ISSN 1678-2496N

b&a BRASILIANO & ASSOCIADOS

GESTÃO de RISCOS

Setembro 2010 | edição 59

SOLUÇÕES INTEGRADAS DE SEGURANÇA

ANÁLISE

Fuga Involuntária da Informação

EM FOCO

Pulseira Eletrônica em Recém-Nascido


equilíbrio
entre técnica X ousadia
178
109
42
A BRASILIANO & ASSOCIADOS analisa e avalia seus riscos, otimiza e oferece soluções.
Com a BRASILIANO & ASSOCIADOS sua empresa terá uma Gestão de Riscos Integrada.
b&a
BRASILIANO&ASSOCIADOS
info@brasiliano.com.br
www.brasiliano.com.br
11 5531 6171

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** | Agencia BM Design

Colunista | Mariana Fernandez **Colaboradores desta edição** | Alex Henrique, Andre Pitkowski, Claudio dos Santos Moretti, Evaldo Tavares Barbieri, Gustavo Vedove, João Aparecido dos Santos e Leandro Fortes

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

Ponto De Vista: Primarização Dos Serviços De Segurança! Retrocesso De Gestão? Parceria Galinha x Porco!

PONTO DE VISTA

Senhores, este editorial visa gerar polêmica e ao mesmo tempo reflexão. O tema é de extrema importância e vem gerando muita controvérsia. Temos uma tendência, que até pode ser revertida, dependendo da postura dos gestores de segurança como contratantes e dos prestadores de serviço como contratados. Vamos ver os questionamentos.

Desde a década de 1980 nos países desenvolvidos e desde a de 1990 no Brasil, grandes empresas vêm buscando adequar sua estrutura organizacional às novas exigências de um mercado competitivo que demanda constante redução de custos, qualidade, velocidade de produção e atendimento ao cliente, com objetivo de encontrar um arranjo organizacional que possibilite maiores e melhores resultados.

Dessa maneira, os modelos de gestão tradicionais caracterizados pelo controle, pela centralização e pela hierarquização passaram a ser substituídos por modelos mais flexíveis, mais horizontalizados.

Ao mesmo tempo, depois de um passado de atuação isolada, em que cada empresa possuía fronteiras nítidas, novas combinações de operações têm sido colocadas em prática, na forma de alianças ou joint ventures, visando solucionar deficiências de conhecimentos, de capital e de acesso a novos mercados.

As estruturas empresariais em rede, representadas em grande parte pelo aprofundamento e maior abrangência dos processos de terceirização, se transformam em tendência. Os negócios passam em parte a ser realizados por um conjunto de empresas: elas somam recursos e fazem intercâmbios técnicos e complementares, sem que percam sua independência.

Nesse quadro, ganhou força a flexibilização da remuneração –por meio da recompensa por resultados–, a flexibilização da jornada –por meio de horários flexíveis– e, em especial a flexibilização do contrato de trabalho –sobretudo por meio da terceirização.

O contexto mostra que a terceirização e ou quarteirização de determinadas atividades da segurança e gestão de riscos pode muito bem suportar as operações da empresa, com uma relação custo versus benefício muito boa. Em contrapartida a primarização, retorno da segurança própria, no nosso setor, no meu ponto de vista, vai demonstrar um forte retrocesso em termos de gestão. O grande problema que nossos colegas gestores e administradores colocam como base para a volta da segurança patrimonial orgânica são dois: o custo versus a qualidade do serviço prestado. A reclamação é a mesma, acaba não compensando porque os gestores pagam para ter determinado nível de serviço e não o tem.

Só para apimentar vamos entender um lado de uma pesquisa quantitativa realizada pelos professores Maria Elizabeth Rezende Fernandes (Fundação Dom Cabral) e Antônio Moreira de Carvalho Neto (PUC Minas Gerais), com a significativa amostra de 513 dirigentes de 179 dentre as 500 maiores empresas em operação no Brasil, abrangendo todos os setores das principais atividades econômicas do Brasil.

Em todos os aspectos da gestão de pessoas pesquisados verificou-se que tanto atualmente como há três anos os terceirizados revelaram médias significativamente inferiores às dos colaboradores efetivos das empresas.

O aspecto de maior relevância foi o referente ao compartilhamento do aprendizado dos colaboradores com os demais profissionais terceirizados. Ficou entendido a dificuldade ainda encontrada pelas empresas em criar mecanismos que propiciem a gestão do conhecimento organizacional.

Destaca- se, portanto, a importância do investimento em sistemas, processos e ferramentas que estimulem o envolvimento dos funcionários na geração e manutenção de aprendizado contínuo. Só para reflexão, talvez seja este um elemento-chave para que as empresas contratantes sejam capazes de atender às exigências do mercado.

Outro aspecto identificado foi o preparo das contratadas em realizar a gestão dos profissionais terceirizados. Levando em conta a relevância da amostra, pode-se inferir que esse despreparo esteja generalizado nas empresas de grande porte do País.

Uma análise conjunta dos aspectos relativos ao comprometimento, à operação, à confiança, ao compartilhamento do aprendizado e à autonomia denota significativa distância entre os colaboradores efetivos e os terceirizados.

A dificuldade constatada pela pesquisa para o estabelecimento de confiança na relação da gestão com os terceirizados pode ser interpretada pela falta de clareza quanto à equidade nas condições de trabalho, às perspectivas de desenvolvimento, à remuneração e ao tratamento diverso com relação aos terceirizados.

Quanto às práticas de gestão referentes à remuneração, à comunicação, ao poder de decisão na contratação, ao treinamento e ao desenvolvimento das pessoas, também é significativa a diferença observada entre terceirizados e colaboradores efetivos.

A pesquisa sugere que, mesmo nas maiores e melhores empresas do Brasil, a remuneração por metas e resultados está longe de se tornar realidade para os terceirizados. Se estes não são remunerados conforme os resultados alcançados, pode-se depreender que encontram dificuldade em se sentir "parte do time".

O que tem prevalecido é a lógica de redução de custos nos processos de contratação dos terceirizados. O paradoxo que se instala parece insolúvel nessa lógica, que, ao mesmo tempo que reduz diretamente os custos, aumenta enormemente os desafios para os gestores e exige das empresas novos investimentos na adequação de políticas e práticas de gestão de pessoas, além de aumentar os custos de transação.

O resultado obtido pelas empresas torna-se questionável, e a aparente redução de custos, discutível.

Será que nosso segmento não trabalha assim também? Como obter resultado nessa lógica inversa e míope?

Eu não sei, você sabe??

Boa leitura e sorte!!!

Antonio Celso Ribeiro Brasiliano
Diretor Executivo

abrasiliano@brasiliano.com.br

b&a
BRASILIANO & ASSOCIADOS

EDITORIAL

Tecnologia e Profissionalismo: pontos-chave da GR

O editorial desta edição não tem seu foco num artigo ou coluna específicos mas em todo o conteúdo da revista. Trouxemos nesta edição, por mais que divididos em várias editorias, a questão da tecnologia na área de gestão de riscos.

Muito já discutimos aqui sobre os erros não somente de pessoas comuns mas de profissionais de segurança e gestão de riscos que confiam demais, e somente, na tecnologia para satisfazer as necessidades de proteção e prevenção da organização. Sem uma análise prévia das necessidades da organização e a escolha e monitoramento correto da solução tecnológica, ao invés de prevenir perdas e proteger a organização, estaremos abrindo uma lacuna na rede de proteção.

Imaginando a organização como um forte, com suas devidas muralhas, torres e portão, se confiarmos apenas na dureza das rochas, na rigidez do portão e na vigilância das torres, corremos o sério risco de sermos dominados ou engolidos pelo inimigo. Temos que poder confiar sobretudo na força tática e técnica dos operadores das armas e sistemas.

Sem o profissionalismo necessário aliado à tecnologia, corremos o risco de, através de um ponto de fragilidade em nossa segurança, possibilitar uma lacuna para que os bens se esvaiam, ou para haja uma possível troca entre colaboradores e concorrentes, ou ainda, para que os "inimigos" ataquem.

Quanto à possibilidade de "os bens" se esvaírem, Cláudio dos Santos Moretti fala nesta edição sobre o enorme, porém ainda muito negligenciado, problema da fuga involuntária da informação - o qual também pode ser caracterizado como uma troca ilícita entre colaboradores e concorrentes.

Englobando, como acima, as duas possibilidades de insegurança, está o artigo de Evaldo Tavares Barbieri sobre a pulseira eletrônica em recém-nascido, uma solução que, se bem empregada pode assegurar tanto as organizações de saúde quanto as famílias e seus bebês.

As antigas torres dos fortes e castelos são hoje as salas de comando e controle, contempladas no artigo de Leandro Fortes, com enfoque operacional.

Num artigo mais amplo sobre TI, o especilista Andre Pitkowski dá uma verdadeira aula sobre mitigação de riscos na área.

E, ainda nesta edição, a opinião de Alex Henrique e um lançamento especial sobre Gestão de Riscos em Shoppings Centers, o mais completo e comprometido no assunto.

Confiram a seguir receitas de sucesso através da aliança de tecnologia com profissionalismo.

Boa leitura!

Mariana Fernandez

Editora

b&a
BRASILIANO & ASSOCIADOS

Fraud Risk Assessment

A fraude hoje nas empresas é um tema de preocupação estratégica, pois afeta de forma direta a competitividade e a imagem. As últimas pesquisas realizadas nos Estados Unidos, pelo ACFE, comprovou um aumento de 65% em relação ao ano de 2002.

Acreditamos, embora haja esta preocupação estratégica, que ainda exista muito o que fazer em termos de prevenção.

A Brasiliano & Associados avalia os riscos de fraudes nos processos das empresas e realiza auditoria investigativa. Oferecemos um trabalho independente, com uma visão prospectiva, utilizando ferramentas de tecnologia da informação voltados à prevenção, detecção e investigação.

Possuímos uma equipe multidisciplinar, com capacidade e visão de vários segmentos empresariais. Prestamos os seguintes serviços:

- Investigação de Fraude
- Gestão de Risco de Fraude – Mapeamento, Avaliação e Respostas ao Risco de Fraude
- Tecnologia Forense
- Verificação de Antecedentes – Background Checks Investigation
- Compliance em antilavagem de dinheiro
- Estruturação e Operacionalização de Canal de Comunicação – Denúncia
- Serviços de Ética Comercial
- Serviços de FCPA – Programas de Prevenção, Monitoramento e Controles Internos – Corrupção e Antisuborno

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

b&a
BRASILIANO&ASSOCIADOS

Pulseira Eletrônica em Recém-Nascido

Evaldo Tavares Barbieri

Resumo

O uso da pulseira eletrônica com RFID em recém-nascidos nos hospitais e clínicas; métodos para evitar o sequestro dos bebês; como agem as pessoas que pretendem cometer o sequestro, fazendo uso de informações, sacolas e outros recursos para o ato ilícito; os processos judiciais sob os quais as instituições de saúde estão sujeitas; e a exposição do assunto nas emissoras de televisão em horários nobres.

Palavras-chave

Recém-nascidos, pulseiras eletrônicas, hospitais, sequestro, maternidade, risco.

Abstract

The use of the electronic bracelet with RFID (radio frequency identify) in newborns in hospitals and clinics; methods to avoid the newborns kidnapping; how people act when they intend to commit the crime of kidnapping, using informations, bags and other resources for the tort; the lawsuits that health institutions are exposure; and the subject on television network prime time.

Em alguns hospitais do Brasil, o uso das pulseiras eletrônicas, que podem impedir ou inibir os sequestros de recém-nascidos ou crianças, pode se tornar uma realidade em pouco tempo, dependendo apenas de assinaturas de prefeitos.

Keyword

Newborn, electronic bracelet, hospital, kidnapping, maternity, risk.

I. INTRODUÇÃO

Não é de hoje que os sequestros de crianças ou recém-nascidos ocorrem em hospitais, maternidades e clínicas pelo Brasil afora e, podemos até falar que isso não é uma atitude somente brasileira. Geralmente quando ocorre um sequestro de recém-nascido, o assunto torna-se manchete para jornais que são exibidos em horários nobres e causa um tremendo desconforto para as pessoas que, naquele ambiente de trabalho, exercem atividades honestas, pois a insegurança paira sobre as cabeças de todas as pessoas. Em primeiro lugar, haverá, por parte da alta gestão do hospital, uma cobrança maciça sobre os colaboradores exigindo informações a respeito de onde pode ter ocorrido a falha para que pudesse ser possível um sequestro de uma criança ou recém-nascido. Nesse processo, a imagem da instituição fica muito comprometida, sem falar no corpo de segurança do local que tem que zelar pela segurança de todos os pacientes e colaboradores que trabalham na instituição.

2. OBJETIVO

Descrever o uso das pulseiras ou tornozeleiras eletrônicas com dispositivo RFID nos hospitais e clínicas que recebem crianças e recém-nascidos de forma a evitar sequestros dentro das instituições de saúde.

3. DESENVOLVIMENTO

Em alguns hospitais do Brasil, o uso das pulseiras eletrônicas, que podem impedir ou inibir os sequestros de recém-nascidos ou crianças, pode se tornar uma realidade em pouco tempo, dependendo apenas de assinaturas de prefeitos.

Em outros países como França, Inglaterra, Austrália entre outros, o uso de um sistema de RFID (Identificação de Radio Frequência), que visa evitar que esses casos ocorram, está sendo exigido por lei. Tal sistema visa, também, evitar a troca de bebês nas maternidades, uma vez que o sistema vai identificar a mãe e o bebê através de uma numeração ou através do RFID.

Hoje em dia nas maternidades brasileiras, é usada uma pulseira de plástico que associa as mães aos bebês, simplesmente colocando os nomes da mãe em ambas as pulseiras. Mas muitas vezes o que ocorre é que quando recebem alta, estas pulseiras são retiradas dos pulsos tanto da mãe quanto do recém-nascido, antes da saída efetiva da instituição de saúde. É preciso entender que o uso das pulseiras visa preservar a segurança e a integridade de ambos, tanto do bebê quanto a mãe, já que, caso o sequestro se concretize podem ocorrer traumas bastante danosos para as mães e parentes próximos.

Algumas instituições entendem que o sistema de CFTV (circuito fechado de TV), já seria o suficiente para evitar o sequestro, não havendo, assim, a necessidade do uso das pulseiras eletrônicas. Segundo essas, a simples presença da segurança e do sistema de CFTV já seriam suficientes mitigar o risco de sequestros ou de outros atos danosos. É verdade que o sistema de CFTV é muito efetivo em inibir o risco, mas não o evita.

É preciso entender que os sensores somente não produzem resultados satisfatórios, há a necessidade de implementar procedimentos que complementem o processo, o que exige um colaborador para fiscalizá-los e monitorá-los.

Para a implantação do sistema de braceletes RFID, é preciso além de investir nos braceletes eletrônicos RFID em si, investir nas antenas, que são as unidades receptoras do sinal de RF (rádio frequência), as quais devem ser posicionadas estrategicamente nas portas ou saídas onde, obrigatoriamente, as crianças devem sair, bem como nas demais portas de acesso às instituições de saúde, para evitar saídas com as crianças.

Conforme observado nos históricos de sequestros de bebês e crianças, esses contam, geralmente, com a participação direta de colaboradores da instituição ou com a conivência para que a informação privilegiada fique exposta para quem deseje cometer a ação criminosa.

Na comunidade materno-hospitalar, há pessoas desempenhando diversos tipos de serviços como: pessoal de limpeza, administrativo, prestadores de serviços, enfermeiros, médicos, entre outras.

Os funcionários da área administrativa utilizam roupas ou uniformes de cores diferentes do branco, enquanto que a cor branca é comumente utilizada no uniforme usado por pessoas ligadas ao trato e cuidado com os pacientes.

Figura1 - Recém-nascido com tornozeleira RFID

Os médicos, geralmente, utilizam uniforme branco, bem como as enfermeiras e auxiliares de enfermagem. Os vetores que mais cometem os delitos, são mulheres, se passando por enfermeiras, técnicos de enfermagem ou auxiliares de enfermagem.

A alegação que os criminosos, geralmente, utilizam é que vão pegar a criança para fazer um exame, pesar, dar banho ou qualquer outra desculpa que possa deixar a mãe da criança entendendo que seu recém-nascido está sendo antendido da maneira que necessita, porém, o que ocorre, é justamente o contrário. Essas pessoas colocam as crianças dentro de sacolas ou bolsas grandes para não causarem suspeita durante o percurso no interior dos hospitais ou clínicas.

Existem hospitais particulares que possuem alguns processos de controle e vigilância para as crianças recém-nascidas, como a existência de elevador privativo para levá-las ao berçário ou para realizar algum procedimento necessário e a escolta de vigilante para levar os pacientes para todos os lugare, ou seja, a criança dispõe de um guarda-costas. Nesses casos, as pulseiras podem ser consideradas desnecessárias, em razão de o segurança estar escoltando todos os passos do bebê do lado de fora do berçário ou do quarto onde a mãe está instalada.

Os processos de revistas e o uso das pulseiras são imprescindíveis, uma vez que, nos hospitais e maternidades, pessoas trajadas de branco entram sem serem questionadas.

Existem algumas empresas certificadoras, que visam, entre as necessidades básicas, o controle efetivo do acesso nos hospitais, de forma a restringir a entrada de pessoas, verificando quem pode e quem realmente precisa adentrar nos hospitais. A vigilância

Figura 2 - Detalhe da Tornozeleira

sanitária também vem fazendo recomendações sobre a restrição de acesso nas alas de maternidade e berçários dos hospitais, de modo a evitar dissabores ao ter ver imagem da instituição nas televisões no horário nobre falando sobre de sequestros e sumiços de bebês. Tal exposição é bastante ruim para a imagem de um hospital, sem falar dos processos judiciais que podem decorrer desses atos criminosos feitos nas instituições ou da pressão do ministério público pela exigência de informações sobre uma situação que fugiu do controle da instituição de saúde.

É comum não haver revistas em sacolas nos hospitais, pois algumas instituições zelam pela integridade do cliente que é considerado, muitas vezes, o único que tem razão. Ocorre, porém, que é nestas sacolas ou bolsas que circulam livremente pelos hospitais e instituições de saúde, que são transportados além dos bebês, roupas de cama, toalhas e outros produtos de uso dos hospitais, que são considerados souvenirs para as pessoas que cometem o ato ilícito.

4. CONCLUSÃO

Basta um jaleco branco para se ter passe livre em muitos hospitais do Brasil. Com esse jaleco e mais uma sacola, o sequestro de um recém-nascido pode ser concretizado se não houver algum tipo de controle como e, principalmente, as pulseiras ou outra forma de controle que tenha um monitoramento efetivo a fim de evitar os crimes. Há, contudo, a necessidade de testes nas pulseiras para verificar se seu uso é eficaz a fim de justificar o investimento no sistema RFID.

REFERÊNCIAS

Site G1: França adota pulseiras eletrônicas para impedir sequestros de bebês

Evaldo Tavares Barbieri

Gestor de Segurança e Transporte do Hospital Santo Amaro no Guarujá/SP; Consultor de Segurança Portuária; Aluno do MBA – Gestão de Riscos e Segurança Empresarial – FAPI/FESP – Faculdade de Administração de São Paulo – Brasiliano & Associados em São Paulo/SP; Oficial de Segurança Portuário - ISPS CODE (International Ship and Port Facility Security CODE). Formado em Administração e em Química. Oficial da Reserva do Exército. Atua na área de segurança corporativa a mais de 20 anos.

sumário

A Divisão de Auditoria de Riscos da Brasiliano & Associados auxilia sua empresa a mitigar e controlar os riscos nos processos, ganhando flexibilidade e competitividade.

b&a
BRASILIANO & ASSOCIADOS

info@brasiliano.com.br
www.brasiliano.com.br
11 5531 6171

Fuga Involuntária da Informação

Cláudio dos Santos Moretti

Na segurança empresarial há um jargão conhecido que diz que "deve-se medir a força de uma corrente pelo seu elo mais fraco". A dita corrente é formada por diversos elos que podem ser representados por: comunicação, sistema de alarmes, barreiras físicas, controle de acesso, recursos humanos, etc.

Desta corrente, normalmente, somos unânimes em dizer que as pessoas são o elo mais fraco, porque qualquer ser humano está sujeito a falhar.

Na fuga involuntária da informação ocorre o mesmo. Por mais que a empresa possua equipamentos e *softwares*, se não houver um treinamento adequado dos colaboradores, as informações vão sair da maneira mais simples possível, mesmo que não haja nenhuma má intenção entre esses colaboradores.

Então não estamos falando em espionagem, hacker ou sabotagem, estamos falando em fuga involuntária, aquela que ocorre sem que o colaborador tenha se dado conta de que pode estar prejudicando a empresa passando a informação adiante.

Sempre que tomamos conhecimento de alguma notícia que não era para ser divulgada, nos perguntamos como alguém teria conseguido aquela informação. É claro que as informações podem ser conseguidas de diversos modos, mas existe um – bem simples - que é PERGUNTANDO. Esse método apesar de parecer estranho, é o mais comum, usado por especialistas em engenharia social.

O conceito de engenharia social abarca o tocante de buscar uma maneira para angariar informações confidenciais sobre determinada pessoa, equipamento, campanha ou empresa, sem o uso da força, apenas com inteligência, técnica, perspicácia e persuasão.

Veja alguns exemplos de pessoas que conseguiram um considerável número de informações apenas usando técnicas da engenharia social.

Um dos precursores do conceito da engenharia social é o ex-fraudador americano, Frank W. Abgnale. Ele ficou tão famoso com seus golpes que chegaram a fazer um filme sobre suas trapaças. O filme dirigido por, nada menos que, Steven Spilberg, foi protagonizado pelos atores não menos famosos, Leonardo DiCaprio e Tom Hanks, em 2002, com o título sugestivo de "Prenda-me se for capaz". Para o ex-fraudador, engenharia social é "a arte e a ciência de induzir pessoas a agirem de acordo com seus desejos".

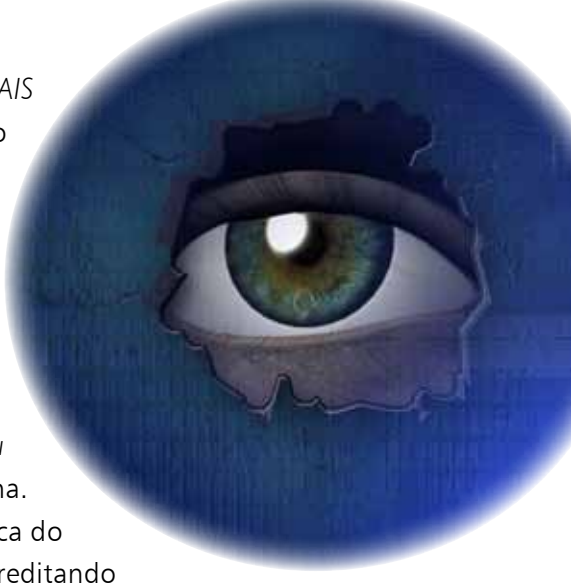
Em 2004, numa entrevista à *Módulo Security Magazine*, onde foi perguntado sobre a melhor maneira de combater a engenharia social, Abgnale respondeu:

"As pessoas precisam estar cientes dos perigos de se passar muitas informações. Vivo sob uma regra muito simples: se não solicitei o recebimento de um telefonema, um e-mail ou uma carta, não vou passar qualquer informação sobre mim, meus clientes, minha companhia, minha família, meus contatos etc."

Outro ícone da engenharia social é Kevin Mitnick, que, após ser preso, lançou o livro *"A arte de enganar"* onde mostra a importância da engenharia social. No livro ele diz que "cerca de 80% das informações são obtidas através de métodos da engenharia social e apenas 20% usando o computador".

No Brasil, nós também temos uma pessoa que conseguiu notoriedade com seus golpes de engenharia social. Trata-se de Marcelo Nascimento da Rocha, que chegou a dar entrevistas ao apresentador Amaury Júnior em programa televisivo onde se passou por vice-presidente da Gol, empresa aérea brasileira, e emprestou até um jatinho para o Amaury, sem nunca ter tido nenhum.

Sua extensa lista de mentiras e trapaças, das mais diversas possíveis, demonstradas no livro *"VIP's – HISTÓRIAS REAIS DE UM MENTIROSO"*, escrito por Mariana Caltabiano, mostra o quanto as pessoas podem ser enganadas.



"As pessoas acabam caindo nas minhas mentiras porque eu mexo com a ambição delas. Sou quem eles quiserem que eu seja", afirmou Marcelo Rocha. Nessa frase, ele nos dá uma dica do porquê as pessoas acabam acreditando no engenheiro social.

Mesmo com toda a sensação de insegurança vivida atualmente pela sociedade, muitas pessoas ainda são ingênuas, confiam em desconhecidos e, pior, não sabem avaliar o valor das informações a eles confiadas, normalmente porque não acham que esses dados são importantes. O engenheiro social é um oportunista com um grande talento para observar as pessoas, avaliando-as para suas investidas. Ele também não deixa de possuir um espírito empreendedor, arriscando-se para conseguir o que quer. Além disso, usa os sentimentos mais comuns das pessoas como armas a seu favor, como medo, vaidade, ambição, cobiça, vingança e ira.

Assim, muitas vezes, as pessoas falam mais do que devem por se sentirem injustiçadas, insatisfeitas com a empresa, etc. Logicamente existem outros motivos, como por exemplo:

- **Vontade de ser útil** – O ser humano, normalmente, procura agir com cortesia, ajudando outras pessoas quando necessário.
- **Busca por novas amizades** – As pessoas sentem-se bem quando elogiadas e ficam mais vulneráveis e abertas a dar informações.

- **Propagação de responsabilidade** – Trata-se da situação na qual o indivíduo considera que ele não é o único responsável por um conjunto de atividades.
- **Persuasão** – A capacidade de persuadir pessoas é quase uma arte, através da qual se busca obter respostas específicas. É possível porque as pessoas têm características comportamentais que as tornam vulneráveis à manipulação.
- **Coleta de informações** – O engenheiro social busca as mais diversas informações dos usuários como número de CPF, data de nascimento, nomes dos pais, informações sobre os filhos, rotina e manuais da empresa. Essas informações o ajudarão no estabelecimento de uma relação com alguém da empresa visada e podem ser obtidas através de ligações telefônicas, em documentos deixados ao acaso, cadastros na Internet, salas de bate-papo ou no Orkut.
- **Desenvolvimento de relacionamento** – O engenheiro social explora a natureza humana de confiar nas pessoas até que se prove o contrário, inclusive porque essa é uma das características do povo brasileiro.
- **Exploração de um relacionamento** – O engenheiro social procura obter informações da vítima ou empresa como, por exemplo, senha, agenda de compromissos, dados de conta bancária ou cartão de crédito a serem usados no ataque. Normalmente essas informações partem de pequenas informações até que juntas formam uma espécie de mosaico, desvendando ou dando condições para que se alcance as informações consideradas reservadas ou sigilosa.
- **Execução do ataque** – O engenheiro social realiza o ataque, fazendo uso de todas as informações e recursos obtidos e conclui seu ataque não apenas tendo acesso às informações, mas fazendo uso indevido delas, podendo causar enormes prejuízos às pessoas ou à empresa.

Vale observar que o sucesso da engenharia social depende da compreensão do comportamento do ser humano, além da habilidade de persuadir outros a disponibilizar informações ou realizar ações desejadas pelo engenheiro social.

Perceba ainda que o medo de perder o emprego ou vontade de ascender na empresa pode resultar na entrega de informação de natureza proprietária. Dessa maneira, observa-se que a engenharia social possui uma seqüência de passos na qual um ataque pode ocorrer:

Quando lemos sobre práticas de engenheiros sociais, parece-nos pouco provável que aconteçam, mas, na realidade, elas acontecem com mais facilidade do que se imagina. Basta ver o que ocorreu em uma auditoria realizada no início de 2005, na Internal Revenue Service (IRS), a Receita Federal americana.

Embora as pessoas que trabalham na instituição sejam treinadas e saibam da importância das informações a que têm acesso, durante uma simulação da auditoria, das cem pessoas envolvidas, incluindo gerentes, 35 delas passaram as informações solicitadas aos pseudo-engenheiros sociais, informando suas chaves e senhas.

Se com essas pessoas treinadas isso aconteceu, imagine o que não aconteceria em sua empresa. Só a conscientização e o treinamento constante podem evitar o êxito de um engenheiro social.

Um estudo recente divulgado pelo instituto norte-americano Gartner prevê que a engenharia social será a principal ameaça para os sistemas tecnológicos de defesas das grandes corporações e usuários de internet daqui a dez anos.

Todos são vítimas em potencial.

Para demonstrar a força da engenharia social, cito o mais famoso hacker do mundo, Kevin Mitinick, que em determinada parte de seu livro diz: *"Em testes de invasão onde são empregadas técnicas de Engenharia Social o índice de sucesso tem sido de quase 100%"*. E ainda: *"a verdade é que não existe uma tecnologia no mundo que evite o ataque de um Engenheiro Social"*

Outra demonstração da força da engenharia social pode ser medida através das inúmeras extorsões realizadas por marginais, que, mesmo estando presos em outras cidades, conseguiram tirar dinheiro das pessoas através de uma simples ligação telefônica.

Nestes casos eles sempre conseguem as primeiras informações de maneira bem simples, passando-se por funcionários da empresa telefônica ou outra empresa qualquer. Através da confirmação de alguns dados, fazendo perguntas inocentes, eles concluem sua ação, posteriormente, com um ataque fulminante usando as armas que você ou alguém de sua família forneceu-lhe inocentemente.

Daí conclui-se que a informação, em qualquer nível, seja pessoal ou empresarial é de suma importância.

Veja a definição de informação apresentada pela NBR ISO/IEC 17799, que é a norma da ABNT – Associação Brasileira de Normas Técnicas, sobre a segurança da informação:

"A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida".

Então, assim como em nossas casas, nas empresas a melhor solução para diminuir a possibilidade de sermos vítimas dos engenheiros sociais é a conscientização do valor da informação, seja ela qual for, o que só é possível através de treinamentos e campanhas esclarecedoras.

Deixar as informações à própria sorte é uma falha na gestão de segurança da empresa, e pode trazer problemas sérios tanto de ordem pessoal, financeira ou de imagem e posicionamento.

Ninguém está livre de ser assediado por um engenheiro social. Ninguém! O próprio Kevin Mitnik foi vítima de uma ação de engenharia social por ocasião do lançamento do seu primeiro livro, A arte de enganar.

Agora mesmo pode haver um engenheiro social ligando para sua empresa.

Você está tranquilo?

Cláudio dos Santos Moretti

Formado em Gestão Empresarial e pós-graduado em Gestão de Segurança Empresarial (MBA)e Gestão de Crise Corporativa. Trabalha a 24 anos na Petrobras, na refinaria de Cubatão - RPBC, no setor de segurança orgânica. É professor do curso de Gestão de Segurança Privada da UNIP - Santos e do MBS da Brasiliano.

"Em testes de invasão onde são empregadas técnicas de Engenharia Social o índice de sucesso tem sido de quase 100%"

sumário

Soluções Integradas de Segurança – Salas de Comando e Controle

Leandro Fortes

Resumo

A implementação de Soluções Integradas, tais como Salas de Comando e Controle em órgãos de Segurança Pública e Privada seria de extrema funcionalidade e operacionalização, por prevenirem perdas patrimoniais e pessoais. Porém, quando se contabiliza os investimentos a serem disponibilizados no contexto de qualquer situação, ficamos diante de grandes dificuldades. Com a divulgação de bons resultados de estruturas já existentes, esse quadro, contudo, pode começar a mudar.

Palavras-chave

Sistemas de Segurança Integrada, Salas de Comando e Controle, Sala de Situação e Meios, Segurança Privada, Segurança Pública.

Mitigar e gerenciar riscos, quando se tem a disponibilidade de amplificar o nível de segurança de qualquer empresa ou instituição com a implantação de sistemas de segurança integrada/salas de situação e meios.

Abstract

The implementation of integrated solutions, such as Command and Control Rooms in organizations of Private and Public Security would be enought functionally and operationally, by preventing property and personal losses. But by accounting the available investments in any situation context, we find great challenges. But, with the strong results release of existing structures, this framework can start changing.

Keyword

Integrated Security Systems, Command and Control Room, Situation Room and Media, Private Security, Public Safety.

I. INTRODUÇÃO

Mitigar e gerenciar riscos, quando se tem a disponibilidade de amplificar o nível de segurança de qualquer empresa ou instituição com a implantação de sistemas de segurança integrada / salas de situação e meios.

Nos últimos 20 anos, o cenário da segurança brasileira tem se modificado gradativamente, a medida em que cresce a demanda por efetivos da segurança pública e privada.

O aumento da criminalidade, a crescente organização do tráfico de drogas, as crises da violência urbana geradas nas principais capitais brasileiras, exigem cada vez mais de nossas autoridades medidas emergênciais e contingenciais para a contenção imediata de crises e prospecção de cenários desejáveis para os próximos 10 anos, inclusive no gerenciamento de grandes eventos esportivos que o Brasil sediará.

2. OBJETIVO

Descrever o uso dos como melhor forma de mitigação de riscos e também como plano de continuidade de negócios.

3. DESENVOLVIMENTO

Eu trabalho na área de segurança privada há pouco tempo. Desde 1996. Digo pouco tempo, porque apesar de ser uma área relativamente nova em nosso País, conheço centenas de profissionais de segurança que estão no mesmo segmento há muito mais tempo, praticamente uma vida inteira. Portanto, sou apenas um "adolescente" na área.

Nesse curto período de atuação no segmento, no entanto, tento acompanhar a evolução tecnológica empregada em sistemas de monitoramento e controle, em desenvolvimento de normas e processos, bem como no treinamento e desenvolvimento de recursos humanos especializados.

Se observarmos as grandes e médias empresas neste período, percebemos que suas respectivas áreas de segurança, têm se aperfeiçoado em relação aos seus procedimentos, seguindo à risca a padronização corporativa e também ao que se refere às determinações e padronizações internacionais.

Já em relação aos nossos recursos humanos, as exigências legais não nos apresentaram mudanças significativas, pois a formação de profissionais de base, ainda exige apenas até o quarto ano do ensino fundamental. Todavia, associações específicas criaram certificações de especialistas e universidades passaram a oferecer cursos de formação superior, com foco em Gestão de Segurança. Há, atualmente, também cursos de pós-graduação, onde o foco do profissional de segurança pode alçar voos maiores e mais bem-sucedidos. Mas, a base ainda é, realmente, deficitária.

Em termos de tecnologia de segurança, assim como em todos os demais segmentos, podemos nos surpreender um pouco mais. Em uma época em que alta

tecnologia, como I-pods e Internet aceleram a globalização mundial, nossa área também ganha muita agilidade na prevenção patrimonial e consequente mitigação e gerenciamento de riscos empresariais.

Tive a oportunidade de iniciar minhas atividades em 1996, como operador de um Centro de Informações e Monitoramento, dentro de um departamento de Segurança - já muito bem segmentado para a época - de uma grande instituição financeira. Naquela época, monitorávamos alarmes de agências bancárias, através de sistemas totalmente analógicos, onde a maioria nos "alertava" de situações de perigo real apenas com um breve sinal sonoro. Alguns, conseguiam ainda disponibilizar sinais também visuais, nas lendárias telas de computadores 386, muitos ainda em sistemas DOS. Era uma forma, hoje, considerada "primitiva", mas com uma visão de longo alcance, já que as atividades não se limitavam apenas ao monitoramento, mas também à integração das diversas informações pertinentes às equipes que, também, atuavam de forma preventiva e ostensiva como: pronta-resposta, transporte de valores, tratamento e atendimento de ocorrências em geral, vistorias técnicas, planos de segurança, projetos especiais, inteligência e contra inteligência e inspetorias e rondas táticas diárias no intuito de mitigação de ações delituosas.

O que quero dizer, afinal, é que a maior limitação até então, era a já comentada tecnologia. Afinal, naquela década, já se operacionalizavam em países como Israel e Estados Unidos tecnologias suficientes aliadas à inteligência estratégica, já muito estudada por essas nações, na concretização e aplicação das chamadas salas de controle e comando.

O objetivo dos profissionais naquela época, ainda estava crescendo em outro foco, o de formação tática de grupos especiais no Brasil, pois estávamos em estágios menos turbulentos, mas não menos preparados, e sim, com massa crítica e tática atuante e em constante desenvolvimento. Além disso, a crença de empresários, industriários e executivos em geral para investimentos tão significativos ainda era muito menos expressiva.

Os anos se passaram e alguns cenários, anteriormente previstos, se concretizaram. Com a formatação daquela equipe divisionária de segurança, já na década de 90, a tão sonhada tecnologia hoje nos proporciona a aplicação de um sistema de segurança integrado muito capaz, se bem administrado e monitorado junto à alta administração de qualquer organização.

Aquele Centro de Informações citado há pouco, hoje é conhecido por Sala de Situação e Meios e, com o conceito de Salas de Comando e Controle, se consolidou como uma referência na América Latina em assegurar a continuidade de negócios, prevenir riscos em todas as esferas corporativas e ainda fomentar a instituição em relação a todas as informações divulgadas nas mais diversas mídias de mercado, em *real time*.

Com imagens de unidades em todo o Brasil sendo monitoradas *on line*, tendo monitoramento exclusivo de tráfego aéreo e terrestre de VIPs, com controles de acesso integrados e controlados o tempo todo em sedes administrativas, de equipamentos de alarme via rede e GPRS, de equipes de pronta-resposta mapeadas e com atendimento padronizado, de equipe de prevenção e combate à incêndios com controle imediato de centros vitais da instituição, tais como CPD, entre outros: estou falando especificamente da primeira Sala de Situação e Meios – 24 horas (Sala de Comando e Controle), implementada à serviço de uma grande instituição e com investimentos agressivos em nosso País.

Em funcionamento desde 2006, e com pequenas inserções tecnológicas a favor da atualização constante, a Sala de Situação e Meios proporciona resultados muito expressivos no Gerenciamento de Riscos Corporativos e na continuidade dos negócios, fazendo, inclusive, a interface com sedes locais da Segurança da Instituição em países como Espanha e México.

O investimento no emprego de tecnologia de ponta, o foco no treinamento de operadores, supervisores e coordenadores e a correta distribuição e aplicação de normas, faz desta sala, o coração de todo o sistema integrado de segurança da dita instituição. E isso, com certeza, pode ser levado à todos os níveis de Segurança Corporativa com ênfase em Gerenciamento de Crises e Planos de Contingência, abrindo novas expectativas no contexto da Segurança Brasileira.

CONCLUSÃO

As salas de Comando e Controle a partir desta década podem se tornar modelos de referência para Segurança Privada e Pública em nosso país. Sua implementação deve atender às necessidades e dificuldades que circundam em nosso cenário de criminalidade, mas, não serão, a solução de todos os problemas, sendo somente o começo de uma nova tendência tecnológica aliada a processos e recursos humanos

Referências – Experiência do autor em 14 anos de trabalhos desenvolvidos em Segurança Bancária.

http://www.cceinteriors.com/

Leandro Fortes

Graduado em Política e Estratégia, Comunicação Social e Segurança de Dignatários e Proteção Executiva na Cidade de Davie, Miami - EUA . Possui MBA em Gestão de Riscos e Segurança Empresarial e é pós-graduado em Política e Estratégia pela USP. Trabalha há mais de 14 anos na área de Segurança Patrimonial sendo atualmente Gestor de Segurança Patrimonial da Boehringer Ingelheim do Brasil.

sumário

Business Continuity Management – BCM
Gestão da Continuidade de Negócios - GCN

Sua empresa está preparada para um evento de DESCONTINUIDADE??

A operacionalização de um GCN é um processo estruturado para:

- Melhorar proativamente a resiliência da empresa contra possíveis descontinuidade;
- Restabelecer a capacidade de fornecimento de produtos e serviços;
- Proteger marca e reputação

O GCN possui normatizações e regulações, com base nas melhores práticas internacionais.

No Brasil, através da ABNT, tem as normas ABNT NBR 15999 - 1 e 2, que descrevem o processo, estrutura e conteúdo de um sistema de Gestão de Continuidade de Negócio.
A empresa deve possuir resilência. A Brasiliano & Associados ajuda a sua empresa a manter o fôlego, mesmo em momentos críticos.

Possuímos uma equipe multidisciplinar, com capacidade e visão de vários segmentos empresariais. Prestamos os seguintes serviços:

- Mapeamento dos Processos Críticos, através de critérios personalizados para o tipo de negócio – BIA – Business Impact Analysis
- Estabelecimento de Critérios de Tempo de Resposta e Tempo de Recuperação
- Elaboração de Estratégias de Continuidade
- Elaboração de Procedimentos Operacionais
- Estrutura Organizacional da Continuidade e da Crise
- Programas de Comunicação de Crise
- Programas de Sensibilização
- Testes Operacionais e de Conformidade

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

b&a
BRASILIANO&ASSOCIADOS

ACONTECE

na Brasiliano

Mariana Fernandez

PALESTRA FRAUD RISK ASSESSMENT

Na cidade de São Paulo, no Hotel Campobelo Plaza, aconteceu no dia 21 de outubro uma palestra especializada no tema Fraud Risk Assessment.

Através das palavras de Antonio Celso Ribeiro Brasiliano e Nilton dos Santos, experts no assunto, a platéia de auditores, Gerentes de Compliance, Consultores de Gestão de Riscos, Coordenadores de Segurança e outros tantos que atuam em operações contra fraude, atualizaram-se sobre as mais novas técnicas, métodos e práticas da área.

CURSO DE AUDITORIA EM CHAPECÓ

Para promover a atualização de conhecimentos sobre modernas técnicas e procedimentos aplicáveis no desenvolvimento dos trabalhos de auditoria, baseada em riscos, para aperfeiçoamento da qualidade e otimização dos resultados alcançados, o curso mais completo de Auditoria baseada em Riscos do mercado aconteceu no mês de outubro em terras catarinenses.

Os colaboradores da empresa Sescoop de Chapecó, nos dias 13 e 14 de outubro, cumprimiram as 16 horas/aula do curso estando aptos a atuar com responsabilidade e eficiência em processos de auditoria baseada em riscos.

Parabéns aos alunos!

BRASILIANO NO IQPC

Após o sucesso das edições anteriores, o IQPC realizou nos últimos dias 21, 22 e 23 de setembro a 4ª edição da conferência Gerenciamento de Riscos Corporativos!

No segundo dia do megaevento, aconteceu a palestra de Antonio Brasiliano - autor do método homônimo que vem sendo aplicado em grandes empresas por ser flexível a mudanças de conceitos de risco - Metodologia E Processos De Gestão Pró-Ativa De Riscos E Diretrizes Da ISO 31000. Em seu discurso, o especialista em Gestão de Riscos discorreu sobre os temas:

- *Análise conjuntural: benefícios e aplicações da gestão de riscos*
- *Interface entre planejamento estratégico e gestão de riscos*
- *Estrutura da ISO 31000 – Processo de Gestão de Riscos*
- *Ferramentas e metodologias a serem empregadas*

A explanação de Brasiliano agradou muito aos presentes que ovacionaram o palestrante ao final da palestra.

CONGRESSO DE CRIMES ELETRÔNICOS

Junto com todos os recursos e facilidades do mundo virtual, surgem mais crimes também. Então, como ficamos? O que devemos fazer para aproveitar os benefícios do online com segurança? Como podemos nos defender dos criminosos virtuais?

As respostas para essas perguntas foram discutidas no II Congresso de Crimes Eletrônicos e Formas de Proteção (Internet e meios de comunicação: e-mail, redes de relacionamento, etc) ocorrido na FECOMERCIO.

A Brasiliano & Associados, que dá assessoria a empresas na área de segurança e perícia eletrônica além de ministrar cursos sobre os assuntos, não poderia ficar de fora do acontecimento e participou como expositora durante os dois dias, 27 e 28 de setembro.

Dentre os visitantes estavam profissionais de Direito, Tecnologia da Informação, Compliance, Investigadores, e afins.

sumário

Mitigando Riscos de TI para Acesso Lógico a sistemas e dados

André Pitkowski

Assim, para começar este artigo de supetão, trago a afirmação: o acesso não autorizado pode causar efeitos devastadores. Empresas e pessoas podem se tornar vítimas de atividades criminosas, tais como: roubo de identidade, fraude financeira, roubo de dados do cartão de crédito (acho que uma vez ao mês temos notícia de um vazamento), imposto de renda (incluindo as noticias relativas às eleições de 2010) e os ataques a redes e sistemas (por exemplo, a negação de serviço numa aplicação pagamentos). Tudo isso pode ser financeiramente prejudicial para os negócios *on line*. Todos esses efeitos nocivos têm sido objeto de várias reportagens em todas as mídias ao longo do tempo.

Criminosos, discriminadamente aqueles com experiência em TI, tornaram-se especialistas em reconhecer deficiências no acesso lógico a sistemas e redes e aprenderam ao longo do tempo sobre as ferramentas necessárias para explorar com sucesso aqueles sistemas fracos. Foi publicado recentemente que cerca de 65% dos sistemas governamentais do Brasil possuem algum tipo de deficiência em segurança da Informação.

Dizem os especialistas, que os criminosos estão se concentrando cada vez mais em crimes baseados em TI ao invés de crimes de rua tradicionais. E as estatísticas do *Computer Emergency Readiness Team* (CERT) juntamente com os analistas de segurança da indústria mostram que

cerca de 80% de todas as atividades maliciosas ainda são provenientes de funcionários atualmente empregados ou ex-funcionários que, por deficiência da segurança da informação, ainda portam acessos que deveriam ter sido cortados no momento da demissão. (1)

Assim, mais do que nunca, uma das principais preocupações de qualquer auditoria de TI, da Segurança da Informação, bem como da gestão da empresa, é relativa ao acesso lógico a sistemas e dados. O crescimento exponencial da TI e da Internet em particular, tem causado aumento considerável dos riscos associados ao acesso não autorizado a sistemas e dados.

Tal assunto fez com que o *American Institute of Certified Public Accountants* (AICPA) tenha apontado esse risco nas *Top Technology Initiativess* todos os anos desde 2005, sendo que na lista de 2010 ele está em primeiro lugar.(2)

Claro que existe algum nível de risco de auditoria e risco do negócio em praticamente todas as empresas e, também, a auditoria enxerga uma variedade de vulnerabilidades relacionadas a TI, mas existe especial atenção dos auditores para com controles de acesso.

No início deste ano, foram identificadas cinco áreas do *IT General Controls* (ITGC) que devem ser examinadas em cada auditoria financeira. (3) O item acesso lógico foi uma das cinco. Este artigo acrescenta ainda o acesso à informação, num sentido mais amplo das auditorias, o acesso lógico.

Para se mitigar os riscos associados com controles de acesso, é necessário primeiro identificar quais são estes riscos e então avaliar seu nível. A área de Segurança da Informação, juntamente com a gestão de infraestrutura deve, então, estabelecer políticas e procedimentos de concessão de acesso para usuários autorizados, enquanto, simultaneamente, deve estabelecer os procedimentos para proteger a informação contra o acesso não autorizado.

Esta área de interesse é geralmente considerada um subconjunto da gestão de identidade. Um método muito utilizado para tratar esses riscos é através do perímetro de acesso autorizado, cujo processo garante a concessão de acesso a apenas ao mínimo necessário (*need-to-know*, incluindo aí os direitos de administrador) e que engloba o processo de rescisão contratual com os empregados.

Mitigando os Riscos de Acessos Lógicos

No perímetro, as boas práticas incluem autorização e autenticação dos usuários baseadas em políticas e procedimentos de segurança da Informação.

Controles para autorização de acesso são aqueles que tem por objetivo garantir que a pessoa que solicitar o acesso está autorizada para tal. Esse controle é associado frequentemente com suas credenciais (cargo e funções) e procedimentos de *login*, por exemplo, o de exigir um ID e uma senha. Do outro lado da moeda, o mundo *hacker* desenvolveu sofisticadas ferramentas que podem descobrir facilmente sistemas cujo acesso é baseado em senhas (nomes (próprios, carros, locais), datas, e todas as palavras encontradas num dicionário, etc.) Portanto, ao longo dos anos, as melhores práticas têm sido atualizadas para incluir senhas consideradas "fortes", somado à sugestão de atualizações frequentes de senhas mais

controles acesso multifatorial (*tokens*, biometria), conforme o caso. Quanto mais sensível é a informação, maior é o risco, maior é a necessidade de acesso mais sofisticados e seguros e, maior é a necessidade de camadas adicionais de controles de acesso. O mais primário dos elementos da camada de segurança inclui uma senha, e ela é considerada mais forte quanto mais atender as regras abaixo:

- Ter no mínimo oito caracteres.
- Incluir, no mínimo, um caractere especial (!@#$%...)
- Incluir, no mínimo, um algarismo.
- Misturar caracteres em caixa alta (tecla shift)
- Usar frases incoerentes (não o endereço, verso de oração ou estrofe de música por exemplo).

O objetivo desses elementos é a criar dificuldades para as ferramentas *hacker* que tentam adivinhar as senhas comparando-as com palavras em dicionários. As senhas fracas e PINs (senhas baseadas em apenas algarismos) são a principal causa de violações de segurança, segundo a empresa de consultoria em TI da Frost & Sullivan. (4)

Nomes de usuário e senhas/PINs são geralmente estáticos ou compartilhados entre várias contas de usuários, tornando-se presas relativamente fáceis para *hackers* e *crackers*. A tecnologia de segurança, juntamente com as instituições financeiras responderam com PINs temporários associados a outras ferramentas e procedimentos de segurança contra acesso não autorizado.

Os controles de autenticação tem um objetivo diferente. Eles tentam assegurar que as pessoas que acessem um sistema são quem elas dizem que são. Quando os controles existentes não são suficientes para os riscos que a informação corre, os riscos de violação tornam-se relativamente elevados e os controles de acesso que são compostos de apenas uma autorização de controle com uma camada de segurança tipo ID e senha, necessitam de uma camada adicional como por exemplo a biometria.

Camadas de segurança para controle de acesso:

1ª camada: ID/senha: é o que você sabe.

2ª camada: *Token*: é o que você tem.

3ª camada: Biometria: é o que você é.

A maioria dos gerentes de TI experientes adicionam camadas de segurança para controle de acesso baseados em dispositivos como *tokens* USB, cartões inteligentes (*smart cards*), PINS temporários e biometria sobre a camada de segurança de acesso ID/senha. Um *token* USB, é um dispositivo de hardware criptográfico (diferente de um simples pen drive) que deve ser conectado ao computador remoto em uma porta USB antes de o acesso ser concedido. Os cartões inteligentes são inseridos em um leitor semelhante à das maquinas de cartão de crédito, e existem em *notebooks* mais recentes, utilizados em combinação com o ID e senha para a concessão de acesso.

PINs temporários são números, normalmente de 4 ou 6 algarismos, enviados de volta a um dispositivo, como uma mensagem de texto para um telefone celular ou *pager,* em situações em que num acesso remoto, os usuários têm um tempo limitado para inserir o PIN junto com seu ID e senha. Quanto maior o risco que a informação corre, como num *login* remoto a dados sensíveis, maior é a necessidade de controles fortes para o procedimento de autenticação.

No entanto, todos estes procedimentos não são suficientes quando se trata de proteger o perímetro. De acordo com CERT em um documento intitulado "*An Introduction to Insider Threat Management*", durante

os últimos 10 a 15 anos, as organizações ao redor do mundo têm gasto bilhões de dólares para construir defesas fortes para proteger seus dados e sistemas contra acesso não autorizado de *hackers*.

Em média, mais de 75% dos orçamentos de TI das empresas de segurança está dirigido para a proteção contra acesso de estranhos, mesmo que o estudo anual do *Computer Security Instituto / FBI Computer Crime and Security* continuem a publicar que gente de dentro foram responsáveis por incidentes tanto quanto com gente de fora. A pesquisa da *Information Security Magazine* de 2009 nos mostra que o aumento com os gastos com TI está na área do IAM (*identify and Access Management*), com o maior foco em impedir o acesso não autorizado às informações confidenciais pelos próprios empregados.

Uma vez conectado, mesmo um usuário autorizado deve ser impedido de ter acesso a todos os dados e aplicações da empresa. Os funcionários devem ter acesso apenas às aplicações necessárias para realizar o trabalho para o qual foram contratados. Essa limitação também inclui os direitos de acesso a dados para somente leitura, leitura/gravação ou não ter nenhum tipo de acesso se for o caso (ou seja, é necessário conceber também o tipo de acesso). Por exemplo, uma boa política de segurança seria ter um sistema efetivo de acesso lógico na rede para se fazer *login* no sistema (por exemplo, *Active Directory* aplicado eficazmente no Microsoft SQL Server). Mais ainda, onde os riscos foram classificados como elevados, deveria coexistir outro sistema de credenciais de *login* e acesso concedido para cada aplicação-chave.

Alguns sistemas aplicativos, tais como *Microsoft Dynamics*, oferecem seus próprios controles de acesso como uma camada adicional de segurança sobre o acesso aos dados através das aplicações. Se ambos os sistemas de controle de acesso forem geridos de forma adequada, a capacidade de alguém para quebrar o perímetro pode ser mitigada por controles fortes de acesso no "Back Office" do sistema, isto é, um forte par de controles para se evitar acessos não autorizados. O conhecimento da abordagem de acesso às aplicações é o elemento chave de sucesso na implementação de controles de acesso.

Direitos de acesso de Administrador é uma área crítica que precisa de controles por causa do amplo direito de acesso que o "admin" tem uma vez conectado ao sistema, e devem incluídas como parte da necessidade "need-to-know". Controles adequados de acesso devem incluir a aplicação de melhores práticas para a função de administrador de bases de dados ou sistemas de gerenciamento de banco de dados (SGBD), como DB2, Oracle e SQL Server; devem incluir, mas não serem limitadores, a não utilização do ID/senha padrão (default) de admin, minimizar o número de funcionários com acesso de administrador e criar um pequeno grau de segregação de funções.

O administrador é também um usuário mas o qual não pode acessar seus sistemas e rede com as credenciais de Administrador. Entramos no campo dos "papéis e responsabilidades". Direitos de "Admin" são especialmente importantes para Sistemas Operacionais em que o acesso ao diretório raiz pode ser concedido, dando a alguém "As chaves do reino". Obviamente, esta área é foco de exame detalhado durante a maioria das auditorias de TI de qualquer natureza.

Finalmente, quando os empregados são demitidos ou pedem demissão, devem haver controles efetivos para se cancelar o acesso do funcionário a sistemas e redes.

Em caso de rescisão, o pessoal de gestão de acesso, às vezes, "esquece" *logins* e direitos de acesso formalmente concedidos ao funcionário ativos depois que este deixa de trabalhar na empresa. Todas as empresas precisam de um controle efetivo ou conjunto de controles para garantir que todos os funcionários demitidos percam, imediatamente, todos os seus direitos de acesso. E, neste momento, não falamos em apenas acessos lógicos mas de físicos, às dependências da empresa também.

Uma abordagem eficaz e lógica é a de direcionar os procedimentos de controle de acesso para a área de Recursos Humanos da empresa. Quando um funcionário é contratado ou transferido ou abandona a empresa, os processos de RH devem incluir os requisitos de alterações para os direitos de acesso daquele funcionário.

Quando um novo funcionário é contratado, ele ou ela "precisa saber" que os seus direitos de acesso vão ser avaliados e que devem ser concedidos apenas aos aplicativos e dados necessários para as suas funções e responsabilidades no trabalho. Qualquer aplicativo local ou de rede deve ter os meios para limitar o acesso de forma adequada.

Se um funcionário é transferido ou promovido, seus direitos de acesso podem mudar por causa das funções e responsabilidades envolvidas na transferência. Assim, que o RH executar um procedimento de transferência, deverá executar um procedimento de revisão e de mudança, se necessário, nos direitos de acesso do funcionário para com os sistemas e rede.

Quando um funcionário deixar a empresa por qualquer razão, mas especialmente se for demitido, seus direitos de acesso devem ser encerrados o mais próximo possível do momento da demissão, mas não se deve esperar até a ultima hora do último dia da pessoa no trabalho.

CONCLUSÃO

Um auditor de TI deve considerar os procedimentos previamente divulgados em uma auditoria para garantir que os controles de acesso estão adequadas para mitigar os riscos associados ao acesso, incluindo a limitação do acesso que os legítimos funcionários precisam saber, bem como para mitigar o risco de um acesso não autorizado.

REFERÊNCIAS:

(1) Hirschhorn, Karen; "Hacker Activities," IT Defense Magazine, Dezembro/Janeiro 2007, p. 12-15. Leia também Insider Threat Research em www.cert.org/insider_threat/.

(2) Na pesquisa conduzida pela AICPA Top Technology Initiatives em meados de 2010, a questão: "Which top ten technology considerations are driving your business or practice today?"

Primeira resposta: "Security of data, code and communications/data security and document retention/ security threats." Veja em http://infotech.aicpa.org.

(3) Singleton, Tommie; "The Minimum IT Controls to Assess in a Financial Audit (Part II)," ISACA Journal, vol. 2, 2010

(4) Ayoub, Robert; "An Overview and Competitive Analysis of the One Time Password (OTP) Market" (White Paper), Frost & Sullivan, Junho 2009, http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1016477

Andre Pitkowski

Formado em Engenharia Civil, possui MBA em Governança de TI, Certificado CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in the Risk of Information Systems and Control) pela ISACA. Atua como Consultor Sênior em Governança Corporativa e de TI, Avaliação de Riscos e projetos de Compliance (GRC), e como instrutor em cursos sobre estes assuntos, sendo palestrante convidado no Brasil e internacionalmente.

"Uma abordagem eficaz e lógica é a de direcionar os procedimentos de controle de acesso para a área de Recursos Humanos da empresa"

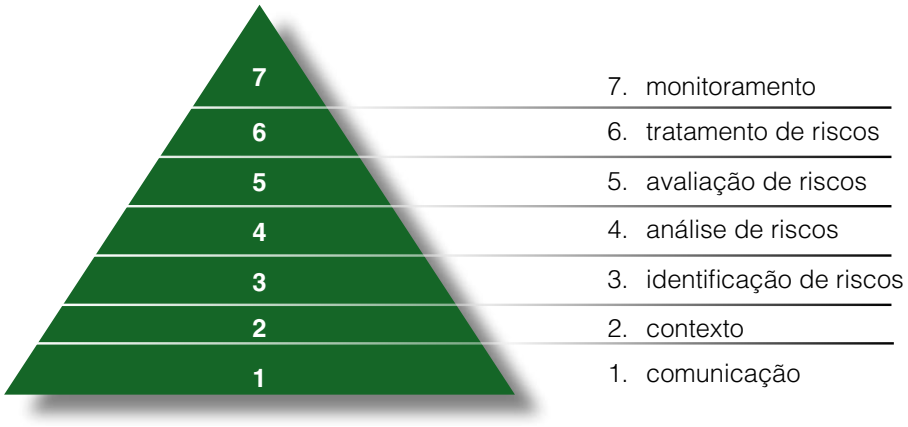
sumário

Serviços de Consultoria
Plano de Gestão de Riscos Corporativos - PGRC

Sua empresa conhece o TAMANHO de seus riscos??

Um PGRC é um processo estruturado para que a empresa possa identificar eventos que expõem os objetivos da organização.

O processo de Gestão de Riscos, hoje é estruturado com base na ISO 31000.



A Brasiliano pode ajudar você a elaborar seu plano de PGRC

Consulte – nos!!!!

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

A Importância da Investigação Empresarial para a Competitividade dos Negócios no Século XXI

Gustavo Vedove

Resumo

Este artigo aborda a importância da investigação empresarial na organização e traz modelo metodológico para análise.

Palavras-chave

Investigação, vantagem competitiva, riscos e interpretação.

Abstract

The article discusses the importance of research in business organization and gives methodological model for analysis.

Keyword

Research, Competitive Advantage, Risk and interpretation.

1. INTRODUÇÃO

Em visão de atuação da atividade de investigação empresarial, o artigo mostra seus resultados através de um modelo prático.

2. OBJETIVO

Descrever o processo de investigação empresarial.

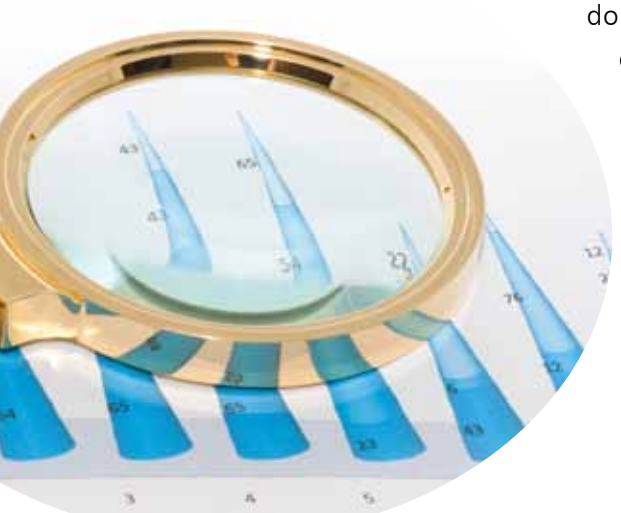
3. DESENVOLVIMENTO

Para superar a concorrência, ser competitiva, a empresa necessita de diferenciais. Neste artigo, abordaremos a importância da investigação empresarial para a competitividade dos negócios.

Considerada como diferencial interno, a investigação empresarial tem como objetivo desvendar casos a fim de evitar perdas acumulativas, as quais impactam diretamente no produto final da empresa. Dado a isso, a atividade passou a ser valorizada nas organizações tendo em vista sua colaboração no processo como um todo ("*EM NÃO PERDER*") e, com isso, ter mais recursos para aumentar sua capacidade competitiva.

Entre as muitas formas de se obter vantagem competitiva, citamos a gestão de riscos corporativos de extrema importância e dentro desta área destacamos a investigação empresarial.

A investigação tem de estar apoiada em métodos científicos - entendendo do que método tem o significado de caminho, meio, - dentre os quais tem-se que decidir qual método é o mais racional, objetivo e ordenado à atividade científica. Podemos pensar em Investigação Empresarial de duas formas, sendo:



- **Investigação Operacional –** Descobrir a agressão e o seu autor. O objetivo é juntar provas suficientes para que a polícia realize seu trabalho.
- **Investigação Estratégica –** Diretamente ligada à Inteligência Competitiva, a investigação estratégica, atualmente, tem como foco saber as mudanças mercadológicas, atividades e fraquezas dos concorrentes.

O objetivo é utilizar as informações colhidas, de forma a contribuir para um posicionamento estratégico da organização.

Vista como um processo bem estruturado dentro da organização, a investigação empresarial é parte integrante da cadeia de valor da empresa.

Em uma empresa, a cadeia de valor é um sistema de atividades interdependentes conectadas por elos. Tais elos surgem quando a maneira como uma atividade é desempenhada afeta o custo ou a eficácia de outras, ou seja, uma atividade otimiza recursos para as outras e investigação empresarial é uma delas.

A investigação empresarial agrega valor para empresa da seguinte forma:

- Mitiga o risco de fraudes em diversas situações como: compras, vendas, transporte, recebimento, expedição, entre outras;
- Recupera ativos roubados;
- Oferece subsídios para resolução de crimes, furtos, fraudes e roubos dentro das empresas;
- Assuntos sigilosos;
- Informações estratégicas.

O resultado de todos os exemplos entre outros que a investigação empresarial

realiza, é a mitigação de perdas na organização e isso deve ser considerado como recursos a mais, dados a outras áreas da empresa que por sua vez vão desenvolver suas atividades com margens maiores de verba e como consequência, as mesmas terão como realizar um trabalho melhor dando chance ao melhor desempenho sobre os concorrentes da empresa.

Além dos cuidados que deve ser tomada com a legislação, a investigação empresarial deve ser realizada de forma estruturada e para isso é preciso ter um processo formalizado.

Processo da Lógica Intuitiva e Entendendo a Agressão.

1 - ENTENDIMENTO DO CONTEXTO

- Entender o problema com base com nos dados obtidos inicialmente e através de históricos.
- Entender o negócio da empresa.
- Avaliar os dados relevantes ao problema identificado.

2 - ENTENDIMENTO DO DELITO

- Como ocorreu?
- Qual o modus operandi?
- Por que ocorreu?
- Entendimento das causas prováveis – levantamento das fragilidades da empresa e do ambiente externo.
- Entendimento das motivações (Ex: financeira, psicológica, material).
- Entendimento da lógica de agressão do agente – Falta de impunidade nas empresas e nas leis.

3 – SÍNTESE E ANÁLISE DAS INFORMAÇÕES

- Consolidar os dados apurados.
- Tirar conclusões com base nas informações obtidas através de diversos métodos (entrevistas, *hot line*, imagens, estudo de banco de dados, investigação social).
- Fazer a síntese da análise das informações é como montar um quebra-cabeça onde os investigadores devem juntar os dados coerentes e correspondentes à ocorrência.

4 – CRIAÇÃO, DESTRUIÇÃO E SELEÇÃO DAS HIPÓTESES

- É pensar quem é o agressor e quando, por que e como este cometeu o delito. Através da criação de cenários/hipóteses em reuniões tipo *brainstorming* com o grupo de análise de investigação.
- O objetivo é eliminar as possibilidades de desvio/fraude não coerentes.

O processo de investigação segue o seguinte *framework:*

CONCLUSÃO

Neste processo aplicamos ferramentas administrativas adaptadas para área de investigação, visando facilitar a identificação das reais causas do delito. O uso das ferramentas visa estabelecer uma linguagem comum entre os gestores da organização, ou seja, demonstra que a área de investigação empresarial fala a linguagem do executivo, tornando-se, assim, parte valorada da cadeia de valor da empresa.

REFERÊNCIAS

Site www.brasiliano.com.br: Artigo: Investigação Empresarial – Joffre Coelho Chagas Junior.

Gustavo Vedove

É Consultor e Auditor de Gestão de Riscos da Brasiliano & Associados há três anos. Graduado em Educação Física, possui MBA em Gestão de Riscos e Segurança Empresarial e MBS - Master in Business Security. Experiência em Projetos GRC no Brasil e em Angola.

sumário

Cultura de Segurança

João Aparecido dos Santos

Quando falamos em projeto de segurança, devemos contemplar três fases importantes, a primeira é a elaboração do projeto, a segunda é a implantação e a terceira e última, embora poucos se atentam, é, na minha modesta opinião, a mais importante:

A utilização dos recursos disponibilizados de forma correta e sua devida manutenção

O tempo passa e o projeto vai se deteriorando. Normalmente, nas duas primeiras fases, existe um planejamento estratégico, tático com acompanhamento, gestão etc..

Após implantado e entregue para o setor operacional, tal projeto tende a não ter uma gestão coerente. Embora a alta gestão imagine que está tudo sob controle, na verdade, não está!

Costumo falar dos *cases* que encontro em minhas visitas. São inúmeros. Confesso que bate uma tristeza quando lembro o quanto foi difícil disponibilizar as ferramentas de segurança existentes, e as vejo renegadas e mal utilizadas.

Senhores gestores, antes de solicitarem mais e mais recursos, precisamos utilizar os recursos existentes de forma correta, valorizando o que já existe.

Estou falando de homens, tecnologias e, principalmente, procedimentos.

Ter uma cultura de obediência a procedimentos não é fácil. Eu sei o quanto é difícil manter um procedimento "vivo", mas isso deve ser uma luta diária, caso contrário, é se iludir e não haverá segurança.

Procedimento é a palavra chave, e o melhor: não tem custo. Uma vez confeccionado e implantado, pode ser usado à vontade, pois já está pago.

É comum chegarmos em uma empresa e, em alguns minutos, encontrarmos situações de desleixo absurdas, como cadeados de portões que nunca foram utilizados, extintores vencidos, sensores de presença obstruídos, portões abertos em áreas de estoques, lâmpadas queimadas, portões de acesso à rua abertos e por ai vai.

Comumente vejo o gestor da unidade com um discurso do tipo: "estou preocupado, aqui está muito vulnerável", "precisamos melhorar a nossa segurança", "estão sumindo produtos", etc...

Meus senhores, eu tenho investido incansavelmente em orientá-los quanto à correta utilização dos recursos disponíveis, me preocupo em disponibilizar mais recursos se os existentes estão sendo subutilizados.

Portanto, a manutenção do sistema tem que estar integrada com o projeto, caso contrário não haverá sucesso. Não basta adquirir mais e mais ferramentas se nem as existentes estão sendo utilizadas corretamente.

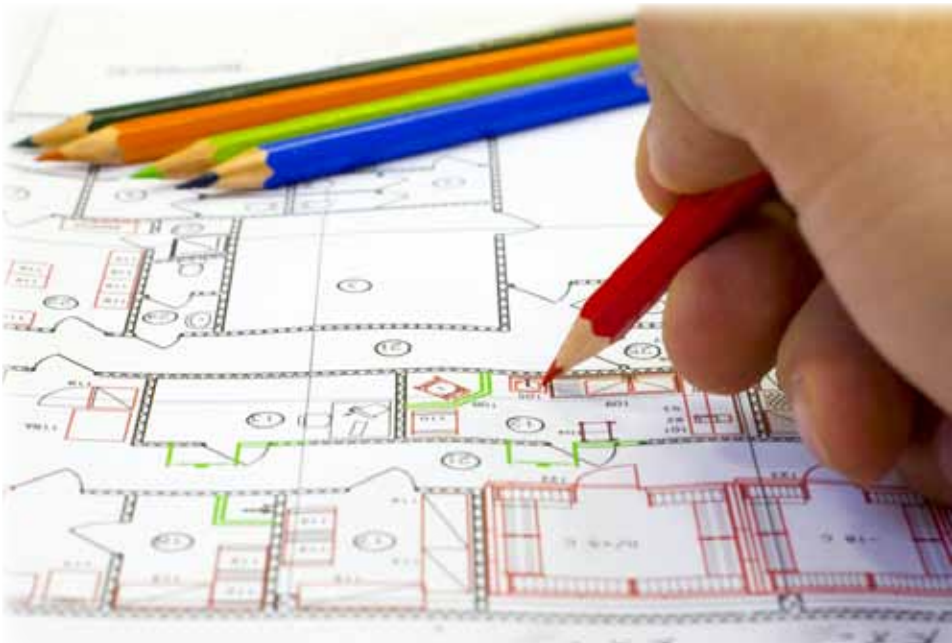
Sugiro uma grande reflexão sobre este tema: temos que investir cada vez mais na cultura de segurança.

Um abraço e até a próxima.

João Aparecido dos Santos

Formado em Administração de Empresas e Pós-Graduado em Gestão de Segurança Pública e Privada (MBA). Atua a 20 anos na área de segurança corporativa. É desde 2004 colaborador do Grupo DPaschoal, trabalhando atualmente como Supervisor Corporativo de Segurança Patrimonial.

sumário



Dias de Experiências

Alex Henrique

Estamos o tempo inteiro atentos, preocupados, em busca das melhores práticas ou experiências que realmente sirvam de valia à nossa organização. Conceitos, tecnologias, demonstrações de cases que deram certo em vários segmentos, despejam inspirações de sucesso aos espectadores, pois apresentam declarações de que a partir dali, o fator determinante para o resultado lucrativo e esperado, aconteceu.

Internamente, somos a massa da empresa que caminha dentro de regras objetivas, atrás de metas, ideais e, até, em algumas vezes, sem rumo!

Explosões de endomarketing em campanhas geniais ilustram esse contexto, mas pasmem, apesar de atingirem uma grande fatia do grupo funcional, paira sempre a dúvida entre os gestores: "Será que realmente foram úteis, e, teremos visível retorno nos próximos balanços?"

É provável que sim, pois mapeamos as respostas dos funcionários para cada setor, ou departamento da empresa, e pelas fiéis estatísticas veremos se o recado foi passado.

É ótimo ouvir a voz da empresa, digo, dos funcionários; é uma maneira honrosa e salutar de saber da conjuntura organizacional, e como diria Max Geringer "Humildade é descalçar os preconceitos e não ignorar os avisos de quem tem os pés no chão".

Materializar objetivos desse nível, na maioria das vezes, é se preparar para uma batalha sem precedentes, pois, enquanto isso, conduzimos estratégias para quem sabe nos aproximar

daquela que realmente irá fazer a diferença. Simples assim.

Apesar de alguns dessa massa, como nomeamos nesta inicial, seguirem sem rumo certo, esses integrantes não têm a menor ciência que estão nesse balão, e ao invés de reagirem como todos, continuam tocando seus dias como os anteriores. Por um lado é normal, e, por que iriam mudar se não sabem que estão em direções opostas?

Pensando um pouco sobre a melhor forma de gerir esses desafios internos, poderíamos facilmente culpar esse ou aquele gestor, ou, até mesmo, o dono da empresa que se apresenta esporadicamente em alguns dias da semana e que pelo Black Berry acompanha os números e resultados on line, delegando seu tempo integral. Parece até que se encontra junto ao aparelho de acesso ilimitado à rede universal *full time*. Será?

Este último comentário se deve, em razão de que a maioria dos e-mails enviados pela secretária do gestor ou presidente ou pela diretoria da empresa é respondido sempre em até 05 (cinco) minutos.

O fato é a prova existencial e sistêmica desses e-mails, que trazem o horário de recebimento e a resposta delegativa do chefe, ratificando a enquete apresentada.

Em 15 (quinze) anos de existência, essa empresa nunca deu tanto lucro como nos últimos 2 a 3 anos. Pois é, o que atrai essa plena e serene situação é apresentado como reflexo do aumento de clientes e do poder de compra dos brasileiros, aliado às frequentes ações internas da empresa de satisfação do funcionário.

Caros leitores, falamos um pouco mais de gestão dessa vez, mas em nosso último contato, apresentamos um verídico e atual relato, de um empresário do setor de transportes, que, após um golpe do destino, sofreu uma fraude em sua empresa, que, até hoje, traz resquícios do golpe.

Em nosso próximo encontro, discutiremos o tema: "Os desafios para a era do conhecimento"

Obrigado e um grande abraço.

Alex Henrique

Ex-militar do 1º Regimento de Cavalaria de Guardas (Dragões da Independência). Formado em Gestão Estratégica de Pequenas e Médias Empresas/ Extensão em Rh e Liderança. Trabalha na Diretoria do Setor de Investigação de Segurança e Fraudes do HSBC Bank Brasil.

sumário

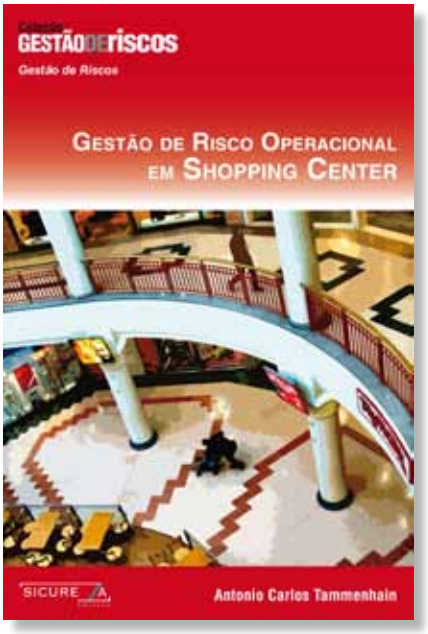
Mariana Fernandez

SEGURANÇA INVISÍVEL MAS NECESSÁRIA

O que você prefere: fazer compras em lojas de rua ou em shoppings centers e grandes lojas ou mercados com grandes variedades de produtos e/ou serviços?

Principalmente para quem mora nas grandes metrópoles, as horas do dia são sempre insuficientes tanto para nossos afazeres quanto para nossos lazeres. A solução, então, encontrada pelos habitantes das cidades, é dirigir-se para um único lugar para satisfazer seus desejos econômicos: um shopping center.

Até mesmo em cidades menores shopping centers são lugares atrativos por oferecerem tanto mais variedades de produtos quanto por reunirem num único local diferentes tipos de serviços. Assim, torna-se mais "econômico" e até mais divertido fazer compras num shopping.



Grandes lojas e supermercados, de estrutura semelhante a de um shopping center também podem ser compreendidas pela obra *Gestão de Risco Operacional em Shopping Center: a segurança que o cliente não vê* (Scicurezza, 2010).

Outro motivo de peso na escolha do cliente pelo shopping ao invés da rua está na questão da estrutura de segurança oferecida pelo shopping. É nesse sentido que o lançamento Antonio Carlos Tammenhain, aborda essa questão que parece tão óbvia mas que ainda não havia sido discutida de maneira comprometida no meio editorial.

"Contando com oito anos de serviço ativo no Exército, quando conheci no MBA, os métodos e ferramentas de Gestão Estratégica de Risco, eu já somava mais de 25 anos em atividades de segurança". Nas palvras do autor vê-se que além de conhecimento técnico, ele possui muita experiência prática.

Segundo ele, o livro, no entanto, não é um manual de de instrução para um Chefe de Segurança de Shopping Center, porque seu objetivo não é demonstrar técnicas operacionais. A obra aborda um leque mais amplo, fornecendo "importantes conhecimentos para que o leitor possa entender o envolvimento estratégico que um Gestor de Risco deve ter em todo o contexto da organização, pura e simplesmente, sabendo associar as suas atribuições aos conceitos de Planejamento Estratégico, Objetivo Estratégico, Fator Crítico de Sucesso e Risco Estratégico".

Na obra, super didática, o autor introduz o texto com as devidas definições dos termos em análise como shopping center e empreendimentos comerciais, bem como seus panorâmas históricos baseados em dados oficiais. Após adentra no organograma de estrutura organizacional para possibilitar aos leitores uma visão macro do assunto, que também pode ser adaptado para qualquer organização.

Mais precisamente na abordagem do foco do livro, o autor traz breve introdução sobre as administradoras de shoppings centers e seus órgãos fiscalizadores. Após segue detalhando as funções relativas aos shoppings centers de profissionais de organismos oficiais como: vigilância sanitária, Conselho Regional de Engenharia Arquitetura e Agronomia, Polícia Militar, Prefeituras etc. Depois lista, da mesma maneira, temas de preocupação dos shoppings como: meio ambiente, lixo, esgoto, etc.

Após esse panorâma básico geral, inicia sobre a Gerência de Operações nos shoppings centers. O capítulo seguinte trata do tema tão importante em Gestão de Riscos e previsto pela norma ISO 31000: a comunicação. Neste caso, entre os departamentos da organização.

A Segurança em Shopping Center é tema do quinto capítulo, abrindo caminho para as discussões mais específicas do sexto: Gestão de Risco, Gestão de Crise e Continuidade de Negócio e Senso de Urgência.

Sua contribuição prática encontra-se no estudo de caso do sétimo capítulo, onde o autor tenta contemplar todas as situações e processos relacionados à questão da segurança.

O livro conta com um conhecimento prático de grande valor, e que é muitas vezes elucidado pelo autor, como no trecho a seguir:

"...embora já tenhamos avançado muito com a profissionalização operacional e administrativa do setor, com a regulamentação e produção da clandestinidade operacional e do amadorismo na gestão, com o surgimento de novas tecnologias de segurança, com a publicação de normas internacionais e com o surgimento de cursos de formação de gestores de risco, até em nível superior e de pós-graduação, ainda estamos no início de um longo processo de mudança de imagem do setor."

Antonio Carlos Tammenhain é pós-graduado em Gestão de Recursos Humanos e possui MBA em Gestão de Segurança Empresarial além de ser formado em Administração de Empresas, ser tecnólogo químico e Técnico em Segurança do Trabalho com especialização em Engenharia de Incêndio.

sumário

você sabe o que é Risco Social ?

PSSE projetos de sustentabiliade social empresarial

A missão da PSSE é contribuir para a sustentabilidade competitiva dos negócios dos nossos Clientes, por meio da análise dos impactos socioambientais de seus projetos e operações e implementação de medidas que mitiguem os riscos sociais, ambientais e de imagem corporativa.

A empresa oferece ao mercado empresarial brasileiro uma ferramenta importante na minimização de riscos sociais de empreendimentos, além de mostrar que ter a sede e as principais unidades sustentáveis é uma forma de grande visibilidade.

Seu objetivo é agregar valor à percepção de imagem corporativa de responsabilidade socioambiental, segurança integrada do empreendimento e identificação de medidas para inclusão social local.

A PSSE é uma Joint Venture entre a SustentaX e a Brasiliano & Associados.

PSSE
Projetos de Sustentabilidade Social Empresarial

SUSTENTAX

b&a
BRASILIANO & ASSOCIADOS

Informações: info@brasiliano.com.br - www.brasiliano.com.br - 11 5531 6171