âmbito interno ou externo. Para facilitar a recepção de tais denúncias, as instituições devem implantar, capacitar e apoiar, por exemplo, a ação das ouvidorias.

Conforme o rol de recomendações apresentado pela Transparência Internacional (Milhorance, 2016), a existência de ouvidorias fortes é um dos fatores de combate à corrupção. Para que isso seja efetivo, a Associação Brasileira de Ouvidores/*Ombudsman* (ABO) defende que elas tenham garantidas a independência e a autonomia, a fim de que possam exercer a representação dos legítimos interesses que lhes são confiados pelo cidadão (ABO, s/d). Esses princípios somente serão respeitados se a alta administração apoiar as ouvidorias e exercer contato direto com elas. Em verdade, essa atuação estratégica pode viabilizar uma "governança

cidadã" nas instituições públicas e privadas, permitindo que o processo decisório considere as informações colhidas diretamente junto aos consumidores e colaboradores, aperfeiçoando o conhecimento da realidade e a melhoria das próprias decisões.

PAPEL DAS ASSOCIAÇÕES EMPRESARIAIS

No ambiente de negócios, a atuação das associações setoriais é fundamental, afinal, a convergência dos legítimos interesses de um setor e sua defesa junto à sociedade e ao poder público representa um ganho para a competitividade e para a compreensão das consequências de determinadas decisões, que poderão impactar a economia, o mercado e, muitas vezes, o próprio interesse do consumidor.

Tais ações setoriais devem, também, respeitar princípios de integridade, fortalecendo junto aos associados a atuação ética, transparente e legal. Portanto, as associações empresariais não podem servir aos interesses que ferem, por exemplo, princípios da livre e leal concorrência e nem acobertar comportamentos ilegais e antiéticos dos seus associados. A adoção de códigos de ética setorial e de programas próprios de integridade cada vez mais são exigências que devem ser cumpridas também pelas associações. A corrupção deve ser combatida igualmente pelas entidades setoriais.

ÉTICA *VERSUS COMPLIANCE* (Fig. 3.2)

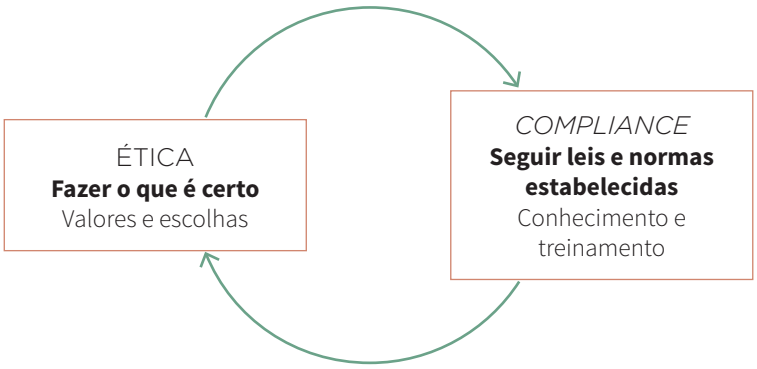


Figura 3.2. Comparativo e imbricações de ética e *compliance*.

Em recente artigo publicado no jornal *Valor Econômico*, Jean-Claude Trichet, presidente do conselho e executivo-chefe do Grupo dos Trinta e ex-presidente do Banco Central Europeu (BCE) e do Banco da França, afirmou estar convencido de que os eventos que desencadearam a crise financeira mundial de 2008 configuraram uma lista de falhas culturais e que, apesar das medidas até agora adotadas para fortalecer o sistema financeiro, ainda resta uma profunda debilidade cultural, no sentido de assumir riscos elevados.

Trichet (2015) afirmou ainda que fortalecer a conformidade legal (*compliance*) não é suficiente; é necessário que mudanças reais alcancem a essência das operações cotidianas de uma instituição. Para ele, é preciso que os bancos alterem as práticas de remuneração que recompensam os riscos excessivos, protejam aqueles que denunciam irregularidades, recrutem e treinem colaboradores que exibam ética alinhada aos objetivos da companhia, bem como assegurem um papel mais ativo por parte dos diretores na supervisão. Requer muito tempo e trabalho estabelecer valores e mudar a cultura de uma companhia; para ter sucesso, é necessário mudar a mentalidade das pessoas e torná-las habituadas à autorregulação.

O ex-presidente do BCE acredita que um código de conduta e ética é parte desta missão, mas por si só não é suficiente. É necessária a constante lembrança por meio de recados e repetições. Os colaboradores precisam entender instintivamente o que pode ou não ser feito, internalizando uma cultura que valorize o respeito a altos padrões éticos de conduta.

Deste modo, Trichet acredita que é essencial que a cultura e os valores de uma companhia sejam parte integral de suas decisões de contratação, demissão e promoção, representando 50% da avaliação anual de desempenho de seus colaboradores. “Deixar de corresponder às normas culturais desejadas de um banco deveria ter impacto na carreira do funcionário – e, quando preciso, encerrá-la” (Trichet, 2015).

As ponderações de Trichet não são aplicáveis somente ao setor financeiro, mas a qualquer segmento empresarial. Sem um profundo trabalho que permita internalizar nas organizações uma cultura ética sólida, a função da *compliance*, por si só, não será eficaz no sentido de prevenir práticas e condutas lesivas aos interesses da sociedade.

A existência de um código de ética, ou de conduta, e sua divulgação aos funcionários são elementos fundamentais em uma organização moderna, mas também não suficientes para garantir a internalização da cultura ética, esta sim essencial a sua sustentabilidade. Para que a cultura ética seja entranhada em todos os níveis é importante que as organizações contem com uma gestão interna da ética, desempenhada por uma comissão atuante, composta por funcionários de reconhe-

cida competência, respeitabilidade e expressão nas funções que desempenham, de preferência com participação direta de dirigentes ou, se isso não for possível, que estes ao menos acompanhem de perto seus trabalhos e mantenham permanente suporte (patrocínio) à comissão.

A atuação da comissão deve contemplar:

- Realização de reuniões com periodicidade definida (de pelo menos uma vez ao mês).
- Pronta resposta às dúvidas e demandas de funcionários, colaboradores, clientes ou qualquer outra pessoa, mesmo as que não tenham relacionamento direto com a organização.
- Investigação profunda, isenta e em caráter sigiloso das denúncias que lhe sejam encaminhadas.
- Publicidade de decisões e processos, preservando o sigilo em relação aos envolvidos.
- Realização periódica de cursos, palestras e *workshops*, formatados de forma a alcançar o maior número de funcionários e colaboradores.
- Atualização permanente do código de conduta, uma vez que o padrão de conduta ética é dinâmico, em constante processo de evolução, ganhando novos contornos a cada dia.

Para garantir que a cultura ética se consolide na organização, é essencial também a existência de canais de denúncia confiáveis, que preservem o sigilo dos denunciantes e denunciados e, até mesmo, que permitam acolher denúncias anônimas. Sem isso, dificilmente funcionários que compõem a base da pirâmide se sentirão encorajados a denunciar atos ou práticas que envolvam seus superiores. Esses canais devem combinar opções de atendimento presencial, telefônico ou via correio eletrônico.

É importante ainda que a comissão de ética se empenhe na construção de uma forte parceria interna com outros setores da organização – tais como as áreas de *compliance*, auditoria, jurídica e recursos humanos – e também na articulação externa com organizações congêneres, institutos especializados, fóruns de debate, auditorias independentes etc.

Como frisou Trichet (2015), a sedimentação da cultura ética em uma organização não é processo simples nem instantâneo, ao contrário, leva tempo, exige criterioso planejamento, boas doses de dedicação e paciência, mas, uma vez alcançada, os benefícios serão muitos e palpáveis, entre eles:

- Maior capacidade de governança corporativa, facilitando o entendimento e aumentando a confiança entre funcionários e gestores.
- Aumento da confiança e do respeito de clientes, de parceiros e da sociedade em geral.

- Melhoria significativa do clima organizacional.
- Mitigação do risco de imagem e preservação da reputação da organização.

Em síntese, podemos afirmar que a sobrevivência e a evolução das organizações modernas e de seus negócios cada vez mais dependem da capacidade de adotarem e aperfeiçoarem condutas éticas marcadas pela seriedade e justiça social, pela preservação da integridade e dos direitos individuais.

No momento de grave crise moral atravessado por nosso país, a responsabilidade social e o compromisso com a conduta ética passam a ser uma exigência, um "selo" que toda organização deve ter, sem o qual dificilmente terá condições de se lançar ou mesmo de se manter nos mercados interno e externo.

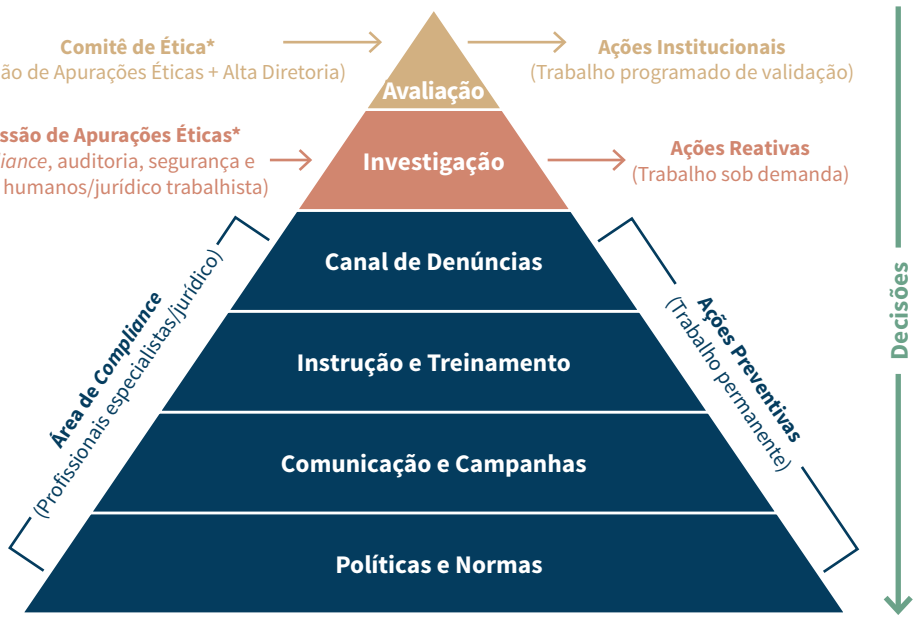
No desenvolvimento de políticas de integridade é importante estabelecer e incutir na cultura da instituição a obediência à conduta da conformidade, com base na ética, valorizando o respeito, a transparência e a aplicação das leis, ou seja, estimular o comportamento que deve ser valorizado e praticado.

A informação ativa voltada para toda a corporação é um requisito. Sem expressar para todos quais parâmetros devem ser obedecidos e demonstrar que a liderança assume o compromisso com essas diretrizes, não será possível consolidar tal processo, que deve ser contínuo. As boas práticas têm que ser explicitadas como um ganho para toda a instituição.

Esse compromisso deve contaminar toda a estrutura organizacional. Respeitados os parâmetros éticos, com certeza será alcançado um ambiente de trabalho motivador e formador de uma equipe segura de seus objetivos.

Saber que a instituição define e obedece a padrões éticos, de respeito à lei, é fator de segurança e continuidade. Princípios e valores são permanentes e enaltecem a credibilidade da instituição.

SEGURANÇA EMPRESARIAL E ATUAÇÃO DENTRO DAS PRÁTICAS DE *COMPLIANCE* (Fig. 3.3)



*Liderança da área de *compliance* e decisões coletivas (grupo).
**Coordenação da área de *compliance* e decisões colegiadas (institucionais).

Figura 3.3. Segurança Empresarial e atuação dentro das práticas de *compliance*.

Os avanços das empresas do setor privado nas ações de prevenção de perdas dentro dos seus departamentos impulsionam seus profissionais a buscar soluções para atuar com maior pró-atividade e assegurar seus direitos quando ameaçados por colaboradores próprios, terceirizados e fornecedores em geral, que agem de forma irregular e, por vezes, ilegal para obter vantagem indevida em prejuízo das corporações.

A realidade da legislação trabalhista no Brasil admite que as empresas somente possam exercer a defesa dos seus interesses dentro de políticas claras, formais e previamente estabelecidas com seus trabalhadores. Os processos de investigação interna, auditoria e produção de depoimentos para um procedimento sindicante somente são válidos com a devida normatização e formalização dos seus atos, de forma a tratar todos assuntos de forma indistinta e imparcial.

Referido grupo de pessoas deve ser composto por profissionais de liderança estratégica nas áreas de riscos, perdas, segurança, auditoria, jurídico e recursos humanos (RH).

Um processo sindicante pode ser realizado em qualquer momento de uma investigação ou apuração administrativa interna, desde que as áreas responsáveis pela

condução do procedimento entendam que há elementos suficientes para realizar o ato. Assim, as prerrogativas de validade incluem:

- Formalidade procedimental (registro, local, componentes, metodologia).
- Formalidade na constituição do local designado à tomada de depoimentos.
- Formalidade na disposição física dos componentes para a tomada de depoimentos.
- Formalidade na ordem da coleta de depoimentos.
- Formalidades documentais (ato de abertura, termo de declarações e relatório final).
- Comitê de Ética e Relações Trabalhistas devem ser os coordenadores do ato formal.
- Padronização corporativa (*template*, logos e outros itens de identificação documental).
- Impessoalidade nos depoimentos (não pode haver manifestações pessoais, apenas perguntas).
- Trabalho executado e deliberado em equipe (decisões emanadas por atas).
- Decisão final colegiada através dos membros do Comitê de Ética.

PROCEDIMENTO DE APURAÇÃO DE IRREGULARIDADES (Quadro. 3.1)

MODALIDADES

Todo procedimento de apuração de irregularidades contempla o início pela apuração preliminar, e conforme a necessidade e aprovação da Comissão de Apurações Éticas seguirá para a instrução por depoimentos.

APURAÇÃO PRELIMINAR

- Entrevista de pessoas envolvidas na apuração e/ou testemunhas que serão resumidas em documento produzido pela Comissão de Apurações Éticas.
- Realizada para simples Apuração de Irregularidades, cujo procedimento subsidiará o Comitê de Ética e auxiliará na tomada de decisões.
- Necessidade de análises de tecnologia da informação (TI), perito, investigação pessoal, entre outras.

INSTRUÇÃO POR DEPOIMENTOS

- A tomada de depoimentos pode ser necessária para subsidiar uma demissão ou uma futura ação judicial. O ato deve ser espontâneo, apresentando-se ao entrevistado a opção de não realizá-lo.
- Os depoimentos deverão ser colhidos por termo em documento próprio, devendo estar fielmente descrita a fala do entrevistado. O ambiente de realização do depoimento deve estar localizado dentro da corporação, em área de acesso comum a outros colaboradores.
- No final do termo de depoimento, o entrevistado (testemunha ou envolvido) deve ler e assinar o documento, rubricando todas as folhas.

- O depoimento do entrevistado só pode ser prestado em horário de funcionamento da empresa, e nunca fora do expediente.
- No termo de depoimento devem constar data, hora, local, número do ato de abertura, nome do depoente e qualificação (número de matrícula, cargo, função e área de atuação).
- Todo o depoimento tomado a termo deverá ser acompanhado por advogado da área jurídica da empresa e representante da gerência de recursos humanos e do gestor do empregado.

PARECER FINAL

- Documento com parecer técnico da Comissão de Apurações Éticas, indicando se houve negligência, imprudência, imperícia, dolo ou transgressão disciplinar.

OBJETIVO

- Avaliar os fatos apurados e disponibilizá-los ao Comitê de Ética, que validará as ações propostas para o encerramento do procedimento de apuração de irregularidades.

PRAZOS

- Conclusão da apuração não excederá 30 dias.
- Início na data do recebimento do ato de abertura pela Comissão de Apurações Éticas.
- Possível prorrogação por igual período a critério da Comissão, mediante solicitação ao Comitê de Ética no mínimo 48 horas antes do término daquele inicialmente previsto.
- Nos casos em que há apuração com fortes evidências e admissibilidade da demissão por justa causa, a tomada de depoimentos deverá ocorrer em um prazo de até 7 dias a partir do ato de abertura.

CONFIDENCIALIDADE

- Não pode ser utilizado em qualquer hipótese para outros tipos de avaliação e/ou informação, bem como atos e decisões geradas por este não podem constar em cadastro dos envolvidos enquanto o colaborador for registrado pela empresa, terceiro alocado ou não na empresa, fornecedor ativo ou inativo.
- As informações referentes à existência do presente procedimento de apuração de irregularidades só poderão ser disponibilizadas às autoridades competentes por ordem judicial expressa e específica.

COMPLIANCE/JURÍDICO
• Coordenação das ações e apresentação dos resultados ao Comitê de Ética. • Organização, manutenção e coordenação do ritmo de trabalho. • Análise jurídica de documentos internos e externos. • Intermediação do uso de assessoria jurídica externa.
AUDITORIA INTERNA
• Condução de análises internas sobre conformidade de procedimentos e processos. • Análise de números financeiros e contábeis dentro dos procedimentos corporativos. • Realização de questionamentos técnicos sobre as áreas envolvidas na apuração. • Intermediação do uso de assessorias contábil e financeira externas. • Condução de entrevista e depoimentos, quando aplicável.
RECURSOS HUMANOS/RELAÇÕES TRABALHISTAS
• Análise da situação funcional dos empregados submetidos ao procedimento de apuração de irregularidades. • Assessoria da tomada de depoimentos formais de colaboradores internos em todos os casos, sendo responsável como mediador. • Análise dos riscos na(s) ação(ões) de desligamento da(s) pessoa(s) na esfera trabalhista, quando aplicável.
SEGURANÇA EMPRESARIAL/ SEGURANÇA DA INFORMAÇÃO
• Realização de ações externas e em banco de dados privilegiados, quando necessário à apuração. • Intermediação do uso de assessoria especializada em investigação ou inteligência externa. • Intermediação dos contatos com autoridades de polícia judiciária, quando necessário à apuração. • Condução de investigação interna com recursos técnicos de controle da segurança patrimonial na corporação.

Quadro 3.1. Áreas que compõem a Comissão Interna de Apurações Éticas e suas respectivas atribuições.

DEZ LIÇÕES DE *COMPLIANCE* PARA SEGURANÇA EMPRESARIAL

1. COMPROMETIMENTO *TOP-DOWN*

A primeira condição unanimemente reconhecida para a efetiva implementação de qualquer regra ou regulamento com enfoque baseado em *compliance* é o comprometimento *top-down*: a alta direção deve se comprometer verdadeiramente com a adoção da correspondente política e assegurar sua implementação efetiva, fazendo chegar essa mensagem a todos os seus colaboradores. Tal mensagem não pode se restringir a uma mera declaração, deve ser veiculada de maneira eficaz, acompanhada dos meios necessários para sua materialização efetiva. Em suma, não pode ser apenas uma declaração de comprometimento inócua.

2. MUDANÇA CULTURAL

A implementação de políticas de prevenção de lavagem de dinheiro e combate ao financiamento do terrorismo, bem como políticas anticorrupção, tem provado que um dos fatores fundamentais para seu sucesso é a concretização de uma mudança na cultura da empresa em todos os níveis. Os colaboradores têm que se conscientizar sobre as necessidades dessas mudanças e não considerar que são apenas ações que tomam um tempo preciso em um processo, de certa forma, não produtivo. Tal percepção tenderá a dissipar-se à medida que esses novos processos se integrem a sua rotina e tornem-se naturais, porém realizados de maneira consciente no que diz respeito a sua finalidade. Em última análise, essa nova cultura deveria permear a própria identidade da empresa.

3. *COMPLIANCE OFFICER*

É marcante o número cada vez maior de empresas que anunciam vagas de *compliance officer* e, nas grandes empresas, de *compliance chief officer* (CCO). Trata-se de uma tendência global contemporânea da preocupação constante com os resultados imprevisíveis, mas com alto potencial de desgaste e custo. Segundo a PricewaterhouseCoopers (PwC), no *2014 State of Compliance Survey*, o papel do CCO adquiriu mais proeminência na última década e aumenta rapidamente, sendo que seu foco tende a compreender outras questões que simplesmente prevenir a corrupção e garantir o respeito de códigos de conduta, desempenhando papel mais estratégico na organização (Starr, s/d). A existência e efetividade do *compliance officer* tem se tornado elemento importante da imagem e reputação da empresa, espelhando o compromisso da alta direção. Ademais, é fator importante para a valorização da mudança cultural e sua disseminação.

4. ENFOQUE BASEADO NO RISCO

O *compliance* tradicional ensina que o enfoque baseado no risco (RBA, *risk-based approach*) permite alocar os recursos adequados, necessários e suficientes para a identificação dos riscos, diretos e indiretos (de fornecedores, parceiros, clientes e outras partes interessadas), e a definição de prioridades. O RBA é fator essencial para a solidez do *compliance* e crucial para fins de prova perante foros administrativos e/ou judiciais, pois uma política de *compliance* construída ou aplicada sobre riscos inexistentes ou mal avaliados é o mesmo que uma não política. No entanto, é sobretudo por razões de segurança – dos processos, jurídica, financeira, da sua reputação e dos negócios – que o RBA deve ser adotado.

5. *CUSTOMER DUE DILIGENCE*

Os colaboradores de uma empresa representam um capital-chave da organização e também um dos principais fatores de riscos do negócio. Assim, as empresas dedicam especial atenção à contratação de pessoas competentes, diligentes e aderentes aos valores da organização. O *compliance* – em matéria de prevenção da lavagem de dinheiro e combate ao financiamento do terrorismo e à corrupção – tornou evidente a necessidade de aplicar a mesma diligência para o conhecimento dos clientes *lato sensu*, incluindo não apenas os clientes em si, mas os colaboradores internos, que representam a empresa de forma mais destacada, e também os colaboradores externos, terceirizados, fornecedores e acionistas.

Esse processo, conhecido como "conheça seu cliente" (KYC, *know your customer*), contempla a fase inicial (identificação e verificação) da *customer due diligence* (CDD), a qual visa conhecer as atividades do cliente (*lato sensu*). Para tanto, é necessária a definição de perfis e sua observância em todas as contratações de pessoas e serviços ou nos negócios (vendas, parcerias etc.). Em determinados casos de riscos mais significativos, definidos na política de *compliance*, deverá proceder-se a uma CDD mais completa (conhecida como EDD, *enhanced due diligence*), sendo fundamental definir ainda o momento em que a CDD ou, se for o caso, a EDD deverá ser realizada. Tratar igualmente riscos distintos quanto a sua gravidade pode tornar o *compliance* frágil, tanto em sua eficácia quanto em sua utilidade como fator atenuante ou mesmo excludente de responsabilidade perante foros administrativos e/ou judiciais.

6. POLÍTICAS, PROGRAMAS E PROCESSOS

Há unanimidade de que as empresas devem definir princípios básicos e orientações, formalizando políticas específicas de *compliance* e não simples anexos

de outras políticas. Elas poderão conter ou coexistir com códigos de ética e de conduta. Cabe à alta direção tais definições e orientações, bem como estabelecer prioridades. As ações baseadas nessas políticas devem ser planejadas em programas destinados a garantir melhorias mediante intervenções a curto, médio e longo prazos. Será necessário definir processos ou adaptar os existentes, incluindo seu aprimoramento e revisão sistemática.

7. REPORTE DE SUSPEITAS

A própria finalidade do *compliance* implica na consideração não apenas das violações apuradas das normas aplicáveis, mas igualmente no tratamento das suspeitas de violações. O *benchmarking* das melhores práticas de *compliance* ensina que é fundamental que o reporte de tais suspeitas:

- Seja obrigatório e imediato.
- Contemple também as tentativas de violações.
- Esteja baseado em processos claros e formulários aprovados.
- Seja objeto de treinamento interno.
- Constitua prática normal dos processos internos de *compliance*.
- Seja feito observando a confidencialidade necessária.
- Seja escalonado e acompanhado segundo procedimento pré-definido.

8. PROCEDIMENTOS DE DOCUMENTAÇÃO CONSISTENTE

Todas as fases dos procedimentos de *compliance* devem ser documentadas de maneira consistente, pois a própria ação de documentar as etapas seguidas constitui elemento essencial do processo. Dispor de procedimentos de documentação consistentes é essencial para:

- Efetivo conhecimento, memória e embasamento para prosseguimento ou medidas subsequentes.
- Diferencial de mercado, pois cada vez mais as empresas que comprovadamente disponham de uma política de *compliance* efetivamente implementada serão preferidas às demais.
- Instrução dos processos internos.
- Eventual prova em foros administrativos e/ou judiciais.
- Avaliação e melhoria do *compliance*.
- Fins estatísticos e, portanto, priorização de ações e elaboração de programas.

Cabe observar que as empresas que dispõem de políticas de *compliance*, mas as implementam sem nunca detectar falhas em seus processos ou sem documentar decisões de não contratação podem ser comparadas a empresas que

não dispõem de tais políticas ou não as implementam. Isso demonstra que, em *compliance*, a documentação do "não" é fundamental.

9. DISSEMINAÇÃO E TREINAMENTO

Compliance não é um processo isolado, nem se restringe a determinadas pessoas na empresa. Deve estar em todos os seus níveis, começando pela alta direção. A disseminação da mensagem de comprometimento da alta direção com o *compliance* até sua efetiva implementação é essencial para a mudança cultural que deve assegurar seu sucesso. Tanto a razão de ser do *compliance* como seu contexto e objetivos devem ser disseminados mediante o efetivo envolvimento da totalidade da empresa e, quando for o caso, de terceiros em treinamentos regulares (no mínimo anuais) e aprofundados para cada área, de acordo com os processos de sua competência, ensejando *feedbacks* relevantes para o próprio aprimoramento do treinamento e dos processos de *compliance*.

A documentação de tais treinamentos, incluindo a comprovação da presença de todos os colaboradores, constitui elemento comprobatório essencial como fator excludente ou atenuante de responsabilidade em eventuais processos administrativos e/ou judiciais. Por fim, a disseminação e o treinamento repercutem na reputação da empresa, pois cada colaborador é sempre um embaixador da organização em que trabalha.

10. CONTINUIDADE DO PROCESSO

O *compliance* não é um produto de prateleira, mas um processo contínuo. Grandes, médias e pequenas empresas devem implementá-lo. O aprimoramento deve ser contínuo e refletir o comprometimento da empresa.

O fato de ser um processo contínuo fortalece a cultura de *compliance* e a identidade corporativa nesse aspecto, além de permitir a avaliação e o aprimoramento, ensejando melhor custo/benefício das medidas adotadas.

Essas 10 lições de *compliance* para a Segurança Empresarial apresentadas de maneira sucinta demonstram que fazer economia na adoção do *compliance* significa desprezar uma das mais úteis ferramentas de Segurança Empresarial, tanto em termos reputacionais quanto em termos jurídicos, financeiros e, logicamente, operacionais.

As experiências mais desenvolvidas de *compliance*, observadas com relação à prevenção da lavagem de dinheiro e ao combate à corrupção, fornecem lições significativas sobre os elementos essenciais do *compliance*.

Tais lições mostram que não apenas as multinacionais ou grandes empresas podem e devem adotar o *compliance*, mas que também as médias e pequenas empresas devem fazê-lo, envolvendo-se em um processo paulatino de adoção do processo.

O futuro deverá ser o da realidade do *compliance* como elemento natural dos processos corporativos, em função do nível de assimilação e implementação das lições aqui compartilhadas.

INCENTIVOS PARA O *COMPLIANCE* NAS EMPRESAS

Alguns detalhes são importantes para que o processo de *compliance* seja implantado nas empresas (Fig. 3.4):

- Adotar o método de avaliação 360°.
- Criar bônus para os agentes do *compliance* e para os que o seguem. As metas devem ser realistas.
- A alta direção deve implementar um programa de capacitação contínua (presencial e/ou ensino a distância [EAD]) sobre este tema (com lista de presença, conteúdo programático e avaliação).
- O presidente da empresa deve incentivar os treinamentos. Uma forma bastante simples é, na abertura de um treinamento, apresentar a palavra do presidente, de forma presencial ou por vídeo.
- Deve-se ressaltar e deixar claro em qualquer treinamento que não há jeito certo para fazer a coisa errada.
- Implantar a cultura de se registrar sempre as ações de não fazer e também as razões de por que não fazer.

PLANEJAMENTO

IDENTIFICAÇÃO
- Existência de vontade da alta direção – decisão do negócio.
- Identificação da necessidade de CE&C com base no escopo do projeto.
- Nomeação de representante do CE&C, que carregue o interesse da corporação e/ou proprietários.
- O representante deve ser *expert* no tema.
- Estimação do custo do projeto para implantação, treinamento, manutenção e atualização.

IDENTIFICAÇÃO DE OPORTUNIDADES

INÍCIO DO PROJETO
- Revisar os riscos, caso existam.
- Projeto significa subir degraus.
- Levantar atuais riscos.
- Iniciar projeto com *draft* do que será o CE&C com base em leis vigentes e boas práticas do mercado.
- Comunicar à empresa que haverá um CE&C.

DESENVOLVIMENTO

PLANEJAMENTO DO PROCESSO
- Nomear internos para trabalhar no relatório do CE&C.
- Internos e consultoria alinham os primeiros passos do CE&C. *Draft* é feito.
- CE&C apresenta *draft* à alta gestão para alinhamento e eventual correção de rumo.

CRIAÇÃO

EXECUÇÃO E CONTROLE
- Iniciar *fine tunning* do *draft*.
- Submeter a alta gestão a treinamentos com o CE&C.
- Internos e consultoria alinham os primeiros passos do CE&C e continuam com correções ao plano original.
- Iniciar treinamento em todos os níveis hierárquicos.
- Executar CE&C com prêmios e denúncias.
- Dar suporte a qualquer iniciativa positiva.

ENTREGA E CONTINUIDADE

FINALIZAÇÃO
- Certificação por órgãos reconhecidos.
- Envolvimento de terceiros e premiação de funcionários por boas práticas.
- Informar a mídia e concorrentes.
- Implantação de política de tolerância zero.

Figura 3.4. Implantação do Código de Ética e *Compliance* (CE&C).

O momento atual não poderia ser mais desafiador para as empresas e para a administração pública brasileiras. Está provado que práticas e costumes ilegais e antiéticos até aqui aceitos em benefício de ganhos imediatos acarretam resultados desastrosos.

Hoje está explícito que a corrupção de parte dos componentes do poder público e de alguns empresário é um dos grandes motivos que inviabilizam investimentos, geração de empregos e renda. Tais práticas acarretam também a falta de serviços públicos e a desvalorização e falência de empresas públicas e privadas, chegando a abalar o futuro do país.

O fortalecimento da ética e do respeito às leis deve ser referência para todos. A sociedade brasileira, sempre leniente com seu próprio comportamento, tem que mudar seus conceitos. De um lado, somos rápidos em condenar o erro dos outros, e de outro, sempre prontos para defender nossos comportamentos errados. Precisamos exercitar uma verdadeira coerência ética, não aceitar e não praticar o que é errado, o que fira o sentido de respeito e responsabilidade em todas as esferas.

Estabelecer novos padrões de convivência ética é imperioso. A ação empresarial deve acompanhar e cumprir os postulados éticos e exigir que o poder público faça o mesmo. Precisamos, enfim, assumir um projeto de nação que valorize os ganhos obtidos de modo leal e lícito.

CONSIDERAÇÕES FINAIS

Os três dias de debates provaram aquilo que já está sendo observado pelo mercado há algum tempo. A Segurança Privada é muito importante para a continuidade da Indústria brasileira. Quando bem planejada e bem implantada, ela é responsável pela diminuição de perdas e pelo aumento imediato dos lucros.

Mostrou-se, por outro lado, que quando implantada sem ter como guia as melhores práticas mundiais, sem seguir a legislação específica e sem o devido planejamento, a Segurança Privada se torna mais uma despesa, que vai, inclusive, impactar no custo final do produto.

A união entre Seguranças Pública e Privada permite, de maneira mais eficiente e eficaz, diminuir as perdas internas e externas e atacar de forma mais efetiva o contrabando e as falsificações, que podem trazer prejuízos bilionários à Indústria. A Segurança Privada não deve agir apenas durante a produção e o armazenamento dos produtos, mas sim dentro de toda a cadeia logística, norteando toda a operação, diminuindo perdas diretas, reduzindo os custos do transporte e armazenagem, custos com seguros e até mesmo com impostos.

A segurança deve ser vista como um todo, como um processo contínuo e inserido em todas as áreas: pesquisa e desenvolvimento (P&D), área comercial, risco de furto de informações/espionagem industrial, compras, produção, distribuição, armazenamento, até a chegada ao cliente final. E os profissionais vêm se especializando cada vez mais para isso. Melhores práticas mundiais, programas (graduação e pós-graduação – presenciais e a distância) e certificações (nacionais e internacionais) diminuem a probabilidade de perdas, agilizam as exportações e, consequentemente, aumentam os lucros.

Proteção das informações é outro assunto que deve ser levado a sério, pois a fuga de dados causa prejuízos elevados e pode macular a imagem das empresas. O uso da tecnologia é uma realidade que deve ser cada vez mais estudada.

Ética, *compliance*, governança são palavras e práticas que devem estar cada vez mais presentes nos negócios. As empresas devem se preocupar em implantá-las junto a seu público interno e fazer negócios preferencialmente com empresas que estejam alinhadas a práticas legais de mercado. E, por fim, é claro, a punição aos crimes deve ser rápida e severa, de forma que a sensação de impunidade não agrave ainda mais os altos níveis de criminalidade de nosso país.

BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 9.000:** sistemas de gestão de qualidade – fundamentos e vocabulário. Rio de Janeiro, 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 22.301:** segurança da sociedade – sistema de gestão da continuidade de negócios – requisitos. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 27.000:** tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação – fundamentos e vocabulário. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 28.000:** especificação para sistemas de gestão de segurança para a cadeia de logística. Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31.000:** gestão de riscos – princípios e diretrizes. Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE OUVIDORES/OMBUDSMAN. Quem Somos. Disponível em: www.abonacional.org.br/quem-somos. Acesso em: 07/04/2017.

BERTOCCELI, R. P. Empresas começam a entender que são parte do combate à corrupção, 2016. Disponível em: http://noticias.uol.br/opiniao/coluna/2016/08/17/empresas-comecam-a-entender-que-sao-parte-do-combate-a-corrupcao.htm. Acesso em: 23/11/2016.

BRASIL. Banco Central. **Resolução nº 3.380**, de 29 de junho de 2006. Dispõe sobre a implementação de estrutura de gerenciamento de risco operacional. Disponível em: http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_L.pdf. Acesso em: 15/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 13/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 7.102**, de 20 de junho de 1983. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para a constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L7102.htm. Acesso em: 24/02/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. **Lei nº 8.429**, de 2 de junho de 1992. Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8429.htm. Acesso em: 15/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. **Lei nº 8.666**, de 21 de junho de 1993. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8666cons.htm. Acesso em: 15/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. **Lei nº 9.426**, de 24 de dezembro de 1996. Altera dispositivos do Decreto-lei nº 2.848, de 7 de dezembro de 1940 – Código Penal – Parte Especial. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9426.htm. Acesso em: 29/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. **Lei nº 10.637**, de 30 de dezembro de 2002. Dispõe sobre a não cumulatividade na cobrança da contribuição para os Programas de Integração Social (PIS) e de Formação do Patrimônio do Servidor Público (Pasep), nos casos que especifica; sobre o pagamento e o parcelamento de débitos tributários federais, a compensação de créditos fiscais, a declaração de inaptidão de inscrição de pessoas jurídicas, a legislação aduaneira, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10637.htm. Acesso em: 13/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. **Lei nº 10.833**, de 29 de dezembro de 2003. Altera a Legislação Tributária Federal e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/L10.833compilado.htm. Acesso em: 13/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 12.815**, de 5 de junho de 2013. Dispõe sobre a exploração direta e indireta pela União de portos e instalações portuárias e sobre as atividades desempenhadas pelos operadores portuários; altera as Leis nºs 5.025, de 10 de junho de 1966,

10.233, de 5 de junho de 2001, 10.683, de 28 de maio de 2003, 9.719, de 27 de novembro de 1998, e 8.213, de 24 de julho de 1991; revoga as Leis nºs 8.630, de 25 de fevereiro de 1993, e 11.610, de 12 de dezembro de 2007, e dispositivos das Leis nºs 11.314, de 3 de julho de 2006, e 11.518, de 5 de setembro de 2007; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/Lei/L12815.htm. Acesso em: 09/03/2017.

BRASIL. Presidência da República. Casa Civil. Subchefia de Assuntos Jurídicos. **Lei nº 12.846**, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm. Acesso em: 09/03/2017.

BRASIL. Receita Federal. **Instrução Normativa RFB nº 1.521**, de 4 de dezembro de 2014. Institui o Programa Brasileiro de Operador Econômico Autorizado e altera a Instrução Normativa SRF nº 248, de 25/11/2002. Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=59000&visao=a. Acesso em: 09/03/2017.

BRASIL. Receita Federal. **Instrução Normativa RFB nº 1.598**, de 9 de dezembro de 2015. Dispõe sobre o Programa Brasileiro de Operador Econômico Autorizado. Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=70204&visao=anotado. Acesso em: 09/03/2017.

BRASIL. Receita Federal. **Instrução Normativa RFB nº 1.624**, de 1º de março de 2016. Altera a Instrução Normativa RFB nº 1.598, de 9 de dezembro de 2015, que dispõe sobre o Programa Brasileiro de Operador Econômico Autorizado. Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=71919. Acesso em: 14/03/2017.

BRASIL. Receita Federal. **Portaria RFB nº 768**, de 5 de junho de 2015. Dispõe sobre a marca do Programa Brasileiro de Operador Econômico Autorizado. Disponível em: http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=64968&visao=anotado. Acesso em: 14/03/2017.

BRASIL tem pior controle da corrupção em 10 anos, diz Banco Mundial. **BBC Brasil**, 10 jul. 2007. Disponível em: http://www.bbc.com/portuguese/reporterbbc/story/2007/07/070710_corrupcao_bird_dg.shtml. Acesso em: 22/03/2017.

CANDELORO, A. P. P.; DE RIZZO, M. B. M.; PINHO, V. **Compliance 360°**. 2ª ed. São Paulo: Trevisan, 2012.

CRIMES virtuais provocam perda anual de US$ 8 bilhões a empresas brasileiras. **Jornal do Brasil**, Rio de Janeiro, 5 abr. 2016. Ciência e Tecnologia. Disponível em: http://www.jb.com.br/ciencia-e-tecnologia/noticias/2016/04/05/crimes-virtuais-provocam-perda-anual-de-us-8-bilhoes-a-empresas-brasileiras/. Acesso em 02/03/2017.

FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO. Departamento de Competitividade e Tecnologia. **Corrupção:** custos econômicos e propostas de combate, 2010. Disponível em: http://www.fiesp.com.br/indices-pesquisas-e-publicacoes/relatorio-corrupcao-custos-economicos-e-propostas-de-combate/. Acesso em: 04/04/2017.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2014**. São Paulo: Fórum Brasileiro de Segurança Pública 2014. Disponível em: http://www.forumseguranca.org.br/storage/8_anuario_2014_20150309.pdf. Acesso em: 24/02/2017.

MANSO, B.P.; BRANCATELLI, R. Em SP, 95% dos crimes ficam impunes. **O Estado de São Paulo**, 16 jul. 2010. Disponível em: http://sao-paulo.estadao.com.br/noticias/geral,em-sp-95-dos-crimes-ficam-impunes,581914. Acesso em: 13/04/2017.

MILHORANCE, F. Oito lições de combate à corrupção que a Dinamarca pode dar ao Brasil. **BBC Brasil**, 27 jan. 2016. Disponível em: http://www.bbc.com/portuguese/noticias/2016/01/160126_dinamarca_corrupcao_fm_ab. Acesso em: 07/04/2017.

PIPOLO, I. Segurança Pública e violência custam bilhões para o país. **LinkedIn**, São Paulo, 16 ago. 2016. Disponível em: https://www.linkedin.com/pulse/seguran%C3%A7a-p%C3%BAblica-e-viol%C3%AAncia-custam-bilh%C3%B5es-para-o-pipolo-ads-ase?articleId=9163507464214302221. Acesso em: 24/02/2017.

STARR, R. The fourth anual PwC State of Compliance 2014 Survey finds CCOs arranging a place at the table. **Big 4**, s/d. Disponível em: http://www.big4.com/news/uncategorized/fourth-annual-pwc-state-compliance-2014-survey-finds-ccos-arranging-place-table/. Acesso em: 17/03/2017.

TRICHET, J. Como corrigir a cultura bancária. **Valor Econômico**, São Paulo, 10 set. 2015. Disponível em: http://www.pressreader.com/brazil/valor-econ%C3%B4mico/20150910/281736973230496. Acesso em: 16/03/2017.

ENTIDADES

Associação Brasileira de Profissionais de Segurança (Abseg). Fundada em 2005, com o propósito de levar conhecimento, aprimoramento profissional e integração aos profissionais de Segurança Privada. Possui forte atuação em defesa, reconhecimento e valorização dos profissionais de segurança. Mantém a certificação de Analista de Segurança Empresarial (ASE), com foco na Gestão de Segurança.

Federação das Indústrias do Estado de São Paulo (Fiesp). É a maior entidade de classe da indústria brasileira. Representa cerca de 130 mil indústrias de diversos setores, de todos os portes e das mais diferentes cadeias produtivas, distribuídas em 131 sindicatos patronais. Principal interlocutora do setor produtivo e um dos maiores símbolos da Indústria, atua de forma a fortalecer o parque industrial brasileiro, aumentar a competitividade e respeitar o meio ambiente, promovendo o desenvolvimento da economia nacional e da sociedade como um todo.

COLABORADORES

Aleksander Grievs. Engenheiro Eletricista. Especialista em Sistemas de Prevenção de Incêndio e Explosão. Especialista em Sistemas Integrados de Segurança. Consultor Sênior em Segurança Empresarial. Membro da Associação Brasileira de Normas Técnicas (ABNT) CB24. Membro da National Fire Protection Association (NFPA). Presidente da Associação Brasileira de Prevenção de Incêndio (ABPI). Sócio-fundador e Diretor do Comitê de Prevenção de Incêndio e Explosão da Associação Brasileira de Profissionais de Segurança (Abseg). Professor do Curso de Pós-graduação em Saúde, Segurança do Trabalho e Professor Coordenador do Curso de Proteção contra Incêndio – Extensão Universitária (Brasiliano & Associados/Fundação Escola de Comércio Álvares Penteado [Fecap]/Centro de Estudos Álvares Penteado [Ceap]).

Anderson Fagundes da Silva. Analista de Segurança Empresarial (ASE) pela Associação Brasileira de Profissionais de Segurança (Abseg), Certificado pela Chartered Institute for Securities & Investment Combate ao Suborno e Corrupção (Cisi-UK), certificado pela Port Facility Security Officer (PFSO), Senior Executives in National and International Security na Universidade Harvard Kennedy School (NIS), certificado pela Global Institute for Risk Management Standards (G31000), Gerente de Segurança Portuária na Santos Brasil. Diretor da Associação Brasileira de Profissionais de Segurança (Abseg). Árbitro do Centro Brasileiro de Arbitragem Marítima (CBAM). Membro do Overseas Security Advisory Council (Osac). Oficial R2 do Exército Brasileiro. Bacharel em Direito. Pós-graduado em Segurança, Violência e Criminalidade pela Universidade Federal do Rio Grande do Sul (UFRGS). MBA em Gestão de Riscos e *Compliance* pela Trevisan Escola de Negócios. Senior Executives in National and International Security pela Universidade de Harvard. MBA em Gestão de Segurança Privada nas Organizações pelo Centro Universitário da Serra Gaúcha (FSG). Pós-graduado em Direito Penal e Processo Penal pela Universidade Gama Filho (UGF). Curso de Estudos de Política e Estratégia de Gestão pela Associação dos Diplomados pela Escola Superior de Guerra (Adesg). Especialização de Oficiais em Controle de Distúrbios Civis pela Polícia Militar do Estado de São Paulo. Certificação de Supervisor de Segurança Portuária (SSP – *ISPS Code*), emitida pela Comissão Nacional de Segurança Pública nos Portos, Terminais e Vias Navegáveis (Conportos) do Ministério da Justiça e Segurança Pública.

Antonio Carlos Hencsey. Analista de Segurança Empresarial (ASE), Certificado de Especialista em Segurança (CES). Psicólogo e Criminologista Empresarial. Coordenador e Docente do Curso de Pós-graduação de Gestão de Riscos de Fraudes Empresariais e *Compliance* da Fundação Instituto de Administração da Universidade de São Paulo (FIA-USP) e Docente do Curso de Pós-graduação em Inteligência Competitiva da Fundação Instituto de Pesquisas Econômicas (Fipe-USP). Gerente de *Compliance* e Inteligência empresarial da ICTS Protiviti. Possui Pós-graduação em Psicopatologia pela USP e pela Santa Casa de Misericórdia de São Paulo, MBA em Gestão de Riscos e Fraudes pela Faculdade de Engenharia São Paulo, Extensão em Política e Estratégia pela Associação dos Diplomados pela Escola Superior de Guerra (Adesg), Programme de Formation Continue Unethical Decision Making in Organizations pela HEC Lausanne – The Faculty of Business and Economics of the University of Lausanne. Curso de Forensic Accounting and Fraud Examination pela West Virginia University, além de outros cursos com foco em Criminologia e Análise de Comportamento Humano. Atua na área de Criminologia Corporativa e Riscos Humanos Empresariais há mais de 10 anos tanto nos segmentos de Inteligência Empresarial como em Processos de *Compliance* Individual e Avaliação de Riscos.

Antonio Russo Filho. Auditor Fiscal aposentado da Receita Federal do Brasil (RFB). Atuou na Alfândega de Santos, na Comissão Estadual de Segurança Pública nos Portos, Terminais e Vias Navegáveis (Cesportos) do Estado de São Paulo. Idealizou e implantou a Central de Operações e Vigilância (COV). Presta consultoria aduaneira nas atividades de logística de comércio exterior, especialmente auxiliando as empresas a obterem a certificação de operador econômico autorizado (OEA) na RFB.

Artur Coutinho. Engenheiro pelo Instituto Tecnológico da Aeronáutica (ITA), turma de 1971. Mestrado em Análise de Sistemas pelo Instituto de Pesquisas Espaciais (Inpe). Atuou nas seguintes companhias: Engesa, veículos especiais, (de 1976 a 1984); Engex, equipamentos de exploração de petróleo (de 1984 a 1987); Embraer, indústria aeronáutica (de 1988 a 2015); Camargo Corrêa, infraestrutura e construção (de 2015 a 2016).

Autair Iuga. Participa ativamente na política do segmento de Segurança Privada no Brasil. Presidente e Fundador do Grupo Macor, empresa que atua na Segurança Privada há 21 anos, tendo como sua principal atividade a escolta armada, destacando-se como a maior do Brasil. Vice-Presidente da Federação Nacional das Empresas de Segurança e Transporte de Valores (Fenavist) para Assuntos de Escolta Armada e Segurança Pessoal Privada 2007-2010 e 2014-2018. Diretor de Escolta Armada da Associação Brasileira das Empresas de Vigilância e Segurança (Abrevis). Diretor de Escolta Armada do Sindicato das Empresas de Segurança Privada, Segurança Eletrônica, Serviços e Curso de Formação de Vigilantes de São Paulo (Sesvesp), 2014-2018. Coordenador do Grupo da Comissão Consultiva de Escolta Armada para Assuntos junto à Polícia Federal pelo Sindicato das Empresas de Escolta do Estado de São Paulo (Semeesp). Presidente e fundador do Semeesp, 2010-2014 e 2014-2018. Membro do Comitê da Escolta na Associação Brasileira de Profissionais de Segurança (Abseg). Autor da Cartilha Nacional de Escolta Armada e Segurança Pessoal Privada. Formação e pós-graduação na Escola Superior de Sargentos da Policia Militar do Estado de São Paulo. Instrutor duplamente qualificado pela Special Weapons and Tatics (Swat), Estados Unidos. Membro colaborador do Pro-Carga Goiás.

Carlos Alberto de Souza. Coronel do Exército Brasileiro. Oficial de Inteligência do Comando do Exército. Instrutor da Escola de Inteligência do Exército. Diretor-Presidente da Security with Intelligence (Swint).

Christian de Lamboy. Sócio-diretor do Instituto ARC, com dez anos de experiência em desenvolvimento de serviços nas áreas Auditoria, Gestão de Risco e *Compliance*. Possui graduação e doutorado em Administração de Empresas (Goethe Universität Frankfurt/Frankfurt School of Finance & Management).

Christian Piiroja Visval. Publicitário. Diretor-geral da Revista *Segurança Eletrônica*. Palestrante. Diretor de Marketing da Associação Brasileira de Profissionais de Segurança (Abseg) e da Associação Latino-americana de Segurança (Alas), Brasil.

Claudio Weschler. *Certified Protection Professional* (CPP), *Certified Fraud Examiner* (CFE). Profissional de *Security and Safety* há mais de 25 anos, com experiências na área de combate à fraude, prevenção de perdas, análise de risco, proteção executiva, investigações, cultura de segurança, dentre outras. Experiência de trabalho internacional nas Américas do Norte e Latina, África do Sul e Reino Unido. Diretor de Segurança para as Américas da Unilever há dez anos, com experiências anteriores em multinacionais, como a British Gas.

Edson Luiz Vismona. Advogado. Graduado e Pós-graduado pela Faculdade de Direito da Universidade de São Paulo. Especialista em Defesa Comercial e Direito do Consumidor. Foi Secretário da Justiça e da Defesa da Cidadania do Estado de São Paulo (2000/2002) e Secretário Nacional da Reforma Agrária (2002). Fundador e Presidente da Associação Brasileira de Ouvidores/ *Ombudsman* (ABO). É membro do Conselho Nacional de Combate à Pirataria (CNCP), da Comissão de Combate à Pirataria da Ordem dos Advogados do Brasil (OAB-SP) e do Conselho de Ética do Instituto Ética-Saúde. Preside o Fórum Nacional contra a Pirataria e a Ilegalidade (FNCP) desde 2009 e o Instituto Brasileiro de Ética Concorrencial (ETCO), coordenando o Movimento em Defesa do Mercado Legal Brasileiro.

Euripedes Abud. Administrador pela Fundação Getúlio Vargas (FGV-SP) e MBA pela Fundação Dom Cabral. Consultor empresarial há 17 anos, com foco no segmento da Segurança Patrimonial Privada (Sindicato das Empresas de Segurança Privada, Segurança Eletrônica e Cursos de Formação do Estado de São Paulo [Sesvesp]). Possui 33 anos de experiência em licitações públicas e privadas, contratos e formação de preços e 13 anos de experiência como executivo do setor elétrico.

Fernando Só e Silva. CEO da Empresa Performance Lab® Sistemas. Diretor do Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Deseg-Fiesp). Membro da Diretoria da Associação Brasileira de Profissionais de Segurança (Abseg). Engenheiro e Mestre em Engenharia de Processos. Autor do livro *Competitividade em Segurança Empresarial*, Ed. Atlas. Oficial R2 do Exército Brasileiro. Possui mais de 20 anos de experiência no setor.

Flavio Porto. Diretor e Sócio-fundador da Empresa Protecães, criada em 1991. Profissional reconhecido há mais de 25 anos, desenvolvendo projetos para o setor de monitoramento exótico e ostensivo, com soluções corporativas que atendem a todo o território nacional. É palestrante, membro do *chapter* Rio de Janeiro da American Society for Industrial Security International (Asis International) e está presente em diversos eventos com ênfase na segurança mundial, realizando estudos em mais de 20 países.

Francisco Tranchesi. *Certified Protection Professional* (CPP), *Physical Security Professional* (PSP). Formado em Engenharia Mecânica com MBA em Administração Industrial, ambos pelo Instituto Mauá de Tecnologia. Trabalhou alguns anos na área de Engenharia e, em seguida, migrou para a Segurança, trabalhando em algumas grandes empresas do setor no estado de São Paulo. Ao participar do curso Planejamento e Gestão de Segurança, na Enforvigil, conheceu as certificações da American Society for Industrial Security International (Asis International). Também possui o título de *Dirección de Seguridad en Empresas* (DSE), da Universidad Pontificia Commillas, Madri. Atualmente é *Head of Security* da Nokia Sistemas, atuando fortemente em novas tecnologias e Info Sec.

Gustavo Dietz. Certificado de Especialista em Segurança (CES) pela Associação Brasileira de Profissionais de Segurança Orgânica (ABSO). Atualmente é Gerente de Segurança Corporativa e Proteção das Marcas da Diageo e Secretário do Overseas Security Advisory Council (Osac), em São Paulo. Possui mais de 15 anos de experiência como consultor e gerente de Segurança Empresarial em empresas multinacionais líderes de seus segmentos, com passagens por MRM, Pfizer, Google e Microsoft. Administrador de Empresas pelo Mackenzie, com MBA em Gestão Estratégica de Segurança Empresarial pela Anhembi-Morumbi. Membro ativo da indústria de Segurança por meio do Osac, da American Society for Industrial Security International (Asis International), da Associação Brasileira de Profissionais de Segurança (Abseg) e da Associação Brasileira de Profissionais em Segurança Orgânica (ABSO).

Hector Coronado. *Certified Protection Professional* (CPP), *Dirección de Seguridad en Empresas* (DSE). Possui mais de 23 anos de experiência na área de Segurança. Atualmente é responsável pelo Programa de Segurança e Prevenção de Perdas no México e na América Latina da Amazon. Tem experiência nas áreas de segurança no trabalho, prevenção de perdas, investigações, segurança da cadeia de suprimentos, segurança logística, proteção executiva, direito criminal, segurança em auditoria, administração de crise, análise de risco, desenvolvimento de procedimentos de segurança e policiais, programas de segurança regional, serviços gerais em recepção e transporte, programas de qualidade (*Green Belt, Liaise*) com agências reguladoras, bem como envolvimento em diversas associações de segurança, treinamentos e administração de contratos. Advogado e Mestre em Direito Criminal. Possui uma série de cursos de alta *performance* em Segurança. É palestrante em conferências nacionais e internacionais sobre proteção executiva, administração de crises, lavagem de dinheiro.

Igor Pipolo. *Dirección de Seguridad en Empresas* (DSE), Analista de Segurança Empresarial (ASE), *Alta Dirección en Securidad* (ADS). CEO da Nucleo, Inc. e Diretor da Sekura (Estados Unidos). Diretor do Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Deseg-Fiesp). Professor convidado da Universidad Pontificia Comillas, Madrid/Espanha. Sócio-fundador e Ex-Presidente da Associação Brasileira dos Profissionais de Segurança (Abseg). Ex-Presidente da American Society for Industrial Security International (Asis International), *chapter* Brasil. Autor da publicação *Segurança de Eventos – Novas Perspectivas e Desafios para Produção*. Atualmente vive nos Estados Unidos, onde desenvolve consultoria em gestão de riscos para empresas americanas estabelecidas no Brasil.

Jeferson Furlan Nazário. Formado em Educação Física e Direito, com 30 anos de experiência em empresas prestadoras de serviços de vigilância e limpeza, atuando nas áreas administrativa, financeira e comercial. Durante 10 anos foi Diretor Executivo da empresa G5, de segurança eletrônica. Desde 1998, é sócio administrativo na empresa Embrasil de vigilância orgânica, Curitiba/PR. Em 2006, foi eleito presidente do Sindicato das Empresas de Segurança Privada do Estado do Paraná (Sindesp-PR), cargo para o qual foi reeleito em 2014. Neste ano, também foi eleito Presidente da Federação Nacional das Empresas de Segurança e Transporte de Valores (Fenavist).

Jeova Ferreira Cardoso Junior. Profissional com mais de 18 anos de mercado, atuando em diversos segmentos das áreas administrativas, logística, operações, qualidade e segurança, saúde e meio ambiente (SSMA), com experiência internacional. Ao longo dos últimos 12 anos, está focado nas áreas de segurança patrimonial, segurança do trabalho, saúde, meio ambiente e qualidade.

João Eliezer Palhuca. Administrador de Empresas e Empresário. Presidente do Sindicato das Empresas de Segurança Privada, Segurança Eletrônica e Cursos de Formação do Estado de São Paulo (Sesvesp). Vice-Presidente da Associação Brasileira de Empresas de Vigilância (Abrevis). Vice-Presidente da Federação Nacional das Empresas de Segurança e Transporte de Valores (Fenavist).

José Augusto Varanda. Engenheiro Mecânico com pós-graduação em Comércio Exterior. Trabalhou no Banco Central do Brasil e também nos Ministérios da Fazenda, Planejamento, Defesa e Casa Civil da Presidência da República. Foi Secretário da Comissão de Ética do Banco Central e atualmente atua como consultor na promoção e consolidação da gestão da ética nas organizações.

José Jacobson Neto. Presidente da Associação Brasileira das Empresas de Vigilância e Segurança (Abrevis). Vice-Presidente do Sindicato das Empresas de Segurança Privada, Segurança Eletrônica, Serviços e Curso de Formação de Vigilantes de São Paulo (Sesvesp). Segundo Vice-Presidente da Federação das Câmaras e Associações de Empresas de Segurança Privada de Países do Mercosul (Fesesul). Presidente do Grupo GP – Guarda Patrimonial de São Paulo S/C Ltda. Diretor da Central Brasileira do Setor de Serviços (Cebrasse). Membro da Comissão Consultiva para Assuntos da Segurança Privada do Departamento de Polícia Federal (DPF). Segundo Tenente da Reserva pelo Centro de Preparação de Oficiais da Reserva (CPOR-SP). Formado em Administração pelas Faculdades Integradas de Guarulhos (FIG). Formado em Direito pela Universidade Mackenzie.

Karina Nigri Cattan. Advogada com mais de 15 anos de experiência na área de *compliance*. Atualmente é responsável pelo Departamento de *Compliance* de uma multinacional farmacêutica no Brasil. Atuou como *Compliance Officer* em diferentes companhias multinacionais, desenvolvendo e aprimorando programas de *compliance*. Além disso, ministra aulas e palestras em cursos no Brasil e no exterior sobre o tema. Possui certificação internacional pela Society of Corporate Compliance and Ethics.

Lilian Ferracini. Jornalista. Possui pós-graduação (*Master Business of Security*) em Segurança Privada pela Fundação Escola de Comércio Álvares Penteado (Fecap) e MBA em *Marketing* pela Fundação Getúlio Vargas (FGV). É Diretora de Comunicação da Associação Brasileira dos Profissionais de Segurança (Abseg).

Maciel Alex Lastória. Diretor/Gerente de multinacionais na área de gerenciamento de riscos, segurança e prevenção de perdas desde 1997. Atual *Regional Security Manager* para o Cone Sul da HPE. Ex-militar do Exército Brasileiro formado pela Escola de Sargento das Armas (EsSA) – Três Corações, MG. Bacharel em Direito pela Universidade Paulista – Campinas. Pós-graduado em Gerenciamento Estratégico da Segurança Empresarial pela Anhembi-Morumbi/*Laureate International Universities* – São Paulo. Auditor certificado Transported Asset Protection Association (Tapa)/ Business Alliance for Secure Commerce (Basc)/Customs-Trade Partnership Against Terrorism (CTPAT), México e Estados Unidos.

Marcos do Nascimento da Silva. Há 25 anos atua na área de Segurança Empresarial em grandes corporações industriais nacionais e multinacionais. Formado em História pela Universidade do Vale do Paraíba. Possui MBA em Gestão de Serviços compartilhados pelo Serviço Nacional de Aprendizagem Industrial (Senai-PR), em Florianópolis, MBA em Gerenciamento de Projetos e MBA em Gestão Empresarial pela Fundação Getúlio Vargas (FGV). Certificado em ISO 14.001, Auditor/*Lead Auditor Training*, e em ISO 9.001:2000. É 3º Sargento Temporário da Reserva do Exército Brasileiro. Foi Gerente Nacional de Segurança da Ericsson e Embraer S. A. Atualmente é *Account Manager* da GIF Consulting International na prevenção de fraudes e gestão de riscos. Foi Presidente da Associação Brasileira dos Profissionais de Segurança (Abseg).

Marcos Serafim. Analista de Sistemas. MBA em Gestão de Segurança Empresarial pela Universidade Anhembi-Morumbi. Especializado em Gestão de Projetos pela Faculdade de Administração e Negócios – Fundação Instituto de Administração (FIA). Presidente do *Chapter* São Paulo/Brasil da American Society for Industrial Security International (Asis International). Diretor do Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Deseg-Fiesp). Diretor de Automação e Segurança Eletrônica do Grupo GPS.

Marcy José de Campos Verde. *Certified Protection Professional* (CPP), *Alta Dirección en Securidad* (ADS). Consultor Sênior em Segurança Empresarial, com mais de 1.700 projetos realizados. Auditor do Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro). Professor Universitário na Universidade Anhembi-Morumbi (UAM), na Business Scholl São Paulo (BSP) e na Fundação Escola de Comércio Álvares Penteado (Fecap). Professor convidado na Pós-Graduação da Universidad Pontificia Comillas, Espanha. Autor de dois DVDs, coautor de dois livros e ex-oficial da Polícia Militar do Estado de São Paulo (PMESP).

Michel Pipolo de Mesquita. Graduado em Direito pela Universidade Federal do Rio Grande do Norte (UFRN). Advogado. Oficial da Reserva do Exército Brasileiro. Especializado em Gestão de Segurança Empresarial pela Fundação Escola de Comércio Álvares Penteado (Fecap). Pós-graduado em Política e Estratégia pela Associação dos Diplomados pela Escola Superior de Guerra (Adesg-BA). Membro da Comissão de Segurança Privada da Ordem dos Advogados do Brasil (OAB-SP). Vice-Presidente da Associação Brasileira dos Profissionais de Segurança (Abseg) e Diretor de Segurança do Grupo GPS.

Paulo Francini. Formou-se em Engenharia pela Faculdade de Engenharia Industrial da Pontifícia Universidade Católica de São Paulo (PUC-SP) em 1963, tendo realizado posteriormente diversos cursos na área de Administração de Empresas. Por diversos anos, fez parte e chefiou a Delegação Brasileira nas negociações da Associação Latino-americana de Livre-comércio (Alalc) nas reuniões setoriais de refrigeração e tratamento de ar. Foi Presidente da Associação Brasileira de Refrigeração, Ar-condicionado, Ventilação e Aquecimento (Abrava) e do Sindicato da Indústria de Refrigeração e Tratamento de Ar no Estado de São Paulo (Sindratar), de 1974 a 1986. Foi Diretor do Departamento de Estatística (Decad) e do Departamento de Economia (Decon) da Federação das Indústrias do Estado de São Paulo (Fiesp), no período de 1980 a 1986. De novembro de 1986 a abril de 1987, foi Assessor Especial do Ministro da Fazenda, Dilson Funaro. É membro do conselho e um dos fundadores do Instituto de Estudos para o Desenvolvimento Industrial (Iedi). Foi Diretor Geral do Iedi no período de 1999 a 2002. Atualmente, é Vice-Presidente do Conselho Superior de Economia da Fiesp e Diretor Titular do Departamento de Pesquisas e Estudos Econômicos (Depecon-Fiesp).

Renato Guilherme Machado Nunes. Sócio do Nunes & Sawaya Advogados. Doutor em Direito Tributário pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Mestre em Direito Tributário pela PUC-SP. Especializado em Direito Tributário pela PUC-SP. Professor do *Master of Laws* (LLM) em Direito Tributário do Insper. Professor convidado dos cursos de pós-graduação da Fundação Getúlio Vargas (FGV-SP – GVLaw) e MBA em Gestão de Tributos e Planejamento Tributário. Autor dos livros *Imposto sobre a Renda Devido por Não Residentes no Brasil*, publicado pela Editora Quartier Latin, e *Tributação e Contabilidade*, publicado pela Editora Almedina. Possui inúmeros artigos em revistas técnicas e periódicos no Brasil e no exterior.

Ricardo Boechat. Apresentador do Jornal da Band desde 2006. Começou a carreira em 1970, no extinto *Diário de Notícias*. Foi Colunista Social, Secretário de Comunicação Social do Rio de Janeiro, Coordenador de Redação do *Jornal do Brasil* e Diretor da Sucursal do jornal *O Estado de S. Paulo* no Rio de Janeiro. Antes de ir para a bancada da televisão, Boechat atuou como Diretor de Redação da Band Rio e da BandNews FM.

Ricardo Franco Coelho. Administrador de Empresas. Especialista em Política e Estratégia pela Universidade de São Paulo (USP) e em *Alta Dirección en Securidad* (ADS) pela Universidad Pontificia Comillas, de Madrid, com o título dos Graduados Europeus. Integrou o Departamento de Segurança do Banco Central do Brasil, onde exerceu atividades relacionadas à Gestão de Riscos Operacionais, Continuidade de Negócios e Contrainteligência. Desenvolveu atividades como Professor em cursos de formação, extensão universitária e pós-graduação na área de Segurança Empresarial. Membro da American Society for Industrial Security International (Asis International), da Associação Brasileira dos Analistas de Inteligência Competitiva (Abraic) e da Associação Brasileira de Profissionais de Segurança (Abseg). Diretor do Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Deseg-Fiesp), instituição que representa no Instituto São Paulo contra a Violência e no Grupo de Trabalho Anticorrupção da Rede Brasil do Pacto Global da Organização das Nações Unidas (ONU). Consultor Associado da Núcleo Consultoria em Segurança.

Ricardo Lerner. Administrador de Empresas e Empresário do ramo de joias há 40 anos. É atual Vice-Presidente e Diretor Titular do Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Deseg-Fiesp). Foi Presidente do Instituto Brasileiro de Gemas e Metais Preciosos (IBGM), da Associação dos Joalheiros do Estado de São Paulo (Ajesp), em que atualmente atua como conselheiro nato. Foi presidente do Sindicato da Indústria de Joalheria, Bijuteria e Lapidação de Gemas do Estado de São Paulo (Sindijoias) e hoje exerce o cargo de 1º Delegado Representante junto à Fiesp. É Cofundador do Instituo São Paulo contra a Violência e Cofundador e Vice-Presidente, por dois mandatos, do Conselho Geral da Comunidade da Polícia Militar do Estado de São Paulo (Congecom), cargo civil máximo daquele conselho, cujo presidente é o Comandante Geral da Polícia Militar. Ao longo dos últimos 35 anos esteve envolvido nos assuntos de Segurança Pública e participou de inúmeros grupos e comitês, principalmente aqueles que dizem respeito ao aperfeiçoamento do serviço das polícias. Na Fiesp, idealizou parcerias junto ao Serviço Nacional de Aprendizagem Industrial (Senai-SP) para criação de cursos direcionados a egressos do Sistema Prisional e a policiais civis e militares do Estado São Paulo.

Ricardo Tadeu Corrêa. Analista de Segurança Empresarial (ASE). Atua no setor da Segurança Privada há 20 anos. Administrador e Gestor de Segurança. Sócio Diretor da Empresa Modus – Centro de Formação de Vigilantes. Presidente da Associação Brasileira dos Cursos de Formação e Aperfeiçoamento de Vigilantes (ABCFAV). Vice-Presidente da Federação Nacional das Empresas de Segurança e Transporte de Valores (Fenavist). Diretor do Sindicato das Empresas de Vigilância e Cursos de Formação do Estado de São Paulo (Sesvesp). Diretor da Abseg.

Roberto Bedrikow. Bacharel em Direito pelas Universidades de Genebra, Suíça, e de São Paulo (USP) e Mestre em Direito pelas Universidades de Genebra, Suíça, e de Leicester, Inglaterra. Advogado (Ordem dos Advogados do Brasil [OAB-SP]) econsultor em *compliance* (prevenção de lavagem de dinheiro e de corrupção, normas fundamentais do trabalho).

Roberto Zapotoczny Costa. Empresário. Diretor do Departamento de Segurança da Federação das Indústrias do Estado de São Paulo (Deseg-Fiesp). Mestre em Educação, Administração e Comunicação. Pós-graduado em Política e Estratégia pela Universidade de São Paulo (USP). MBA em Gestão Empresarial. Especialista em Administração de Segurança (Estados Unidos, Israel e Espanha). Autor dos livros *Gerenciamento de Crises em Segurança Empresarial* e *Sequestros* (2008) e *Segurança é Estilo de Vida* (2016).

Salvador Dahan. Bacharel em Direito. MBA em Gestão de Riscos e Segurança Empresarial. Pós-graduado em Liderança Organizacional. Certificado pela American Society for Industry Security (Asis) International como *Certified Protection Professional* (CPP) e pela Modulo Security como *Chief Security Officer* (CSO). Possui especializações em Proteção Executiva, Gerenciamento de Crises, Terrorismo Internacional e Inteligência Competitiva. É membro da Society of Corporate Compliance & Ethics (SCCE) e Vice-Presidente Regional da Asis International. Com mais de 20 anos de carreira, foi Diretor Executivo e Consultor da Prot – Consultoria em Segurança, Gerente de Segurança Corporativa da Procter & Gamble, Gerente Geral de Compliance e Segurança Empresarial da Gerdau e atualmente é o Diretor de Governança, Riscos, Compliance e Auditoria Interna da Nissan Motors para a América Latina.

Tácito Augusto Silva Leite. *Dirección de Seguridad en Empresas (DSE)*, Analista de Segurança Empresarial (ASE), certificado em ISO 31.000 (Gestão de Riscos), concedido pelo Global Institute for Risk Management Standards (G31.000). Ex-Presidente da Associação Brasileira dos Profissionais de Segurança (Abseg). Diretor de Segurança da Indra. Escritor. Pós-graduado em Segurança Empresarial pela Universidad Pontificia Comillas, Espanha, com MBA em Gestão de Segurança pela Universidade Anhembi-Morumbi, Gestão de Recursos de Defesa pela Escola Superior de Guerra e Oficial do Exército.

Tatiana Diniz. *Certified Protection Professional* (CPP), Analista de Segurança Empresarial (ASE). Presidente da Associação Brasileira dos Profissionais de Segurança (Abseg). Sócia Diretora da Cadiz Segurança e Vigilância Ltda., empresa nacional prestadora de serviços de vigilância. MBA em Gestão Estratégica de Segurança Empresarial pela Universidade Anhembi-Morumbi. *Master Business Security* (MBS) pela Fundação Escola de Comércio Álvares Penteado (Fecap). Graduada em Direito. Carreira profissional na área de segurança, desenvolvendo, implementando e administrando projetos e equipes. Diretora da American Society for Industrial Security International (Asis International). Recebeu menção honrosa da Câmara Municipal de São Paulo por seu conhecimento em segurança.

Teanes Carlos Santos Silva. Analista de Segurança Empresarial (ASE). Possui mais de 25 anos de experiência em Segurança Privada. Inscrito no Conselho Regional de Administração (CRA-SP 60.000-11), atuando como consultor de segurança e riscos na Consultoria Intelligencia. Professor na Universidade Anhanguera. Instrutor na Modus – Formação de Vigilantes e Diretor Suplente da Associação Brasileira dos Profissionais de Segurança (Abseg).

Vagner D'Angelo. Diretor de Segurança Corporativa – Merck Sharp & Dohme. Possui 31 anos de experiência nas áreas de Segurança Pública e Segurança Empresarial. Advogado. MBA em Gestão Estratégica de Segurança de Empresarial. É diretor da Associação Brasileira dos Profissionais de Segurança (Abseg) e membro do Overseas Security Advisory Council (Osac), São Paulo. Professor universitário e palestrante em eventos de Segurança Empresarial, investigação, *compliance* e segurança da informação.

Vander A. Giordano. Advogado. Administrador de Empresas com MBA em Gestão de Negócios pelo Ibmec. Trabalhou cerca de 9 anos na Varig S.A., na Diretoria de Logística. Durante 17 anos atuou na Kroll Inc., onde desenvolveu projetos nas áreas de gestão de crises e riscos, implementação de políticas de *compliance* e anticorrupção, bem como análise de novos mercados na América Latina em diversos setores. Atualmente, é Diretor Corporativo e Institucional do grupo Multiplan. Membro da Ordem dos Advogados do Brasil (OAB-SP), do Conselho Regional de Administração (CRA-RJ), International Bar Association (IBA), do Overseas Security Advisory Council (Osac) – Rio de Janeiro, da Câmara Americana, do Instituto de Relações Governamentais (Irelgov), da Associação Brasileira de *Shoppings Centers* (Abrasce) e do Grupo de Líderes Empresariais (Lide).


RICARDO LERNER


CIESP

FIESP | DEPARTAMENTO DE SEGURANÇA

Av. Paulista, 1313, São Paulo – SP
CEP: 01311-923
Telefone: (11)3549-4499
www.fiesp.com.br

ISBN 978-85-7201-030-6
9 788572 010306