ISSN 1678-2496N

b&a BRASILIANO & ASSOCIADOS

GESTÃO de RISCOS

agosto 2009 | edição 46

PERÍCIA ELETRÔNICA

Entrevista com o presidente do IBP Giuliano Giova

TREINAMENTO

Liderança: um tema velho, uma necessidade sempre atual

EM FOCO

Segurança Bancária: de quem é a responsabilidade?

ANÁLISE

Auditoria de Controles Internos

A revista Gestão de Riscos é uma publicação eletrônica mensal da Sicurezza Editora.
Rua Barão de Jaceguai, 1768. Campo Belo - São Paulo - SP, 04606-004, BRASIL

Diretores | Antonio Celso Ribeiro Brasiliano e Enza Cirelli. **Edição e Revisão** | Mariana Fernandez. **Arte e Diagramação** | Marina Brasiliano

Colunistas | Álvaro Takei e Mariana Fernandez. **Colaboradores desta edição** | Fernando de Bonneval de Carvalho, Gustavo Vedove e Rosangela Aparecida Stringher, Dr. Rony Vainzof e Dra. Camilla do Vale Jimene

Brasiliano & Associados Online | www.brasiliano.com.br **Blog da Brasiliano & Associados** | www.brasiliano.com.br/blog

Que tipo de atitude a Gestão de Riscos deve ter?

Estamos no olho do furação neste 2009: crise financeira, gripe suína pandêmica!!. Isso faz com que o exercício de olhar para a trajetória percorrida seja estimulado. Nessa atitude, recompomos o itinerário e elaboramos planos para fazer do futuro um tempo de real mitigação de riscos.

Ao observar o retrovisor do tempo e fazer uma pequena retrospectiva nos últimos 05 anos, sinto que perdemos (nós profissionais da área de segurança e de riscos corporativos) inúmeras oportunidades, pois ainda falta visão prospectiva. A consequência direta dessa falta de visão prospectiva é a falta da formalização de planos, tanto preventivos quanto de contingência e de continuidade de negócios. Fato é, que a grande maioria das empresas brasileiras foram surpreendidas tanto pela crise financeira como pela pandemia H1N1.

Sou obrigado a repetir o que já escrevi em abril deste ano, citando o cenarista francês Michael Godet, que descreve os homens com quatro atitudes diante do futuro:

- avestruz (atitude passiva): sofre com a mudança;
- bombeiro (atitude reativa): aguarda que o fogo se declare para combater;
- segurador (atitude pré-ativa): se prepara para as mudanças possíveis porque sabe que a reparação é mais cara que a prevenção;
- conspirador (atitude pró-ativa): atua no sentido de provocar mudanças desejadas.

Não houve demonstração de uma atitude de segurador e pouca, muito pouca, atitude de bombeiro. Ficou latente a atitude de avestruz, que coloca a cabeça no buraco, torcendo e rezando para que nada de errado aconteça. Uma atitude amadora para quem administra ou gerencia riscos nas empresas!!

É preciso entender que mais do que um plano formal, é preciso ter metas claras. O planejamento serve como medida de eficiência para nortear os objetivos de prevenção. A atitude conspiradora, a de provocar mudanças, evita ou mitiga riscos, envolve muita criatividade, relacionamento interpessoal, desenvolvimento de equipes, diversidade, logística e capacidade de gerir situações de crise.

Sugiro aos profissionais das áreas de segurança e de riscos que utilizem técnicas de endomarketing e marketing pessoal para a sensibilização de seus executivos e respectivos diretores. Mas, por favor, falem a linguagem deles, utilizem ferramentas gerenciais para as apresentações, utilizem argumentos técnicos e não o famoso "ACHOTÉCNICO", sejam incisivos ao ressaltar os prováveis impactos e consequências para o negócio (para isso os senhores devem entender muito bem o negócio, a operação!!!).

Torço que consigam, caso contrário vamos continuar perdendo oportunidades!!

Boa leitura e sorte!!

Antonio Celso Ribeiro Brasiliano
Publisher
abrasiliano@brasiliano.com.br


sua EMPRESA possui TÉCNICAS para GERENCIAR riscos ?
Ou simplesmente salta para o infinito...
Para sua empresa ser COMPETITIVA, possuir FLEXIBILIDADE e AGILIDADE, há necessidade de compreender a dinâmica dos seus riscos corporativos
A Brasiliano&Associados ajuda você através de metodologia interativa, identificar, analisar e tratar os riscos e os seus fatores facilitadores. Propõe soluções integradas, com uma visão holística do contexto, otimizando recursos na mitigação e gerenciamento de riscos.
b&a
BRASILIANO&ASSOCIADOS
informações | www.brasiliano.com.br
| info@brasiliano.com.br

EDITORIAL

As evidências não negam, nem mesmo as virtuais

Contra os fatos, não há argumentos. E como esses são provados? Nos tribunais, pela perícia, através do estudo das evidências. Ao contrário do trabalho do advogado , que é argumentativo e frenético em busca de provas, o do perito é paciente, científico, trabalhando sobre as provas angariadas, confirmando incertezas ou refutando hipóteses.

A perícia, antes profissão de poucos, vem ganhando terreno e profissionais. Com o aumento da demanda, aumentaram também os profissionais da área mas nem tanto e às vezes nada, a qualidade da formação. Há a necessidade crescente de especialistas tanto na esfera jurídica quanto na esfera privada, será que a formação dos peritos ?

Nesta edição da revista Gestão de Riscos, o perito eletrônico Giuliano Giova, diretor do Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática fala da formação, do mercado de trabalho e de muitos outras facetas da perícia digital, que disseca os aparatos tecnológicos em busca de registros de informações que cabem "num piscar de olhos".

A entrevista exclusiva começa nesta edição e continua na próxima, examinando todos os pontos questionativos desse tipo de perícia tão peculiar.

No campo virtual, a experiência Google Street View é analisada do ponto de vista jurídico pelos advogados Rony Vainzof e Camila do Valle Jimene.

Ainda no terreno estratégico, esta edição traz um artigo conceitual de Rosangela Stringher de tema Auditoria de Controles Internos, abordando a diferença entre controles internos, auditoria interna e auditoria de controles internos.

No plano operacional, a RGR traz temas quentíssimos sob o ponto de vista técnico dos consultores da Brasiliano & Associados. Fernando de Bonneval de Carvalho fala do polêmico tema de assalto a condomínios no estado, no mesmo âmbito Gustavo Vedove explica o planejamento tático e técnico das soluções integradas de segurança e a responsabilidade da segurança bancária é questionada num artigo de minha autoria.

Na coluna Acontece na Brasiliano, você verá as realizações do Ensino Digital da Brasiliano & Associados, prestes a completar 1 ano. Já na Treinamento, de Álvaro Takei, a liderança é o tema em pauta e na Ler & Saber um lançamento e um sucesso esperam por você.

Boa leitura,

Mariana Fernandez
Editora

b&a
BRASILIANO & ASSOCIADOS

Destrinchando a PERÍCIA eletrônica

Mariana Fernandez

Qual a formação de um perito eletrônico? Como os peritos são escolhidos pelos juízes? Como, tendo experiência prática no assunto, se deve proceder para tornar-se um perito digital? Tudo o que envolve a perícia eletrônica você vai conferir nesta entrevista exclusiva com o professor e perito Giuliano Giova, presidente do Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática, uma entidade especializada que apoia a condução de estudos e investigações científicas e tecnológicas, além de exames e laudos nos âmbitos administrativos, arbitral ou judicial.

Giova atuou como executivo e profissional de processamento de dados por 25 anos, tendo sido por mais de dez anos gerente de desenvolvimento de sistemas do Banco Itaú. Economista e especialista em informática, o perito é conselheiro do Conselho de Comércio Eletrônico da Federação de Comércio do Estado de São Paulo e membro dos comitês sobre telecomunicações, tecnologia da informação, e-bussines e direito da tecnologia, da Câmara Americana de Comércio. E também da Conferência sobre Fraudes e Crimes Corporativos (Unicorp) e presidente da Conferência sobre Riscos Legais em Empresas no Uso de E-mail e Internet (ADPO).

Como professor, é docente no curso de extensão universitária em Prova e Perícia Eletrônica da Brasiliano & Associados e em muitos outros. Giova também atua como instrutor, palestrante e perito, é claro.

Nesta edição, você vai conferir a primeira parte da entrevista que abordará o perfil profissional do perito Giuliano Giova e esclarecimentos sobre a formação e atuação do perito digital.

Há quantos anos o senhor é perito eletrônico?

Nós começamos aqui em 2000 e em 2001 nos fundamos o Instituto Brasileiro de Peritos. Naquela época estávamos entre os primeiros atuar nessa área. Existiam algumas atuações, mas nada organizado.

Quando o senhor decidiu que queria ser perito?

Esta é uma questão fascinante. Na verdade, eu decidi isso na Câmara Americana do Comércio. Lá eu havia me inscrito em dois comitês: um comitê de tecnologia da informação que era minha carreira e um outro comitê que se chama Comitê de Legislação, que é basicamente um comitê de advogados. Por alguma razão, naquela época eu já percebia que a tecnologia da informação vai ficar muito próxima do direito. Curiosamente, conheci um laudo feito pelo Dr. Renato Opice Blum, que hoje é o líder nessa área de direito eletrônico. Daí resolvemos juntos fundar o Comitê do Direito da Tecnologia que é um pequeno comitê onde começaram a ir alguns advogados e alguns profissionais tecnologia da informação e, realmente, a discutir essa questão da pericia; e foi lá que nasceu o Instituto Brasileiro de Peritos, inspiração desse pequeno Comitê de Direito da Tecnologia da cCâmara Americana. Surgiu aí o IBP.

E quantos membros participavam do Comitê?

Naquela época era meia dúzia não tinha quase ninguém.. (risos). Era, realmente, uma coisa pioneira. O doutor Renato foi pioneiro no bug do milênio... não sei se você era nascida naquela época... (risos)

Era sim... quando achavam que ía ocorrer um bug nos computadores com a virada do ano 2000, não é?

Isso exato. O doutor Renato foi o representante oficial do Brasil na ONU. Então, logo depois, praticamente, nos criamos o Comitê de Tecnologia e, era realmente algo inovador, ninguém conhecia. Hoje não, hoje explodiu. Todo mundo quer ser perito, todo mundo precisa de perícia... infelizmente.

E quanto à sua formação, me corrija se não estiver correto, o senhor se formou economista, fez pós-graduação em Gestão de Empresas e está cursando mestrado em Engenharia Elétrica.

Isso. Estou fazendo os dois: gestão de empresas e engenharia elétrica. Porque o que acontece Mariana é o seguinte: pra ser perito precisa ter formação superior. Normalmente a perícia é realizada em profissões regulamentadas, e o que é uma profissão regulamentada? É aquela que é reconhecida por lei, por exemplo, a medicina. Só pode ser perito médico o profissional formado em medicina, só pode ser perito em engenharia o formado em engenharia. Mas isso não ocorre em tecnologia da informação, porque a tecnologia da informação não é regulamentada. Então, por exemplo, até pouco tempo os diretores do núcleo de perícias de informáticae do núcleo de estudos de criminalística aqui de São Paulo,

eram farmacêuticos. Porque não há essa necessidade, essa obrigatoriedade da pessoa ser formada em ciência da computação ou sistema de informação e assim por diante. O que é importante sim, é que o profissional de fato, o perito da tecnologia da informação tenha uma larga experiência na área. Acho que é claro para as pessoas que o perito é o homem de confiança do juiz naquele assunto, então, ele tem que ser, realmente, um homem experiente nesta área. Mas como minha carreira, por mais de 30 anos, foi na área de tecnologia da informação - trabalho desde 73 no mercado, comecei a trabalhar com os main frames dentro de bancos -, foram aí muitos e muito anos com vivência de informática.

E como não tem uma formação específica para ser perito eletrônico, o senhor acha interessante que as pessoas tenham uma formação como a do senhor, que abrange tanto a área humana quanto a área exata, para ser um profissional completo?

Acho que não, a tendência é que o perito seja, cada vez mais, um profissional especializado, até porque essa área está ficando muito mais complexa de uns anos pra cá pela própria evolução da tecnologia da informação, da telecomunicação, etc. Por isso, a recomendação para os profissionais que queiram atuar na área, é que ele se formem em ciência da computação, sistema de informação e assim por diante. Quanto a questão humana sim, aí o que ocorre é: uma vez que ele tenha formação e nível de graduação técnico, é bom que ele faça pós-graduação em perícia envolvendo questões como direito, gestão de empresas e assim por diante. São conhecimentos complementares à especialização dele na área da tecnologia.

Então a formação especializada do perito na área eletrônica vem mais relacionada à pós-graduação?

Mais ou menos. Tem que ter tanto experiência profissional na área digital, na área eletrônica, na área de sistemas, como experiência profissional mesmo, prática, porque o perito não pode ser apenas acadêmico. Até algum tempo atrás era comum que as perícias fossem encaminhadas às universidades brasileiras envolvidas em atividades de perícia. Qual o problema disso? O problema é que, muitas vezes, falta visão prática. E as questões que o juiz tem que julgar são questões práticas. Por isso, a experiência prática como perito é fundamental. Vamos imaginar um médico que vai avaliar, vai fazer uma perícia, um exame de uma questão médica. Imagina se esse médico nunca trabalhou, ele só ficou na universidade estudando. Tem uma distorção. Então, essa área principal do perito, tem de ser uma área onde ele tenha atuado efetivamente. O restante sim, é a metodologia pericial, noções de direito, etc.

Seria também pelo motivo de que as tecnologias na área eletrônica avançam muito rápido sendo necessário ao perito ter uma vivência, uma prática na área eletrônica, além de estar sempre se aperfeiçoando, estudando?

Obviamente é uma área muito dinâmica. Aquilo que se aprendeu há dois, três anos atrás, rapidamente é superado, é substituído por novos conhecimentos, novas técnicas, novas ferramentas. Então, o profissional que decide atuar com perito tem que estar continuamente em atualização. Tem que estar ligado, tem que ter network, é importante

estar conversando com os colegas... a tecnologia ficou tão complexa que você corre o risco de cair em falsos positivos e falsos negativos. Vou dar um exemplo: imagine que eu vá examinar o disco rígido de um suspeito, o disco rígido hoje de qualquer computador tem na faixa de cento e vinte, cento e sessenta gigabytes. Se você pensar o disco rígido tendo cento e sessenta gigabytes, tem cento e sessenta bilhões de caracteres, cento e sessenta bilhões de letrinhas! Percebe? Então tem que ter o que há de mais sofisticado em termos de programas, para poder quebrar a privacidade, software pra processar esses caracteres, etc. Se o perito não estiver muito atualizado, ele pode cometer erros, como por exemplo, o erro de achar que uma pessoa é culpada quando é inocente, porque ele não encontrou a evidências no disco, porque elas estavam perdidas no meio daqueles dados, ou vice-versa. Tem tantos dados, que, ao interpretar indevidamente alguns deles ele pode achar que a pessoa é culpada quando não é. Por isso essa necessidade de atualização é extremamente importante.

Além de poder ser um homem de confiança, digamos assim, do juiz, qual seria uma outra área de atuação do perito eletrônico?

O primeiro ponto no qual nós precisamos pensar sobre perito eletrônico, perito digital ou perito virtual, é que existem duas grandes categorias de peritos na área eletrônica. A primeira categoria é a dos chamados peritos oficiais. O que são os peritos oficiais? São aquelas pessoas que prestam concurso para ingressar tanto na Polícia Federal como nas polícias estaduais. Ao passo que eles são aprovados nesses concursos, eles se tornam policiais de carreira. São funcionários públicos que começam sendo treinados na academia de polícia. Na época de serviço, geralmente eles ficam de seis meses a um ano recebendo treinamento e depois eles vão atuar como funcionários públicos, em tempo integral, nos institutos de criminalística. Tanto no Instituto Nacional de Criminalística que é da Polícia Federal, como nos institutos dos estados. No estado de São Paulo, na entrada da Cidade Universitária fica a superintendência da Polícia Científica, os institutos de criminalística, um comitê de perícia em informática, entre outros... contabilidade, engenharia, medicina e assim por diante. Quanto aos peritos judiciais, eles não são funcionários, são pessoas que mantêm seus empregos, suas atividades normais, só que são, eventualmente, chamados pelos juízes para atuar numa causa específica. No momento em que surge a necessidade de um perito, o juíz chama o perito de sua confiança, o nomeia para aquela ação, para aquele trabalho pericial daquela ação. Findo o trabalho, ele volta à sua atividade normal.

Então esses peritos, que são apenas peritos judiciais, teriam que ter uma outra profissão para terem uma remuneração menos variável?

Isso, exato. São muito poucos os peritos que só atuam como peritos judiciais porque eles são tão conhecidos no meio, que são continuamente nomeados por muitos juízes. Mas não é a totalidade, muitos mantêm sua outra profissão, seu outro emprego e, de vez em quando, fazem uma perícia judicial.

Em sua opinião, quais são os conhecimentos imprescindíveis para os profissionais que desejam atuar na área de perícia?

Ele tem que ser muito bom na área de tecnologia de informação, tem que entender muito de informática, conhecer banco de dados, linguagem de programação, sistemas operacionais e assim por diante. Tem também que conhecer metodologia pra modelagem de banco de dados, metodologia pra levantamento de sistema, ou seja, todas aquelas coisas que são normais dos profissionais de informática. Isso é fundamental, senão como é que ele vai poder avaliar, imagine você, uma software house, uma empresa de desenvolvimento de sistema que desenvolve um sistema para um hospital por exemplo. Imagine você que depois de um ano o hospital ache que aquele sistema não está funcionando adequadamente, por outro lado a software house diz que o sistema dela é ótimo, maravilhoso e que o hospital não sabe usar direito. Para que o perito possa ajudar o juíz a decidir quem está certo quem está errado, ele tem que ter muita experiência. Além disso, obviamente, o perito tem que ter noções de direito para que ele saiba as fases, as etapas que existem dentro do processo da tecnologia. Finalmente, ele precisa conhecer as ferramentas periciais específicas. Por exemplo: ao examinar o disco rígido de um computador, o perito tem que saber que não existem arquivos deletados. Aquilo que o usuário comum considera como arquivo deletado, na verdade, não existe, pois foi apenas retirado de um circuito, mas aquele dado, aquela informação permanece no disco até que seja sobrescrita. Então o perito tem que ter a habilidade de saber isso e buscar aquela informação aparentemente morta dentro do disco rígido, porque ela não está mais indexada, não está mais visível ao usuário comum, mas com uma ferramenta especializada, pode ser encontrada.

Com a nova prática de salvar os documentos na internet - utilizando o Google Docs por exemplo - e não mais no disco rígido, o trabalho da perícia fica dificultado?

Ainda na questão do perito, do seu campo de atuação, existe um terceiro tipo que é o chamado de assistente técnico. O assistente técnico é o perito da parte. Se nós voltarmos naquele exemplo do hospital que está processando a software house porque acha que o sistema não funciona, quando se inicia a fase pericial, o perito judicial é nomeado pelo juiz mas cada uma das partes a autora da ação e a ré da ação têm o direito de nomear os seus próprios peritos, só que esses peritos recebem o nome de assistente técnico. Na prática isso é importante, porque na prática, para cada ação é mais ou menos como se existissem três peritos. Isso multiplica o campo do trabalho porque os peritos das partes, os assistentes técnicos, são contratados diretamente, livremente, pelas próprias partes. Então, para cada ação, são três peritos discutindo sobre as provas, sobre as evidências e assim por diante. Mas, voltando à sua pergunta, a questão da privacidade e da tecnologia, você tocou num ponto extremamente grave porque os fabricantes de software, os fabricantes de computadores, estão atualmente inventando tanto ferramentas para proteger a privacidade do usuário e, portanto, estão protegendo a privacidade do bom usuário, mas também estão protegendo a privacidade do mal usuário, do fraudador, do bandido. Outra questão que você levantou é o fato do processamento distribuído. Hoje não há, necessariamente, a necessidade de os dados ficarem guardados nos computadores pessoais, podem estar em qualquer lugar do mundo. É aquilo que nós comentamos: o perigo, hoje em dia, do falso

positivo e do falso negativo aumentou muito, porque se tornou muito mais complexo ter certeza se uma pessoa fez ou não alguma coisa. Por exemplo, eu posso através do meu computador entrar num webmail, criar um email fictício e com esse email ameaçar uma empresa ou difamar uma empresa e assim por diante, sem que, a rigor, um desses dados fique armazenado no meu computador. A contrapartida disso é que, em verdade, tudo que passa pelo meu computador, mesmo que fique armazenado num disco externo, num hd externo, que fique armazenado numa nuvem, num serviço na internet, teve algum processamento no meu computador. Então, com um pouco mais de trabalho, eu ainda tenho a habilidade de localizar rastros do que houve.

Mas e se a pessoa apagar o cache do que ela visitou na internet? Mesmo assim tem como vasculhar por onde ela andou enviando mensagens, recebendo documentos ou alguma coisa do tipo?

Tem sim pelo seguinte. Se você pensar na velocidade da CPU do computador - hoje qualquer computador tem uma CPU tipo Pentium, Dual Core, dois giga hertz. O que significa dois giga? Significa que enquanto a gente dá uma piscadela, a CPU processa dois bilhões de instruções. É algo espantoso, algo fenomenal uma CPUzinha de um computadorzinho qualquer processando dois bilhões de instruções num piscar de olhos, num segundo. Em contrapartida o disco rígido é muito lento. Se você imaginar neste momento o disco rígido, o hd, você vai ver que ele é formado por dois disquinhos de metal com quatro cabecinhas com feltrinho na ponta pra não arranhar, movimentado por um eletroímã, um motorzinho. Isso é uma coisa muito antiga. Mas, para que a CPU possa conversar com seu disco rígido, é necessário alguém que faça o meio de campo. Esse meio de campo é feito com a memória Ram, por isso se diz que a memória Ram quanto maior é, melhor para a performance de um computador. Acontece que tudo que passa pela memória Ram é gravado em áreas especiais do disco que não tem nada a ver com as tais áreas temporárias. Então é lá que o perito vai recuperar estes rastros que não são facilmente apagáveis por essas limpezas feitas pelo usuário final.

Confira na próxima edição a continuação da entrevista com Giuliano Giova.

Mariana Fernandez
Editora

sumário

BRASIL E ANGOLA,

AGORA JUNTOS NA GESTÃO INTEGRADA DE RISCO

Em 2008, a Brasiliano & Associados, através de um contrato de transferência de know-how da sua metodologia, processos e experiência abriu a Brasiliano & Associados Angola. A Brasiliano & Associados Angola é uma empresa 100% angolana, trabalhando com os mesmos padrões, moldes e processos da sua co-irmã brasileira. O objetivo é formar e qualificar consultores técnicos angolanos para estarem elaborando soluções na Gestão de Riscos Corporativos.

COMPARTILHE DESTE DESAFIO!!!!

b&a
BRASILIANO & ASSOCIADOS

Sede Angola: | Rua Comandante Kwenha, 2º edifício, 2º andar Cnj 21. Município das Kinachiche - Luanda - Angola
| Telefone Fixo: 244 222 008835 | Telemóvel: 244 914 656226 / 224 914 653224 / 244 929 529908 / 224 928 227713 / 224 923 609049
| e-mail: riboldi@brasiliano.com.br / mauro.ao@brasiliano.com.br / dviana@brasiliano.com.br / abrasiliano@brasiliano.com.br
| site: www.brasiliano.com.br

O Google Street View e as Questões de Privacidade

Dr. Rony Vainzof e Dra. Camilla do Vale Jimene

Recentemente, o Google anunciou o início das atividades no Brasil de sua ferramenta denominada *Google Street View*, subproduto do *Google Maps*, que tem como principal finalidade a visualização pelos internautas de imagens de ruas em 360°, capturadas por câmeras instaladas em carros que circulam nas grandes metrópoles, possibilitando um verdadeiro *tour* virtual.

Antes de iniciar suas atividades no Brasil, o *Google Street View* já chega ao país, assim como ocorre nos países em que o serviço já é executado, levantando receios acerca de seu impacto na privacidade dos cidadãos e na segurança pública.

De um lado as ruas são ambientes públicos e, em tese, não haveria qualquer violação à privacidade dos transeuntes que tiverem suas imagens capturadas ao caminhar por determinada via e posteriormente serem disponibilizadas na Internet, de outro lado, está o direito à imagem, outra garantia Constitucional de qualquer cidadão brasileiro.

Fato é que num mundo amplamente interconectado através da Internet, quando uma imagem é inserida nesse meio, torna-se ela incontrolável, o que inegavelmente pode causar danos imensuráveis aos ofendidos.

Algumas imagens já causaram polêmica, por exemplo: uma mulher com saia curta, garotas de programa na rua, homem passando mal em frente ao bar, outro caminhando com uma boneca inflável, um rapaz no banheiro com a porta aberta, prisão de alguns indivíduos, mulheres de topless, entre outras.

Em alguns países o confronto entre a privacidade e o novo serviço do *Google Street View* já teve início: os gregos proibiram temporariamente a captura de imagens em algumas cidades até que o Google garantisse formas de identificação do carro e definisse previamente áreas em que circularia; os japoneses solicitaram ao Google que editasse imagens capturadas de seus cidadãos e os ingleses chegaram a entender por ofensivas algumas imagens capturadas em suas cidades; nos Estados Unidos uma Juíza Federal julgou improcedente uma ação movida por um casal de Pittsburgh que alegava que a ferramenta violava a privacidade em razão de imagens gravadas da residência (entrada da garagem e própria garagem, além de uma área da piscina). O Google retirou as imagens quando cientificados, afirmando que prima pela privacidade individual e disponibiliza ferramentas para manter esta privacidade.

Infelizmente, é comum a utilização inadequada das novas tecnologia. Podemos citar o caso do seqüestro de uma pessoa em razão de fotografias postadas no Orkut que retratavam o patrimônio da vítima, o auxilio ao suicídio através de um blog de um garoto de dezesseis anos de idade e o furto de residência que estava vazia, pois o morador teria postado no Twitter que viajaria nos próximos dias.

O ponto essencial da discussão é: as vítimas desses crimes divulgaram por vontade própria as suas informações ou manifestaram suas vontades que posteriormente vieram lhe causar prejuízos, mas no *Google Street View*as imagens são capturadas e disponibilizadas na Internet sem a anuência dos "personagens".

Em outros países o Google já adotou algumas medidas de proteção à privacidade, dentre elas o emprego de software que borra os rostos dos transeuntes e as placas dos carros que tiveram suas imagens capturadas. Mas esse recurso não foi suficiente para evitar problemas causados a um americano que foi flagrado pela esposa na casa da amante, em razão da imagem do carro estacionado na rua, identificado pela mulher por ter rodas personalizadas.

Segundo algumas matérias jornalísticas, a equipe do Google disse que o *Street View* nacional usará o mesmo software que estreou na versão francesa do serviço para borrar tanto os rostos de brasileiros capturados como placas de veículos fotografadas (www.idgnow.uol.com.br).

Mais que isso: caso um usuário sinta que sua privacidade está sendo invadida

mesmo com o rosto borrado, é possível entrar em contato com o Google para pedir a remoção da foto. Nesse caso, a empresa tira a imagem do ar e a substitui por uma alternativa.

De fato, além da nossa Constituição, o Código Civil Brasileiro dispõe que a utilização da imagem de uma pessoa poderá ser proibida, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingir a honra, a boa fama ou a respeitabilidade, ou caso se destine a fins comerciais, bem como que a vida privada da pessoa é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Tanto é assim que, em casos semelhantes, nos quais o Google foi cientificado dos ilícitos perpetrados pelos seus serviços e não agiu diligentemente na remoção das ofensas, a justiça brasileira já o condenou, em razão de sua inércia.

Nesse contexto nebuloso, vamos aguardar o início das atividades do *Google Street View*nas cidades brasileiras e acompanhar os problemas que surgirão, sendo certo que não podemos deixar ocorrer que novos serviços de grande utilidade publica deixem de nos prover em razão de situações excepcionais, nas quais as empresas provedoras podem ser diligentes na resolução dos problemas e se assim não fizerem, nosso Poder Judiciário consiga atuar de forma justa para cessar os ilícitos e condenar os responsáveis.

Dr. Rony Vainzof
Sócio do Opice Blum Advogados e
Professor de Direito em diversas instituições;
Dra. Camilla do Vale Jimene
Advogada associada à Opice Blum Advogados e
Professora de Direito Eletrônico em diversas instituições.

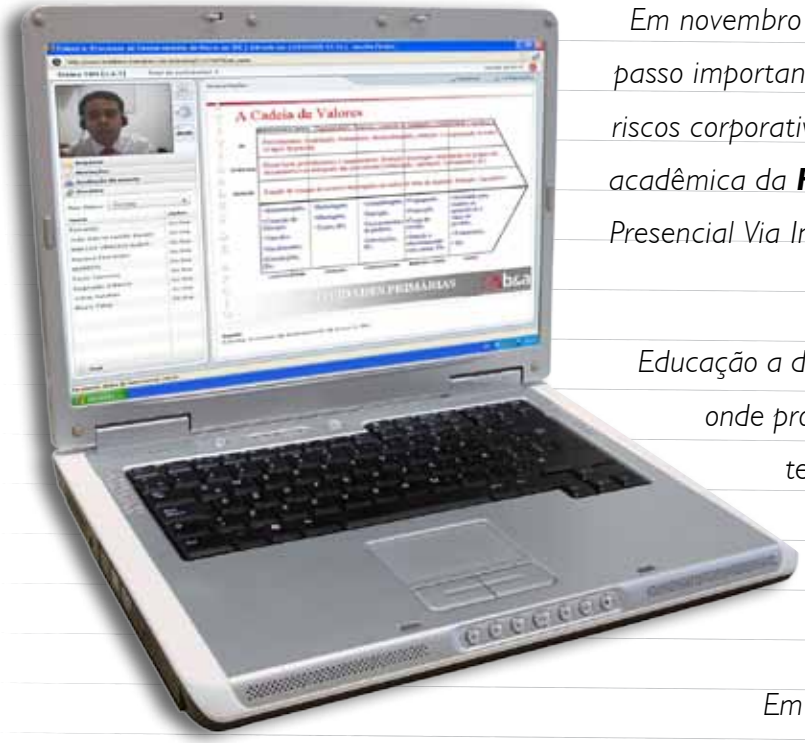
sumário

ACONTECE

na Brasiliano

Mariana Fernandez

ENSINO DIGITAL DA BRASILIANO & ASSOCIADOS: UMA EXPERIÊNCIA VENCEDORA



Em novembro de 2008, a Brasiliano & Associados deu um passo importante para a formação na área de gestão de riscos corporativos, iniciou seu Ensino Digital, com supervisão acadêmica da ***FAPI – FESP****, através dos métodos de Ensino Presencial Via Internet e Educação à Distância (EAD).*

Educação a distância é o processo de ensino-aprendizagem, onde professores e alunos estão separados espacial e/ou temporalmente, mas podem estar interligados por tecnologias, principalmente as telemáticas, como a Internet.

Em sua forma empírica, a EAD é conhecida desde o século XIX. Entretanto, somente nas últimas décadas passou a fazer parte das atenções pedagógicas. Ela surgiu da necessidade do preparo profissional e cultural de milhões de pessoas que, por vários motivos, não podiam frequentar um estabelecimento de ensino presencial, e evoluiu com as tecnologias disponíveis em cada momento histórico, as quais influenciam o ambiente educativo e a sociedade.

Este tipo de ensino caracteriza-se pelo estabelecimento de uma comunicação de múltiplas vias, suas possibilidades ampliaram-se em meio às mudanças tecnológicas como uma modalidade alternativa para superar limites de tempo e espaço. Seus referenciais são fundamentados nos quatro pilares da Educação do Século XXI publicados pela UNESCO, que são: ***aprender a conhecer, aprender a fazer, aprender a viver juntos e aprender a ser.***

A SALA DE AULA ANTES E DEPOIS DA INTERNET

	Na educação tradicional	***Com a nova tecnologia***
o professor	*um especialista*	*um facilitador*
o aluno	*um receptor passivo*	*um coloborador ativo*
a ênfase educacional	*memorização de fatos*	*pensamento críticos*
a avaliação	*do que foi retido*	*da interpretação*
o método avançado	*repetição*	*interação*
o acesso ao conhecimento	*limitado ao conteúdo*	*sem limites*

Fonte: Revista Nova Escola, Ano XIII, Nº 110, Março de 1998.

No Ensino Digital da Brasiliano & Associados, a Educação deixa de ser concebida como mera transferência de informações e passa a ser norteada pela contextualização de conhecimentos úteis ao aluno. Nas metodologias de ensino à distância utilizadas, o aluno é desafiado a pesquisar e entender o conteúdo, de forma a participar da disciplina.

Os cursos online possibilitam o ingresso de alunos de diversos cantos do Brasil, enriquecendo a troca de experiências com repertórios diversos. O mais importante, contudo, é a promoção da formação especializada em locais que não dispõem de cursos na área de gestão de risco.

Desde o início do Ensino Digital da B&A, já foram formados 62 alunos, nos cursos: de Extensão em Análise de Risco Empresarial, de Extensão em Técnicas Operacionais para a Equipe de Segurança, Avançado em Segurança Empresarial - 26ª Turma MBS, de Controle de Acesso e Veículos (Digital).

Álvaro Takei, Diretor do Ensino Digital da Brasiliano & Associados, explica que "para o desenvolvimento do método, verificou-se a forma como o adulto aprende" concluindo-se que "são auto-direcionados" e que "esperam ter responsabilidade e participação durante as aulas".

Para o diretor e professor, "os cursos digitais da Brasiliano & Associados têm sido uma experiência muito proveitosa, em especial aos alunos que, sendo de diversos locais do Brasil, teriam dificuldade para deslocarem-se aos locais em que os cursos seriam oferecidos. Com a modalidade digital puderam freqüentar os cursos e obtiveram o conhecimento desejado, com a mesma qualidade dos cursos presenciais, tendo como adicional a possibilidade de montar uma rede de relacionamento com pessoas cujos interesses são comuns, mas de diferentes regiões. Para os professores, que ministraram as diversas disciplinas, foi um aprendizado importante, uma vez que o ensino a distância é uma tendência que, cada vez mais, se consolidará. Assim, todos eles estão preparados para o ensino contemporâneo e do futuro."

Claudia Sartori, diz haver ficado "surpresa" com seu aproveitamento no curso. A coordenadora de segurança das Casas Bahia da região sul do país, que nunca havia feito curso digital, "achava que não traria o resultado esperado". Contudo, após a experiência no curso digital de Controle de Acesso e Veículos, Sartori acredita ser o curso digital "melhor do que presencial para quem trabalha o dia todo" pois, segundo ela, "prende a atenção e há uma interação maior entre os participantes".

Elder dos Anjos, Diretor de Operações da Prisma Segurança e aluno do curso de extensão em Análise de Risco Empresarial, considera o sistema utilizado pela Brasiliano uma "excelente ferramenta" que "minimiza as distâncias e nos leva a uma real interação".

Para Giovanni Raphael de Oliveira, Segurança Patrimonial da Souza Cruz e aluno do MBS digital, o formato do curso permite "mesmo durante viagens a trabalho acessar o site e acessar a aula sem nenhum problema". Oliveira, que já foi aluno de cursos presenciais da Brasiliano & Associados, afirma que "o curso digital nada deixou a desejar de cursos presenciais". Para ele, "a forma de comunicação visual (webcam) e auditiva (microfone) não opuseram em nada em obstáculo para a interação entre aluno e professor."

Quanto ao quadro de professores do curso avançado, o aluno avalia como "altamente profissional", pois, segundo ele, "a gama de experiência vivenciadas por eles (professores), bem como o conhecimento técnico e operacional proporcionam uma aula com didática excepcional".

Helio de Moura , aluno dos curso de Controle de Acesso e Veículos e analista na Marinha do Brasil, considerou "a atualidade do conteúdo e a forma prática como foi apresentado" um ponto positivo do curso. Moura também ressaltou serem várias as vantagens de um curso online, "indo desde custos menores até a facilidade de estudar em sua residencia ou local de trabalho" e sobre seu aproveitamento avaliou como "excelente" pois o curso foi "extremamente importante" para sua atividade profissional.

CONFIRA OS CURSOS DO ENSINO DIGITAL QUE ESTÃO COM MATRÍCULAS ABERTAS NO SITE DA BRASILIANO & ASSOCIADOS.

Segurança Bancária: DE QUEM É A RESPONSABILIDADE?

Mariana Fernandez

Os funcionários das agências exigem, os sindicatos brigam, o governo cria leis, mas, afinal, a responsabilidade da segurança bancária é apenas dos bancos? Ou o poder público também deve ser exigido quanto a essa necessidade?

Neste artigo, iremos, primeiramente, descrever o que é segurança pública, explicando seu papel no que tange à segurança bancária e à contenção do crime; depois, iremos tratar do papel das instituições públicas e financeiras com relação à segurança física nas agências bancárias, além de mostrar com dados verídicos a mudança do cenário no país.

O QUE É SEGURANÇA PÚBLICA?

A segurança pública garante a proteção dos direitos individuais e assegura o pleno exercício da cidadania, numa sociedade em que se exerce democracia plena. NesSe sentido, a segurança não se contrapõe à liberdade e é condição para o seu exercício, fazendo parte de uma das inúmeras e complexas vias por onde trafega a qualidade de vida dos cidadãos.

As forças de segurança buscam aprimorar-se a cada dia e atingir níveis que alcancem a expectativa da sociedade como um todo, imbuídos pelo respeito à defesa dos direitos fundamentais do cidadão. Sob essa óptica, compete ao Estado garantir a segurança de pessoas e bens na totalidade do território brasileiro, a defesa dos interesses nacionais, o respeito pelas leis e a manutenção da paz e ordem pública.

A segurança pública enquanto atividade desenvolvida pelo Estado é responsável por empreender ações de repressão e oferecer estímulos ativos para que os cidadãos possam conviver, trabalhar, produzir e se divertir, protegendo-os dos riscos a que estão expostos.

As instituições responsáveis por essa atividade atuam no sentido de inibir, neutralizar ou reprimir a prática de atos socialmente reprováveis, assegurando a proteção coletiva e, por extensão, dos bens e serviços.

Atualmente as funções de prevenção do crime e policiamento ostensivo estão divididas entre o Estado, a sociedade e a iniciativa privada.

SEGURANÇA BANCÁRIA

Segundo Antonio Celso Ribeiro Brasiliano, especialista em segurança bancária, "o ambiente estratégico da segurança bancária possui como condições causais as tendências sócio-demográficas e tecnológicas, bem como as das áreas de segurança pública, incluindo o poder judiciário. Como reação estratégica observa-se as tendências de comportamento da sociedade e da empresa, que, por conseguinte impactam na segurança privada de uma forma geral."

A insegurança bancária, que nos últimos anos tem crescido vertiginosamente e assustado o brasileiro, tem destaque especial entre as reivindicações dos trabalhadores do sistema financeiro.

Mas de quem é a responsabilidade da segurança física dos bancos? Do poder público ou das instituições financeiras privadas?

O governo pressiona os bancos, cada vez mais, através de leis para que esses sempre reforcem e atualizem seus sistemas de segurança. O governo, por sua vez, é pressionado pelos trabalhadores bancários, que através dos sindicatos exigem mais segurança.

A Lei federal 7.102/83 estabelece os dispositivos que devem compor o sistema de segurança da agência bancária, fixando, como obrigatórios, vigilância e alarme. Além desses dois itens, a instituição financeira deve adotar um dos seguintes recursos de segurança: cabine blindada; ou, porta de segurança com detectores de metais; ou, câmera; ou, fechadura eletrônica programável no cofre etc.

Anualmente, por força da lei federal, é obrigatória a apresentação à Polícia Federal do plano de segurança de cada agência. De posse do plano, que contém descrição pormenorizada de todos os itens de segurança existentes, um representante da Polícia Federal visita e vistoria a agência para sua aprovação.

Em trecho da Carta do III Seminário Nacional de Segurança Bancária - escrita em Curitiba em 30 de maio de 2007 pela Confederação Nacional dos Trabalhadores do Ramo Financeiro (Contraf-CUT) e Confederação Nacional dos Trabalhadores em Vigilância Sindicatos e Federações de Bancários Sindicatos e Federações de Vigilantes - , estabelece-se as obrigações do poder público:

"O governo federal deve incluir a segurança bancária em sua política nacional de segurança pública, estabelecendo diretrizes e estratégias e integrando ações coordenadas com os estados e municípios;

Os governos estaduais devem investir mais em políticas públicas, como forma de melhorar a qualidade de vida e reduzir a criminalidade, bem como ampliar os recursos para a área de segurança, contratando policiais e adquirindo viaturas para prevenir ações criminosas e combater a violência na sociedade;

As polícias militar e civil devem realizar ações integradas de inteligência para enfrentar os ataques a bancos e o crime organizado, organizando também patrulhas e monitoramento nas imediações dos bancos em dias de pico, pagamento de aposentados e funcionários públicos, vésperas e após feriadões, como forma de prevenir assaltos e garantir a segurança de trabalhadores, clientes, usuários e população em geral.

A Polícia Federal deve fiscalizar com rigor os planos de segurança das agências e postos, verificando o cumprimento da legislação e a garantia de proteção da vida de bancários, vigilantes e clientes.

As secretarias estaduais de segurança pública, a exemplo do Rio Grande do Sul, devem constituir grupos de trabalho de segurança bancária, integradas por representantes dos bancários, vigilantes, bancos, polícias militar, civil e federal, para discutir os problemas existentes e buscar soluções;"

Em outro trecho, seguem as obrigações do poder legislativo:

"O Congresso Nacional deve atualizar a lei federal nº 7.102, de 20 de junho de 1983, que rege a segurança privada no país, uma vez que se encontra totalmente defasada frente à evolução tecnológica, às ações criminosas e ao quadro atual de violência e insegurança no país;

As assembléias legislativas e câmaras municipais devem aprovar leis estaduais e municipais para melhorar as condições de segurança nos bancos em estados e municípios, como obrigatoriedade de instalação de portas giratórias e câmeras de vídeo."

A Carta dispõe também sobre os deveres dos bancos:

"Os bancos devem organizar planos de segurança para agências e postos com enfoque na proteção da vida dos bancários, vigilantes, clientes e população em geral. Hoje, a preocupação das instituições se concentra na guarda do patrimônio e não da integridade física e psicológica das pessoas;"

"Os bancos devem cumprir a legislação federal que estabelece pelo menos dois vigilantes em cada agência, sendo que eles não podem exercer tarefas alheias a sua função, como porteiro e organizador de filas.

Os bancos devem contratar vigilantes em número compatível com o volume de circulação de pessoas e com a área de abrangência das agencias;

Os bancos devem ter maior rigor na seleção e contratação de empresas de vigilância privada, além de realizar fiscalização constante dos serviços prestados;

Os bancos devem garantir treinamento específico e constante dos vigilantes, bem como acompanhamento psicológico;

Os bancos devem estudar a possibilidade do uso de armas não letais pelos vigilantes;

Os bancos devem cumprir a portaria da Polícia Federal que obriga o uso de coletes a prova de balas pelos vigilantes;

Os bancos devem efetuar maior investimento em tecnologia de vigilância e em comunicação para orientar os clientes sobre comportamentos seguros que devem ser adotados quando da realização de transações financeiras e utilização das portas giratórias, além de dicas de segurança para evitar golpes.

Os bancos devem instalar portas giratórias de segurança, com detectores de metais e vidros blindados, na entrada das agências e postos, antes da sala de auto-atendimento, protegendo todos os acessos destinados ao público;

Os bancos devem criar sistemas de gravação eletrônica de imagens e centrais de monitoramento de vídeo em tempo real, integrada às Polícias Civil e Militar e Secretarias de Segurança Pública, como forma de prevenção de assaltos e melhoria das imagens para a identificação de criminosos e suspeitos;

Os bancos devem acabar com o método ultrapassado e perigoso de guarda de chaves dos cofres pelos gerentes, tesoureiros e vigilantes, contratando empresas especializadas em segurança para abertura e fechamento das agências;

Os bancos devem mudar o layout das agências para resguardar o sigilo das transações financeiras, impedindo a observação de terceiros nos caixas eletrônicos e facilitando o posicionamento dos vigilantes;

Os bancos devem colocar grades e vidros blindados com películas nas agências e postos;

Os bancos não podem utilizar os seus funcionários para o transporte de numerário, devendo ainda zelar pela segurança na chegada e saída de valores;

Os bancos devem emitir a Comunicação de Acidente de Trabalho (CAT) para quem presenciou assaltos ou foi vítima de seqüestros e outras formas de violência no trabalho, garantindo assistência à saúde dos trabalhadores, extensiva a seus familiares em caso de seqüestros;

Os bancos devem contratar mais funcionários para agilizar o atendimento, reduzir as filas intermináveis e evitar a aglomeração de pessoas no interior das agências, o que irá garantir mais segurança para todos."

Como se vê, a maior parte da reponsabilidade pela segurança física nas agências bancárias, segundo os sindicatos dos trabalhadores da área, é dos bancos, o que a própria carta justifica em sua parte conclusiva:

"A implementação dessas demandas, que na sua maioria dependem da vontade dos bancos, é plenamente viável diante dos lucros gigantescos do sistema financeiro. Para tanto, os gastos com equipamentos e medidas de segurança não podem continuar sendo tratados como custos, que muitas vezes são ainda reduzidos para aumentarem os ganhos, e sim como investimentos necessários para defender o bem mais valioso, que é a vida humana.

A morte de bancários, vigilantes, clientes e policiais, além de muitos feridos e pessoas traumatizadas para o resto de suas vidas exige ações imediatas e eficazes de todos. A situação de violência e insegurança não pode prosseguir. Chegou a hora de os bancos considerarem a segurança como questão de responsabilidade social frente aos seus trabalhadores e à sociedade."

Ocorre, contudo, que, segundo dados da Febraban, os bancos vêm investindo sistematicamente em sistemas e serviços de segurança, para maior proteção e conforto dos funcionários, clientes e usuários dos serviços bancários, totalizando em 2007, R$ 7,0 bilhões, 133% superior aos R$ 3,0 bilhões investidos em 2003.

Os bancos estão sempre tentando satisfazer as exigências das leis de segurança bancária que entram em vigor sem levar em conta reflexões técnicas a cerca do que exigem, visando apenas, e, sobretudo, atender às exigências dos sindicatos dos trabalhadores de bancos.

As leis abaixo destacadas são alguns dos inúmeros dispositivos legais que tratam sobre segurança bancária, com a especificação de cada uma das exigências, cujo descumprimento enseja a imputação de rigorosas penalidades às instituições financeiras.

- Lei n.º 6.403, de 06/06/2007, do Município de Rio Grande/RS, que "Torna obrigatória a instalação de portas de segurança nas agências e postos bancários do município do Rio Grande";
- Lei nº 2.533, de 27/12/2007, do Município de Vacaria/RS, que "Dispõe sobre o horário de carga e descarga, local de estacionamento privativo para carros-fortes, de transportes de valores e torna obrigatória a instalação de dispositivos de segurança nas agências e nos postos de serviços das instituições Bancária e Financeiras";
- Lei n.º 12.971, de 22/07/1998, do Estado de Minas Gerais, que "Torna obrigatória a instalação de dispositivos de segurança nas agências e nos postos de serviços das instituições bancárias e financeiras";
- Lei n.º 10.501, de 09/09/1997, do Estado de Santa Catarina, que "Dispõe sobre normas de segurança para o funcionamento de estabelecimentos financeiros e dá outras providências";
- Lei nº 10.397, de 02/04/2008, do Município de Porto Alegre/RS, que "Obriga, nas fachadas externas no nível térreo e nas divisórias internas das agências e nos postos de serviço bancário no mesmo piso, no Município de Porto Alegre, a instalação de vidros laminados resistentes a impactos e a disparos de armas de fogo e dá outras providências".
- Lei n.º 8.062, de 12/12/2001, do Município de Goiânia/GO, que "Instituiu sistema de cabinas nos caixas dos estabelecimentos bancários."
- Lei n.º 7.013, de 24/07/2007, do Estado do Pará, que "Dispõe sobre a obrigatoriedade de instalação de portas eletrônicas de segurança nos estabelecimentos bancários em funcionamento nos municípios do Estado do Pará e dá outras providências."

O cumprimento material das exigências contidas nas leis é uma tarefa árdua, executada com plena das instituições bancárias bem como de seus prestadores de serviço de segurança.

A mudança de cenário devido ao investimento em segurança pela iniciativa privada

"Os bancos começaram investir com mais intensidade na segurança das agências a partir da segunda metade da década de 90. O resultado dos investimentos foi a redução de 3.575 assaltos em 1997 para 1054 em 2002. Isto significa uma queda de 71%. Se levarmos em consideração as perdas financeiras, chegamos a uma diminuição na ordem de 45%. Podemos concluir que os assaltos diminuíram significativamente. O nível de profissionalização e a questão da fuga de informação foram variáveis preponderantes." (Brasiliano)

HISTÓRICO DE ASSALTOS NO BRASIL		
	Qtde	Valores R$
1997	3575	84.321.235,30
1998	3466	107.874.375,00
1999	2523	126.919.250,64
2000	1903	74.794.906,22
2001	1302	52.224.192,56
2002	1054	46.235.405,65
Total	13.823	492.369.365,37

Dados da Federação Brasileira dos Bancos (Febraban) revelam que os assaltos a banco estão em queda no país: ocorreram 529 roubos em agências bancárias em 2008, aproximadamente um terço do número registrado em 2000, 1.903 roubos.

Conforme pode-se notar na tabela abaixo, o número de assaltos a banco vem diminuindo gradativamente ao longo dos anos no Estado de São Paulo, isso devido a medidas de segurança efetuadas pelas instituições bancárias juntamente com o poder público:

ANO	OCORRÊNCIA	MEDIDAS PREVENTIVAS ORGANIZACIONAIS	MEDIDAS PREVENTIVAS RECURSOS TÉCNICOS
1999	486	Evolução da operação bancária via internet	Apoio da Segurança pública
2000	425	Conscientização Normas e procedimentos Mudanças de itinerário do numerário	Apoio da Segurança pública Alarmes
2001	358	Diminuição do Numerário Regras Rigorosas na Logística do Transporte de valores	Apoio da Segurança pública Instalação de porta giratória

ANO	OCORRÊNCIA	MEDIDAS PREVENTIVAS ORGANIZACIONAIS	MEDIDAS PREVENTIVAS RECURSOS TÉCNICOS
2002	267	Conscientização e normas de procedimentos para os funcionários	Apoio da Segurança pública Instalação de Câmeras CFTV
2003	206	Melhoria nas normas internas Treinamento e Conscientização	Apoio da Segurança pública Implantação de equipamentos eletrônicos Mudança de Lay - out
2004	351	Redução do numerário Conscientização e treinamento Disponibilização das operações Via Internet	Apoio da Segurança pública Instalação de equipamentos
2005	351	Automatização de Processos Implantação de Plano de Segurança	Apoio da Segurança pública
2006	351	Conscientização Redução do numerário Internet Implantação do plano de segurança Treinamento	Apoio da Segurança pública Instalação de equipamentos eletrônicos
2007	285	Redução do numerário Internet Implantação do Plano de Segurança Conscientização Treinamento	Apoio da Segurança pública Instalação de equipamentos eletrônicos
2008	139	Implantação do Plano de segurança Redução do numerário Internet Conscientização Treinamento	Apoio da Segurança pública

Fontes: Redação Terra 04 de agosto de 2008
Escrito por Contraf/CUT 14/01/2009
http://aprendiz.uol.com.br/content/nosebrivet.mmp - 02/05/2007

Observando os dados, podemos concluir que houve uma queda da atratividade por assaltos a banco, isso devido às medidas preventivas tomadas pelos bancos, tanto sistêmicas quanto organizacionais. Isso gerou a queda da ocorrência de assaltos organizados, pois quando quadrilhas especializadas estudam a lógica dos sistemas implantados, tendem a desistir da ação criminosa.

Segundo Antonio Celso Ribeiro Brasiliano, dentre os fatores inibidores de assaltos a banco, os principais são "aumento de barreiras físicas integrados com normas organizacionais e sistemas eletrônicos e o pouco dinheiro nos caixas".

Essas mudanças fizeram com que os criminosos migrassem para outros tipos de crimes, como, por exemplo, os crimes virtuais. Segundo estudo do FBI – USA, um assalto a banco tradicional é roubado, em média, US$ 15 mil e os assaltantes têm 75% de chance de serem presos, enquanto que em um "assalto" digital bem-sucedido, o faturamento médio é de US$ 1 milhão e o risco de prisão é de apenas 5%.

CONCLUSÃO

As Políticas de Segurança aplicadas em nosso sistema são deficientes. Nesse ponto, convém lembrar, que, em todo o país, a manutenção da segurança interna deixou de ser uma atividade monopolizada pelo Estado.

Entre as causas dessa deficiência estão o aumento do crime, do sentimento de insegurança, do sentimento de impunidade e o reconhecimento de que o Estado apesar de estar obrigado constitucionalmente a oferecer um serviço de segurança básico, não atende sequer, às mínimas necessidades específicas de segurança que formam a demanda exigida pelo mercado.

É impossível pensar num quadro de estabilidade com relação à segurança pública de tal maneira que se protegesse por completo dos efeitos da criminalidade em sentido amplo. Porém, isso não significa que o Estado tenha de abster-se de sua responsabilidade e conformar-se com o quadro, devendo, portanto, tomar medidas sérias e rígidas de combate à criminalidade e à preservação da segurança nacional, adotando novas soluções tanto no quadro jurídico e institucional como no operacional que estejam à altura da sofisticação da criminalidade.

As instituições bancárias fazem o seu papel tentando atender às demandas das leis tanto estaduais quanto federais e os lucros dos bancos não devem servir de justificativa para que a classe trabalhadora exija da iniciativa privada a solução para a segurança das agências bancárias, seus locais de trabalho.

A insegurança é pública e é dever, principalmente, do poder público. Enquanto o Brasil for um país inseguro e violento como o é, não haverá investimento em segurança da parte dos bancos que supra as necessidades tanto de seus clientes como de seus funcionários.

Conforme foi mostrado neste artigo, houve uma grande diminuição de ocorrências criminosas quando do investimento conjunto entre o Estado e a iniciativa privada em segurança.

Contudo, os investimentos em segurança pública estão muitíssimo aquém do que seria necessário para se começar a pensar em oferecer segurança. Proporcionalmente, os Estados Unidos investem 70 vezes mais que o Brasil no combate à violência, nossos índices nos apontam como um país 88 vezes mais violento que a França.

Mariana Fernandez
Editora

sumário

Serviços de Consultoria

Laudo Técnico - Segurança Bancária

Seu banco possui Laudos Técnicos para ajudar em ARGUMENTAÇÕES JURIDICAS??

Laudos Técnicos são peças processuais elaboradas por especialistas que visam amparar as justificativas e argumentações no variado processo.

O principal benefício do laudo advém da credibilidade e experiência dos especialistas.

Tipos de Laudos Técnicos

- Blindagem
- Sistemas eletrônicos
- Procedimento
- Equipamentos
- Contexto estratégico e modus operandi

Consulte a Brasiliano, empresa que já possui EXPERIÊNCIA!!

b&a
BRASILIANO&ASSOCIADOS

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

Soluções Integradas de Segurança - Plano Tático e Técnico

Gustavo Vedove

As soluções integradas de segurança são cada vez mais procuradas no mercado atual, mas a grande questão é: as empresas sabem quais são suas reais necessidades?

Diversas soluções no mercado oferecem muito mais do que realmente será aproveitado e utilizado pelas empresas. É o caso de aplicações de softwares e plataformas completíssimas oferecidas por grandes empresas sem o devido planejamento frente às necessidades do cliente.

Toda solução integrada necessita de estudo e planejamento.

Estudo: O primeiro estudo desenvolvido deve dar a base de toda Solução Integrada. Entendimento da real necessidade do cliente considerando o ramo de atuação da empresa e conceito aplicado na solução e frente aos riscos em que a empresa está inserida. O estudo deve ser desenvolvido através da análise de riscos.

Planejamento: Dividimos o planejamento de um projeto de solução integrada em dois capítulos: Planejamento Tático e Planejamento Técnico.

- **Tático**: Soluções que visam otimizar recursos de segurança para a mitigação dos riscos identificados através do primeiro estudo. As soluções aplicadas devem, obrigatoriamente, focar focar no resultado da empresa. O planejamento tático deve oferecer detalhes da implantação dos sistemas, ordem de prioridade e prazos estabelecidos.
- **Técnico**: Na segunda fase do projeto, o planejamento técnico detalha as características, padrão de qualidade e especificações dos equipamentos, sob o ponto de vista técnico, além de descrever todo o sistema proposto na solução integrada para empresa.

Através do Planejamento Tático e Técnico os gestores podem desenvolver soluções integradas aos mais diversos segmentos como: presídios, transporte, indústria, shoppings, hospitais, bancos, varejo, condomínios residenciais, prédios comerciais, residências e plataformas de petróleo.

O Planejamento Tático e Técnico tem por finalidade dimensionar a tecnologia a ser utilizada e os recursos humanos, incluindo o posicionamento e a função adequada dos homens de segurança e meios organizacionais. Ou seja, aplicações de políticas de segurança, normas, procedimentos e implantação de barreiras físicas ou mecânicas.

Tecnologias de segurança mais utilizadas:

- **CFTV- Circuito Fechado de Televisão**.

  O Circuito Fechado de Televisão tem um valor dissuasivo muito forte, além de ser a ferramenta principal para auxiliar o operador do sistema a "enxergar" o que acontece.

  Atualmente o sistema de CFTV mais utilizado é o de gravação digital, que ocupa aproximadamente 95 % do mercado, considerado o melhor custo x beneficio para o cliente.

- **Rastreamento de veículos**.

  Tecnologias: Satelital, Celular Digital – GSM e Rádio Freqüência – RF.

- **Sensoriamento perimetral**.

  Os sistemas mais utilizados atualmente para a proteção perimetral são o sistema infravermelho ativo e a cerca eletrificada.

  As principais aplicações dos sistemas são: em condomínios residenciais, residências e indústrias de pequeno e médio porte.

- **Sensor infravermelho ativo**.

  O sistema infravermelho é composto de sensores ativos de dispositivos

compostos por um emissor e um receptor. O emissor envia um feixe de luz infravermelha para o receptor que recebe essa luz.

Qualquer pessoa ou objeto que obstrua o feixe faz com que o receptor pare de receber o sinal de luz infravermelha do emissor, disparando o alarme.

- **Cerca eletrificada**.

  Sistema ativo que provoca choques de eletricidade de 8.000 a 12.000 volts, além de gerar alarmes.

- **Botão de pânico**.

  O botão de pânico é um dispositivo que funciona com ou sem fio através de rádio frequência. A função desse dispositivo é permitir às pessoas informar a central de segurança interna ou externa, de maneira silenciosa e discreta, sobre a ocorrência de algum problema.

MEIOS ORGANIZACIONAIS:

- Política de segurança.

  A Política de Segurança de uma empresa deve estabelecer a diretriz a ser seguida. Seus objetivos devem estar sempre alinhados às estratégias corporativas de maneira a atender os seguintes objetivos:

  - Alinhar a exposição de riscos corporativos à estratégia;
  - Otimizar as decisões de resposta a riscos;
  - Reduzir surpresas e prejuízos operacionais;
  - Identificar e gerenciar riscos inerentes aos negócios;
  - Fornecer respostas integradas aos diversos riscos;
  - Melhorar a alocação de recursos;

  Conscientizar todo pessoal, contratados, parceiros, fornecedores e prestadores de serviços sobre a importância estratégica de suas ações na eficácia da Política de Segurança.

- **Normas e procedimentos**.

  Realização de tarefas de forma padronizada, quem faz o que, como, quando, onde. A criação e o objetivo de normas e procedimentos é fundamental para a melhoria dos processos de segurança.

- **Barreiras físicas e mecânicas mais eficientes**:

  Muros.

  Catracas.

  Torniquetes.

  Cancelas.

Toda essa integração cria um ciclo completo para a segurança com o objetivo de dificultar e diminuir as chances dos riscos identificados virem a acontecer. A solução integrada, independentemente do setor e área de atuação da empresa, deve sempre ter o foco no usuário, ou seja, em suas expectativas.

Gustavo Vedode
Consultor da Brasiliano & Associados
gvedove@brasiliano.com.br

sumário

Serviços de
Outsourcing

Tire o peso de suas costas !
Deixe para quem é ESPECIALISTA!!

Outsourcing é a terceirização do processo de gestão de riscos e da segurança empresarial. O escopo inclui o planejamento, a implantação e a administração de todos os serviços e processos terceirizados.

Vantagens do Outsourcing:

- Mão-de-obra especializada
- Melhoria da qualidade do serviço
- Otimização de recursos
- Aumento da produtividade
- Liberação da estrutura da empresa para sua atividade fim
- Simplificação da estrutura interna
- Redução de ação trabalhista
- Agiliza decisões e ações

Consulte – nos!!!

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

Assalto a condomínios no estado de São Paulo

Fernando de Bonneval de Carvalho

Desde 2005, a onda de assaltos no estado de São Paulo vem ganhando grande importância no índice de criminalidade do estado. Entre 2006 e 2007, o aumento dos casos chegou a 200%, sendo a região preferida dos assaltantes o bairro dos Jardins. Os condomínios estão vulneráveis à ação de bandidos. Essa é a realidade das grandes cidades brasileiras. Os arrastões tornaram-se o crime da moda e os síndicos correm atrás do prejuízo. O que queremos neste artigo é verificar as possíveis causas do aumento de assaltos em condomínios, bem como identificar o *modus operandi*.

Não foi difícil para a marginalidade descobrir que os prédios de condomínios fechados apresentavam inúmeras fragilidades no sistema de controle de acesso, principalmente o de veículos. Em uma reportagem da Rede Record (disponível no link http://tudosobreseguranca.com.br/portal/index.php?option=com_content&task=view&id=340&Itemid=142), a produção do programa, com um veículo descaracterizado e com uma câmera escondida, tentou entrar em 10 prédios de um bairro nobre de São Paulo. "Com uma simples buzinada ou uma conversa fiada, conseguiram entrar em 5 prédios, pela garagem", constatou o repórter na matéria.

A invasão pela garagem é um dos caminhos mais procurados pelos bandidos. O plano de gangues especializadas em invadir prédios, tem como fator principal a rendição da guarita.

Com o porteiro dominado, fica fácil para os bandidos gerenciarem a invasão dos apartamentos, pois, dessa forma, têm o controle da entrada e saída de pedestres e veículos. Assim, usam diversos ardis para dominar moradores que entram no prédio ou saem de seus apartamentos.

Portanto, conseguindo-se entrar pela garagem, fica fácil abordar o porteiro usando o trunfo da surpresa, já que a atenção dele é normalmente voltada para as áreas externas do edifício.

Abaixo um breve relato de ocorrências relacionadas ao risco de arrastão:

DATA	LOCAL	CRIME
08.03.2009	Vila Mariana	Oito bandidos foram presos durante uma tentativa de assalto a um condomínio na Vila Mariana. Cerca de 18 pessoas foram rendidas pelo bando, formado por pelo menos 9 assaltantes. Por volta das 23h deste sábado, os bandidos invadiram um prédio localizado na rua Afonso de Freitas, rendendo o porteiro. - Porteiro: "Eu já tinha percebido que ele estava andando meio perdido no prédio, então acionei o botão de pânico antes dele chegar até mim.". Após a chegada da polícia militar, os criminosos acabaram fugindo para um prédio vizinho, tornando reféns pelo menos sete moradores. Houve troca de tiros entre policiais e assaltantes, mas ninguém foi ferido. Fonte: oglobo.globo.com
08.03.2009	Centro	Os sete homens que invadiram um prédio na Rua Rangel Pestana, no Brás, região central de São Paulo, na manhã de domingo dia 08/03/2009, tinham como alvo comerciantes orientais. Dois assaltantes foram presos e cinco ainda estavam foragidos na noite de domingo. Os criminosos, que tinham a chave do portão de entrada, invadiram 7 apartamentos. Três vítimas foram agredidas com socos e coronhadas, os assaltantes que fugiram levaram dinheiro e aparelhos eletrônicos como celulares. O prejuízo de um dos moradores chega a mais ou menos R$ 6 mil. Fonte: g1.globo.com
02.03.2009	Perdizes	Uma quadrilha armada fez mais um arrastão em um condomínio residencial na cidade de São Paulo. Desta vez, o alvo foi o edifício Sumaré Tower na rua Piracuama, no bairro de Perdizes, zona oeste da capital. Os bandidos utilizaram o controle remoto de acesso à garagem para invadir o prédio e render o porteiro, na manhã desta segunda-feira. Segundo testemunhas, pelo menos 20 homens bem vestidos e fortemente armados com fuzis e metralhadoras participaram da ação.
11.01.2009	Bairro Pedra Branca	Trinta homens fortemente armados, com fuzis, metralhadoras e pistolas, invadiram o condomínio onde o crime ocorreu por volta das 02h30min, o grupo chegou ao local em dez carros. Um balanço parcial do roubo esta em torno de 18mil reais em jóias, dois carros, 13 aparelhos celulares, uma maquina fotográfica, um tocador de DVD, um notebook além de mil reais em dinheiro. Fonte: Portalleprestsserv.com.br
10.01.2009	Alameda Lorena / Bairro Jardins	Dez assaltantes invadiram um condomínio de luxo e fizeram um arrastão em nove apartamentos, levando jóias, dinheiro, notebooks, celulares e um automóvel. Dois assaltantes invadiram o prédio pelos fundos, provocando o disparo do alarme do local. O porteiro foi pessoalmente checar a situação e acabou sendo rendido pelos ladrões, onde foi obrigado a liberar a entrada dos outros assaltantes. Fonte: Portalleprestsserv.com.br
17.11.2008	Condomínios Residenciais Jardim Petrópolis/ Itapecerica da Serra	Criminosos armados invadiram um condomínio residencial, eles usavam camisetas com inscrição da policia civil e roubaram várias casas. Permaneceram duas horas e fugiram em carros dos moradores. O grupo seria formado por vinte homens. Segundo a polícia, eles teriam entrado no condomínio após dizerem que estavam investigando uma ocorrência de tráfico de drogas. Fonte: g1.globo.com

Fonte: jovempan.uol.com.br,

Poderíamos dizer, então, que somente a classe A é visada pelos assaltantes? Infelizmente não.

Devido a grande preocupação com o combate a esta modalidade desde 2006, as ditas quadrilhas esfacelaram-se e os criminosos partiram para investidas particulares, ainda nos condomínios, mas especificamente em unidades isoladas.

Contudo, à medida que foram ganhando experiência, os meliantes começaram a formar novas quadrilhas e voltaram a atacar. Dessa forma obtiveram mais sucesso, mesmo mantendo o *modus operandi* de antes.

Como é possível combater tal ameaça? Muitos podem dizer através do armamento dos funcionários de segurança do condomínio. Porém, de acordo com o Sindicato das Empresas de Segurança e Vigilância do Estado de São Paulo (Sesvesp), aproximadamente 70% dos condomínios brasileiros com vigilância armada estão à mercê de empresas pouco qualificadas. O que, à primeira vista, pode parecer mero detalhe, representa grande risco, porque as armas não bastam para tornar o condomínio mais seguro.

É preciso ainda, segundo o sindicato, um projeto de segurança que inclua análise de risco, normas e procedimentos, além de um Plano de Contingência, para ser acionado em situações emergenciais. Para que um vigilante armado esteja no interior de um condomínio sem representar perigo, é necessário que esteja atento à posição da guarita, e ainda, aos equipamentos de segurança disponíveis. É essencial obter um levantamento das ocorrências mais comuns na região para poder se prevenir.

O importante também é aceitar que apenas os equipamentos eletrônicos não garantem a segurança. Como foi dito antes, primeiro o condomínio deve conhecer o seu risco para depois investir em treinamento, procedimentos e equipamentos.

Se o condomínio não quantificar os riscos a que ele está exposto, corre o risco de investir em equipamentos e, literalmente, jogar dinheiro fora (conforme notado em http://www.direcionalcondominios.com.br/materias/agosto_05/assaltosemcondominios.htm). O condomínio precisa entender a importância de contratar um profissional de segurança.

Através de uma consultoria, ele irá definir um projeto com as melhores práticas de segurança para cada edifício. A partir do projeto, o condomínio vai então buscar os equipamentos no mercado.

Notamos, então, que a qualidade da segurança em um condomínio está amarrada à qualidade da mão-de-obra de segurança. O fator humano é uma das chaves para a efetiva segurança, ou não, de um condomínio.

É imperativo que os condomínios tenham rigor ao selecionar uma prestadora de serviço ligada à segurança, porém, o padrão da qualidade da mão-de-obra no mercado brasileiro é fraco.

Para isso, é extremamente importante que o condomínio avalie as empresas de segurança existentes no mercado que se adequam às suas necessidades.

Porteiros e garagistas são os responsáveis pelos controles de acesso de um edifício e costumam ser facilmente enganados pelos bandidos por pura ingenuidade. Há

inúmeros casos que comprovam o fato: falsos entregadores de pizza que chegam para presentear o porteiro com uma pizza, porteiros que saem da guarita para receber encomendas como flores, bichos de pelúcia, ou cestas de café da manhã. Todos esses problemas estão intimamente ligados à falta de treinamento desses profissionais.

O maior problema é que muitos síndicos acham desnecessário investir em cursos específicos para funcionários. Onde existem pessoas prestando serviços para outras pessoas, a única forma de modificar comportamentos distorcidos é através de um bom treinamento.

As pessoas devem deixar de ver o treinamento apenas como um mero gasto. Esse deve ser visto como um investimento para o condomínio, onde o retorno vem através da maior qualidade da mão-de-obra na portaria, acarretando um nível satisfatório de segurança para todos.

O *modus operandi* é organizado, ou seja, ele exige uma arquitetura baseada nas falhas de segurança do condomínio visado. Portanto, é imperativo desenvolver uma análise de risco no condomínio para verificar quais são os riscos a que esse está exposto, para assim, desenvolver medidas preventivas para coibir assaltos.

Porém, mesmo destacando que o fator humano de segurança é uma das peças chaves para a segurança dos condomínios, não podemos deixar de levar em conta o descuido dos próprios moradores. Segundo o professor do Senac e instrutor de segurança, Carlos Eduardo Machado, "as quadrilhas estão se especializando e os condôminos devem ajudar os porteiros no controle de acesso".

Não é somente o síndico, a administradora ou os funcionários, os únicos responsáveis pela segurança dos condomínios. O morador deve fazer sua parte, para que haja uma proteção mais efetiva. Essa participação é fundamental para que os riscos possam ser detectados, controlados e minimizados no interior dos condomínios.

Fernando de Bonneval de Carvalho
Consultor da Brasiliano & Associados
fbonneval@brasiliano.com.br

sumário

Auditoria de Controles Internos

Rosângela Aparecida Stringher

A busca por eficiência operacional pelas grandes organizações tem aumentado consideravelmente nos últimos anos. Isso devido tanto à ocorrência de prejuízos por riscos operacionais e à competitividade acirrada do mundo globalizado, quanto à Resolução 2.554/1998 editada pelo Banco Central do Brasil e às recomendações das normas pertinentes à Gestão de Riscos Corporativos.

Contudo, para alcançar tal propósito surge um desafio: o de fazer com que haja entre todas as áreas, efetiva integração e sinergia.

É de suma importância o envolvimento da auditoria no processo de avaliação dos controles internos das instituições. Nesse novo cenário, é igualmente importante conscientizar os gestores da responsabilidade dessa política, que é de todos os funcionários e não mais de interesse exclusivo de profissionais.

Embora existam várias definições de controles internos, todas visam assegurar que as fases de processos decisórios e do fluxo de informações sejam de extrema confiabilidade, por isso remetem-se às políticas adotadas pelas organizações, tendo por objetivo mitigar riscos e melhorar processos.

É importante ressaltar que, os controles internos devem atender às necessidades da organização e, para isso, sua qualidade não é ditada pela quantidade, como demonstra a figura abaixo.

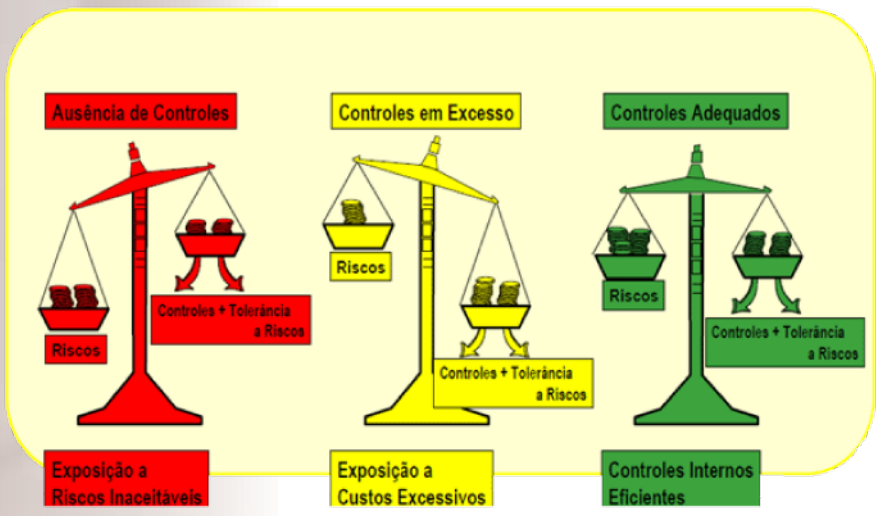


Figura 1 (Brasiliano & Associados)

A avaliação de controles internos é o meio pelo qual a adequação e a efetividade são analisadas, visando garantir a continuidade de todos os negócios da instituição. Esse mecanismo deve ser sempre repetido como incentivo a constantes melhorias, certificando-se que cada uma de suas etapas seja devidamente documentada.

A Auditoria Interna, entre outras atividades, executa a avaliação de controles internos, a fim de determinar a eficiência desses, a exposição aos riscos, a qualidade dos planos de ação para corrigir aspectos falhos ou vulneráveis, bem como a probabilidade de se alcançar as metas do negócio.

É preciso esclarecer que a metodologia de avaliação dos controles internos, para muitos, é nova e apresenta-se em crescimento. Seu sucesso está diretamente relacionado com o envolvimento dos participantes.

Todas as áreas da empresa podem sofrer eventuais problemas que interfiram na efetividade dos controles internos adotados. Isso significa que um adequado sistema de controle sobre cada uma dessas funções assume fundamental importância para atingir resultados mais favoráveis, pois a falta de procedimentos de controles internos propicia erros e desperdícios.

A Auditoria de Controles Internos favorece as empresas no que diz respeito à proteção mais eficaz por um custo reduzido, tendo em vista que a Auditoria determina a extensão de seu exame e os procedimentos a serem aplicados, os quais, inclusive, devem prever investigações mais detalhadas em contas ou em áreas perigosas das companhias.

Entende-se que a auditoria é necessária e fundamental não só na estruturação dos controles da organização, como também na formulação de outros planos empresariais. Trata-se de um braço da empresa que auxilia o gerenciamento efetivo de seus riscos.

Determinar a eficácia e a eficiência de mecanismos corporativos estabelecidos, a fim de "fechar as portas" para possíveis fraudes é a finalidade da revisão da adequação do sistema de controles internos, não deixando de observar além da organização interna e procedimentos existentes, alguns outros aspectos, como:

- consecução de metas estratégicas e táticas da organização;
- fiel cumprimento de normas e legislação;
- proteção dos ativos e segurança física e lógica;
- qualidade das informações, serviços e produtos;
- redução de custos quanto à eficiência e efetividade na obtenção e no uso dos recursos econômicos, materiais e humanos.

O SCI - Sistema de Controles Internos - que não esteja apoiado em processos da auditoria, pode ser considerado, até certo ponto, inútil, uma vez que não é possível confiar plenamente nas informações prestadas pelos gestores da empresa. Cabe ressaltar que, considerar a confiança nos subordinados não deixa de ser correto, porém, é necessário admitir que esse pode ser um fator facilitador de irregularidades, as quais podem ter resultados catastróficos para as empresas, seja no que tange a imagem ou até mesmo o aspecto financeiro.

Controles internos ou auditoria interna, à medida que desempenham funções da maior relevância no mundo dos negócios, são necessidades impostas àqueles que buscam a eficácia organizacional.

Rosângela Aparecida Stringher
Consultora da Brasiliano & Associados
rstringher@brasiliano.com.br

sumário

Liderança: um tema velho, uma necessidade sempre atual

Álvaro Takei

Liderança é um diferencial profissional e, sem dúvida, continuará sendo.

A afirmação acima faz relembrar antigas questões:

1. A liderança pode ser desenvolvida?
2. Assumindo que possa, de quem é a responsabilidade pelo desenvolvimento, do colaborador ou da empresa?

Vamos tentar, ao longo deste texto, (re)discutir estas questões.

Constatamos, há vários anos, uma série de evoluções e revoluções nos modelos de gestão de empresas. Uma parte deles indica técnicas baseadas em uma determinada tendência, outra parte indica ações praticamente contrárias. Tais modelos surgem e, muitas vezes, são adotados como modismos, sem que haja tempo para aprender e assimilar profundamente seus conceitos e princípios. Exemplos disso foram a reengenharia, o *downsizing* e o *rightsizing*, que vieram com propostas de repensar todos os processos e procedimentos operacionais e de tornar as empresas mais enxutas ou, ainda, no tamanho certo.

Hoje, contradizendo ou corrigindo essas teorias, vários autores fazem propostas de novos caminhos. Fala-se muito na necessidade das empresas darem especial atenção ao conceito da estratégia empresarial, destacando a questão da competitividade na sua aplicação. Assim, o foco na criação de produtos e serviços, de forma planejada, sempre visando o futuro da empresa, criando mercados e consumidores de forma sustentável, passa a ser muito mais importante do que instituir um processo de demissões, acabar com postos de trabalho e reestruturar uma organização.

A variedade de modelos e soluções, no meio de um contexto econômico altamente dinâmico, que gera incertezas e dificulta previsões e planejamento de longo prazo, faz com que o líder assuma importância fundamental, uma vez que passa a ser responsável pela decisão entre reduzir e reorganizar estruturas e processos ou incentivar e promover o crescimento de uma empresa, o que exige grande capacitação.

É neste cenário que o líder deve atuar; organizando, dirigindo e relacionando-se com pessoas, de forma que elas alcancem seus objetivos profissionais, que levarão à realização dos resultados empresariais e, o principal, fazendo com que seus colaboradores trabalhem motivados. É um grande desafio!

O desafio da liderança provoca dúvidas sobre como deve ser o perfil do líder na empresa contemporânea, bem como, sobre a forma como ele deve se preparar para gerir a empresa, de maneira que ela tenha alta competitividade, para garantia de sua permanência no mercado. Estas dúvidas, pela dificuldade de serem sanadas, levam empresários e gestores de pessoas a apurarem seus processos de recrutamento e seleção, na esperança de encontrar líderes prontos no mercado de recursos humanos. Entretanto, esquecem que raramente os encontrará tão prontos como esperam e, principalmente, disponíveis.

Surgem, dessa maneira, mais dúvidas: Qual a solução? Como conseguir profissionais qualificados e capacitados? Como obter a motivação dos colaboradores? São perguntas cujas respostas indicam, invariavelmente, a educação continuada e o treinamento *in company* como formas de desenvolver o quadro de pessoal. Isso faz acreditar, então, que líderes podem ser difíceis de serem encontrados, mas podem ser formados dentro das organizações, com a vantagem de já conhecerem as empresas em que atuam e suas respectivas culturas.

A solução apontada, apesar de ser simples de expor, é algo que exige certos cuidados, os principais são:

- Por iniciativa da alta direção, deve haver ampla divulgação da missão, visão, princípios, valores e objetivos da organização, para que cada profissional possa ter claro o que a empresa espera e o que é necessário para que ele se torne adequado às expectativas;
- Um movimento *top/down*, incentivando a busca do desenvolvimento profissional, por meio de políticas e diretrizes de educação, treinamento e aprendizagem;
- Criação de um ambiente que privilegie o aperfeiçoamento,

em que o erro é encarado como forma de aprendizagem e os sucessos são recompensados;

- Promover a gestão do conhecimento, de maneira que todos os dados e informações, que sejam relevantes para o desempenho profissional com excelência, fiquem disponíveis a todos;
- Diagnosticar falhas ou faltas na qualificação e/ou capacitação dos colaboradores, em relação aos objetivos empresariais, e promover formas de supri-las, ou seja, facilitar a busca de conhecimentos e habilidades, que levem às atitudes esperadas.

Os cuidados mencionados são os mínimos esperados, para que as empresas possam incentivar e facilitar o crescimento dos colaboradores, promovendo a possibilidade de desenvolvimento de lideres.

Até aqui respondemos à primeira pergunta inicial, ou seja, liderança pode ser desenvolvida. Sabemos que existem aqueles que a tem como algo nato, mas, os que não são afortunados com a liderança, como se fosse um dom, podem adquiri-la.

Resta responder à segunda pergunta do início. O texto indica ações e cuidados que levam a crer que a responsabilidade no desenvolvimento da liderança é das empresas. Entretanto, não se engane! Nada do que a empresa fizer vai funcionar, se em cada profissional não existir a vontade de aproveitar o que foi oferecido. Mais, se a empresa não fizer nada do que foi dito, cabe a cada um buscar seu próprio desenvolvimento.

Portanto, independentemente do que a empresa está fazendo por você, busque sempre seu desenvolvimento, seja responsável pelo seu crescimento, seja dono do seu destino profissional. A educação continuada é o caminho.

* Texto original do autor

Álvaro Takei
Diretor de Ensino Digital da Brasiliano & Associados
takei@brasiliano.com.br

sumário

treinamento

VOCÊ ESTÁ PREPARADO PARA OS NOVOS DESAFIOS DE RISCOS DO MERCADO??

PREPARE-SE !! FAÇA DIFERENÇA !!

Frequente os cursos da Brasiliano&Associados, empresa com mais de 20 anos de experiência em Gestão de Riscos Corporativos !!

informações | 11 5531-6171
| www.brasiliano.com.br
| info@brasiliano.com.br

b&a
BRASILIANO&ASSOCIADOS

LER & SABER

Mariana Fernandez

TOMANDO AS RÉDEAS EM NOVOS CENÁRIOS

A *Nova Governança Corporativa* (Saint Paul, 2009) de Martin Hilb publicado em diversos idiomas (alemão, chinês, espanhol, inglês, russo e vietnamita) chegou ao Brasil vitorioso internacionalmente. A obra fala das ferramentas bem-sucedidas para conselho de administração.

Martin Hilb é professor de Business Administration na University of St. Gallen, Suiça, onde também dirige o IFPM Center for Corporate Governance, um centro de pesquisa, educação e consultoria em Governança composto por pesquisadores e consultores de diversas nacionalidades. Luiz Fernando Turatti desenvolve seu PhD no IFPM, sendo consultor e pesquisador do centro e autor do prefácio da edição brasileira.

Hilb é também consultor de trabalhos realizados em mais de 60 países, tendo adquirido parte de sua experiência em transnacionais como Nestlé S.A., Martin & Co. e Schering- Plough Corporation.

O autor divide o livro em várias esferas, abrangendo além de introdução e conclusão, quatro princípios para o conselho de Governança Corporativa, sendo as dimensões: situacional, estratégica, de gestão integrada do conselho de administração e do controle.

"O fundamental dessa abordagem é o jogo de instrumentos desenvolvidos e testadoss pelo autor; os quais podem ser empregados pelos conselhos de administração para conferir às suas organizações direção estratégica e controle efetivos".

Os principais conceitos desenvolvidos por Hilb são ilustrados através de organogramas, ferramentas práticas ou estudos de caso, sendo a obra adequada à linguagem prática almejada pelos gestores empresariais.

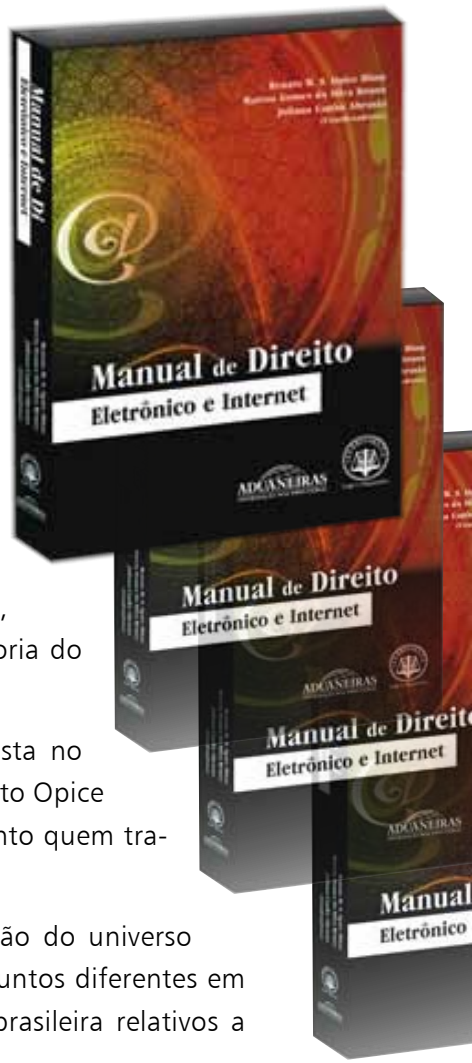
Na quarta parte do livro, Dimensão do Controle (mantenha-o controlado), o consultor introduz a abordagem integrada, onde a dimensão de monitoramento do conselho engloba funções de auditoria e gerenciamento de risco.

Dentre as funções de gerenciamento de risco do conselho, Hilb destaca "o processo de detecção prematura, prevenção e gerenciamento de perigos, e com a identificação e a realização efetiva de oportunidades empreendedoras... (isto é, a consciente) exploração de riscos, nas quais possa haver oportunidades, e a prevenção ou redução de riscos, em que o risco antecipado supera os retornos esperados. O gerenciamento de risco lida principalmente com maiores garantias no planejamento e com uma probabilidade maior de que os objetivos da empresa sejam atingidos, aumentando o valor da empresa".

O autor ainda ensina através de ferramentas como a matriz de risco do negócio, a controlar o risco existente, definir a estratégia de risco desejada, identificar as barreiras de risco e traçar medidas de gerenciamento de risco.

As conclusões, contudo, são breves, tratando-se sinteticamente de um manual de governança frente aos novos cenários.

TOMANDO CIÊNCIA DE SEUS DIREITOS ELETRÔNICOS



Quais as responsabilidades civis de quem pratica spamming? Que direitos tem o autor sobre uma foto ou um texto publicado na Internet? Quando a Certificação Digital será obrigatória nas transações eletrônicas? Essas e outras questões relacionadas à sociedade digital e aos meios eletrônicos estão no *Manual de Direito Eletrônico e Internet* (Aduaneiras, 2006), uma obra inédita pela forma de sua organização.

Com o êxito de reunir trinta e seis especialistas em Direito Eletrônico e Direito Digital o livro traz textos revestidos de uma apresentação objetiva e atual dentro de seus respectivos temas.

O manual compreende importantes questões como a segurança, prova, certificação digital, privacidade, uso da Internet em ambiente eletrônico, spam, informatização do judiciário, processo judicial eletrônico, e-gov, aspectos jurídicos do software, crimes informáticos, contratos eletrônicos, responsabilidades e questões tributárias. Todos coordenados por Renato Opice Blum, Marcos Gomes da Silva Bruno e Juliana Canha Abrusio. O prefácio é de autoria do presidente da entidade, Abram Szajman.

A obra aborda questões legais e jurídicas para Web. Segundo o especialista no assunto e presidente do Conselho de Comércio Eletrônico da Fecomercio, Renato Opice Blum, o manual servirá para orientar tanto profissionais da área juridica, quanto quem trabalha com tecnologoia da informação e informática.

Com textos de fácil entendimento, permitindo ao internauta a compreensão do universo virtual e de questões jurídicas que regem o segmento, o livro trata de 33 assuntos diferentes em 680 páginas, discutindo os pontos mais polêmicas encontrados na justiça brasileira relativos a segurança eletrônica.

É indicado para advogados interessados em atualizar-se em relação às novas questões legais e jurídicas dos meios digitais, a consultores de risco em TI e gestores em geral.

Como se vê, uma obra ampla, completa e interdisciplinar, apta a contribuir e auxiliar o interessado por este novo ramo do Direito, fruto da evolução dos meios eletrônicos e de telecomunicações.

O **prefácio e os temas introdutórios do livro**, de autoria de Aires José Rover, estão disponíveis na internet.

sumário