ISSN 1678-2496N

b&a
BRASILIANO & ASSOCIADOS

GESTÃO de RISCOS

www.brasiliano.com.br | Agosto 2011 | edição 69

Análise: Qual o rumo da gestão de riscos na cadeia logística?

Entrevista: com Claudio Peixoto, presidente da ACFE, associação contra as fraudes

GESTÃO DE RISCOS
técnica e objetividade

princípio básico da *gestão de riscos*

b&a
BRASILIANO & ASSOCIADOS

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

Sumário




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.

Revisão | Ana Paula Deodato.

Edição, arte e Diagramação | Agencia BM Design

Colunista | Ana Paula Deodato

Colaboradores desta edição | Ana Paula Deodato, Claudio Peixoto, Egle Dorminda Cascino, Gustavo Vedove, Reginaldo Catarino Ferreira e Wander Steves Carbone

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

Responsabilidade e Risco Social: Novo ENFOQUE estratégico

A responsabilidade social está relacionada como um tema importante dentro das organizações, exercendo impactos nos objetivos, estratégias e no próprio significado da empresa, propondo inúmeros processos de transformações na área econômica, política, social e cultural que, gerando laços entre as instituições, mercados, organizações e a sociedade.

A responsabilidade social pode ser tratada de diferente forma dentro das organizações: como estratégia de marketing institucional, como estratégia de valorização das ações da empresa, como estratégia de recursos humanos, estratégia de valorização de produtos/serviços, estratégia de inserção na comunidade, estratégia social de desenvolvimento na comunidade, como exercício de consciência ecológica, como exercício de capacitação profissional e a estratégia de relacionamento.

São fatores que significam mudanças de atitudes, que geram uma gestão empresarial nas qualidades das relações e na geração de valor para a organização, as empresas socialmente responsáveis são aquelas que buscam atitudes diferentes para o seu desenvolvimento, ainda se trata de um assunto novo em vários países, inclusive no Brasil, um assunto que deve ser explorado.

Falando sobre a responsabilidade social, lembramos, no dia 8 de dezembro de 2010, foi lançada no Brasil a versão em português da norma, a ABNT NBR ISO 26000, Diretrizes sobre responsabilidade social. Esta nova norma traz uma grande uniformidade nos conceitos, fornecendo diretrizes para que as organizações se preocuparem de uma forma ética e transparente com impactos das atividades realizadas na sociedade, contribuindo de uma forma sustentável para o meio ambiente. A Responsabilidade Social deve estar presente no desenvolvimento do projeto nas organizações, propondo as responsabilidades sociais e fazendo com que as empresas identifiquem os seus impactos na sociedade como um todo.

1. É necessário tratar de sete temas centrais, para que as empresas estejam alinhadas com a ISO 26000:Governança organizacional: Trata de processos e estruturas de tomada de decisão, delegação de poder e controle, é o fator que se responsabiliza pelos impactos sobre o qual a organização deve agir e uma forma de incorporar os princípios e práticas da responsabilidade social à sua forma de atuação cotidiana.

2. **Direitos humanos:** onde engloba situações de risco para os Direitos Humanos, como evitar cumplicidades, resolução de queixas, descriminação e grupo vulneráveis, direito civis e políticos, direitos econômicos, sociais e culturais.
3. **Práticas trabalhistas:** Vão além da relação da organização com os colaboradores, referindo-se tanto a emprego direto quanto ao terceirizado e ao trabalho autônomo.
4. **Meio ambiente:** Reforça o uso sustentável de recursos e a proteção do meio ambiente, da biodiversidade e restauração de habitats naturais.
5. **Práticas leais de operação:** Compreendem práticas anticorrupção, envolvimento político responsável, promoção da responsabilidade social na cadeia de valor e respeito aos direitos de propriedade.
6. **Questões dos consumidores:** Proteção à saúde e a segurança do consumidor, consumo sustentável, atendimento e suporte ao consumidor.
7. **Envolvimento e desenvolvimento da comunidade:** Refere-se a educação e cultura, geração de emprego e capacitação; desenvolvimento tecnológico e acesso a tecnologias; geração de riqueza e renda; saúde e investimento social.

Esta norma aumenta a amplitude do Gestor de Riscos, fazendo com que a área de Riscos tenha uma maior versatilidade e transversalidade. Cresce a nossa responsabilidade!!

Boa leitura e sorte!!!

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

Information Risk Assessment - IRA

As empresas enfrentam, hoje, desafios em várias frentes, tais como consumidores exigentes, regras cada vez mais complexas, novas regulamentações e o mercado cada vez mais competitivo.

A fuga de informações estratégicas e o roubo de documentos corporativos é hoje uma ameaça real. Segundo a Câmara de Comércio Americana dos EUA, os custos com a perda de propriedade intelectual giram em torno de US$ 25 bilhões de dólares. E o pior é que estas informações estratégicas não estavam armazenadas em computadores, mas disponíveis em recipientes de lixo, jogados em copiadoras, impressoras e nas mesas dos executivos e gerentes.

A fuga e ou roubo de informações estratégicas, por não proteger adequadamente e não saber elimina, por exemplo dados financeiros de cliente, podem resultar na responsabilidade direta de violação de privacidade. Ou seja as empresas podem ser processadas a indenizar seus clientes pela fuga e ou roubo de informações!

Acreditamos que no mercado brasileiro ainda exista muito o que fazer em termos de prevenção de fuga e roubo de informações estratégicas.

A Brasiliano & Associados avalia as fragilidades do ambiente, foco no Fator Humano, identificando o nível de risco da Fuga e ou Roubo de Informações Estratégicas. Tudo isso através de um processo prático e objetivo.

Oferecemos um trabalho independente, com uma visão prospectiva, utilizando metodologia própria, levando em consideração a informação exposta, o acesso aos documentos estratégicos, os equipamentos que contém informações e não estão devidamente protegidos e a infra estrutura física.

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

- Gestão de Risco de Fuga e Roubo de Informações Estratégicas
- Mapeamento, Avaliação e Respostas aos Riscos
- Políticas de Segurança da Informação
- Programas de Sensibilização – Trato das Informações Estratégicas
- Programas de Inteligência e Contra Inteligência Empresarial
- Programas e Processos de Eliminação de Informações Estratégicas
- Avaliação das Fragilidades – Nível de Risco – Testes Operacionais

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

Editorial

Nesta edição, Reginaldo Catarino, diretor da divisão de Supply Chain Risk Management, traz no seu artigo "Os Novos Rumos da Gestão de Riscos na Cadeia Logística", explicações à função da gestão de riscos dentro da cadeia, mostrando ao leitor a questão do risco no processo de planejamento estratégico empresarial e o que é a família da norma ISO 28000. Dando a oportunidade para o leitor entender e saber o que e processos sob a dimensão do risco.

A matéria sobre Riscos Ambientais na área de trabalho apresenta quais são os riscos que as organizações estão sujeitas, o que fazer para que o risco não traga danos maiores para as organizações, quais são as consequências que as organizações podem enfrentar.

Nesta matéria eu, Ana Paula Deodato, trago um mapa de riscos mostrando o índice dos riscos dentro das organizações.

Gustavo Vedove explica em seu artigo quais são os cuidados que as organizações, escolas, residências, condomínios entre outros devem tomar com o sistema de segurança implantado nas mesmas, como manter adequadamente o Circuito Fechado de Televisão, Alarmes e Controle de Acesso. O artigo conta com dicas para todo tipo de proteção, em todos os tipos de condomínios, dicas em geral.

Egle Dorminda Cascino e Wander Steves Carbone escreveram para a Revista Gestão de Riscos, o artigos Engenharia Social a Arte de Enganar, o meio mais utilizado para obter acesso as informações sigilosas dentro da organizações, onde o golpista entra no sistema e descobre informações importantes, neste artigos os autores identifica o que é a Engenharia Social, os conceitos, o perfil do engenheiro social, as ferramentas e aplicações, a engenharia na internet, pontos fracos explorados pelo engenheiro social e outras informações que estão na coluna Sistema da informação.

O entrevistado do mês é Claudio Peixoto, diretor de investigação da Ernst & Young Terco e presidente da ACFE – Association of Certified Fraud Examiners Brasil, associação que combate e prevenção de corrupções e fraudes nas organizações. Nesta entrevista você saberá como a associação surgiu, quais as principais metas e soluções que a associação trabalha para conquistar.

Acontece traz todos os eventos que passaram e que estão para ocorrer no próximo mês.

Brasiliano no jornal interno Acontece Metrô BH, lançamento do livro do Brasiliano, Guia Prático para a Gestão de Continuidade de Negócios – GCN e do livro do Humberto Orlá, As fraudes contra as Organizações e o papel da Auditoria Interna, confira o que aconteceu na noite de autógrafos. Os cursos que a Brasiliano & Associados ministrou no mês de julho, além da participação do Brasiliano com diretor da ACEF – Association of Certified Fraud Examiners Brasil e o 1° Congresso de Combate e Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, que a Febraban – Federação Brasileira de Bancos está organizando, todas as informações no Acontece.

Editorial

O Capital Baseado em Risco uma Abordagem para Operadoras de Planos de Saúde é o lançamento desta edição, obra sobre os riscos que as operadoras estão expostas e o que fazer quando acontecer algum imprevisto, Renata Gasparello de Almeida autora traz todas as informações necessárias a você leitor, não deixa de conferir na coluna Ler&Saber.

Boa Leitura!

Ana Paula Deodato
anapaula@brasiliano.com.br

OS NOVOS RUMOS DA GESTÃO RISCOS NA CADEIA LOGÍSTICA

Reginaldo Catarino Ferreira I Graduado em Administração de Empresas - Planejamento Estratégico Empresarial pela Faculdade UNINOVE; Certificado ISO 31000 pelo QSP (Centro de Qualidade, Segurança e Produtividade para o Brasil e América Latina); Especialista em Segurança Empresarial – Master Business Security (MBS) e em Gerenciamento de Riscos em Transporte Rodoviário de Cargas pela Faculdade FECAP e Brasiliano & Associados; Ex-oficial do Exército Brasileiro; atuou como Diretor de Operações em grandes Gerenciadoras de Riscos e atualmente é Diretor de Supply Chain Risk Management da Brasiliano & Associados.
reginaldo@brasiliano.com.br

Introdução

Para iniciar um assunto tão complexo que é a Gestão de Riscos na Cadeia Logística, primeiramente, é importante entender que Gestão de Riscos é um processo integrado e amplo, não se restringindo apenas a segurança, mas envolvendo estratégia, tecnologia, fluxo de informações, processos e operações.

Logo é necessário enxergar os Riscos Logísticos integrados ao negócio das Organizações. Traduzindo, é enxergar como as práticas de gestão contribuem para o cumprimento da Missão definida pela empresa e como tais ações podem se tornar diferenciais que possibilitem alcançar as Visões pretendidas. Ou seja, a Gestão de Riscos na Cadeia Logística deve ser compreendida como parte de um processo estratégico que tem como principal objetivo à garantia de sucesso dos objetivos empresariais.

Desta forma, torna-se imperativo abordar aspectos do processo de Formulação de Estratégia e a importância da Logística Empresarial como diferencial competitivo de negócio.

Assim, passa a ser coerente discorrer sobre a Gestão Riscos como uma importante Atividade de Suporte na Cadeia de Valores para suportar os Fatores Críticos de Sucesso do negócio. E para tanto, a Gestão de Riscos se torna, explicitamente, parte integrante do Planejamento Estratégico Empresarial.

Entendendo a Questão do Risco no Processo de Planejamento Estratégico Empresarial

Entendendo que a primeira fase de um Planejamento Estratégico é a Análise de Ambiente, já nos defrontamos com o primeiro grande desafio: Quais serão as ameaças ao nosso negócio?

Trazendo essa questão para a Logística, devemos prospectar quais seriam as possíveis ameaças a serem originadas no Ambiente Geral (Social, Econômico, Tecnológico, Legal e Político) e no Ambiente Operacional (Fornecedores, Concorrência, Mão-de-Obra, Clientes e aspectos Internacionais).

Seguindo essa mesma linha de raciocínio, devemos novamente perguntar quais são as vulnerabilidades do Ambiente Interno da Logística da Organização.

Neste contexto, o conceito de Supply Chain necessita ser explorado com a máxima atenção, pois a Cadeia Logística em muitos casos se equivale à própria Cadeia de Valores do negócio, pois acaba abarcando toda composição das Atividades Primárias.

O que podemos concluir com tudo isso que existe a necessidade de entender o Mapa Estratégico da Organização, seus Fatores Críticos de Sucesso e as relações com os Objetivos e Metas existentes para a Cadeia Logística. Pois esse entendimento permitirá identificar os riscos existentes, sejam de cunho estratégico, sejam de cunho operacional.

Porém essa tarefa de identificação não é fácil e nem mesmo intuitiva... E para tanto, devemos observar e utilizar melhores práticas e normas internacionais, como a ISO 28000.

A ISO 28000

Hoje temos a família ISO 28000 – Especificações para Sistemas de Gestão de Segurança para a Cadeia Logística. Uma família composta pelas normas:

- ISO 28001:2007 - fornece os requisitos e orientações para as organizações desenvolverem e implementarem processos de segurança em suas cadeias de logísticas;
- ISO/PAS 28002:2010 – especifica requisitos para um sistema de

gerenciamento de resiliência na cadeia logística;

- ISO/PAS 28003:2006 – contém princípios e requisitos para as entidades de auditoria e certificação;
- ISO 28004:2007 – fornece conselhos genéricos sobre a aplicação da ISO 28000:2007;
- ISO 28005:2011 – contém especificações técnicas que facilitam a troca eficiente de informações eletrônicas entre navios e em terra.

A ABNT (Associação Brasileira de Normas Técnicas), que representa a ISO no Brasil, publicou a ABNT ISO 28000 em 24 de junho de 2009.

Dentre vários requisitos importantes da ABNT ISO 28000 abaixo serão citados alguns:

- Assegurar o controle de processos terceirizados;
- Fornecer evidências do comprometimento da alta gestão;

- Estabelecer e manter Estrutura para Gerenciar Riscos compatíveis com as necessidades da organização;
- Assegurar que os responsáveis estejam adequadamente capacitados no que tange a formação, treinamento e experiência;
- Estabelecer, implementar e manter procedimentos documentados;
- Deve analisar periodicamente a eficácia de sua prontidão e respostas a emergências e recuperação de segurança;
- Investigar itens relacionados a falhas, incluindo alarmes falsos e quase ocorrências de falhas de segurança;
- Investigar incidentes e situações de emergência;
- Estabelecer, implementar e manter um programa de auditoria de gestão de segurança;
- A Alta Administração deve analisar o sistema de gestão de segurança, em intervalos planejados, para assegurar a continuidade de sua conformidade, adequação e eficácia;
- Os resultados das análises devem incluir decisões e ações possíveis quanto a modificações nas políticas de segurança, nos objetivos, nas metas ou outros elementos dos sistemas de gestão.

Com a ISO 28000 vemos claramente a preocupação global de garantir a segurança das Cadeias Logísticas.

"o foco de desenvolver e melhorar processos passa, basicamente, sob a ótica de duas dimensões: tempos e custos. O que é plenamente correto e consagrado"

No Brasil, especialmente, existe um contexto *sui generis* devido ao tamanho do país, sua cultura, problemas políticos, estrutura precária de portos e aeroportos, estado ruim das estradas, desbalanceamento da matriz de transportes, crime organizado, criminalidade urbana e outros graves problemas que contrastam com as necessidades de um país que hoje é a 7ª economia do mundo.

Agora temos uma oportunidade de alinhar nossos modelos com os padrões mundiais e também de olhar para a segurança de nossas Cadeias Logísticas com uma mesmo referencial.

A utilização de melhores práticas, sob um mesmo referencial, como a ISO 28000, torna possível estabelecer comparações, estabelecer metas alinhadas, direcionar esforços de forma inteligente, agir com base em planejamento e aumentar as garantias de sucesso.

Isso ocorre porque essa norma possui em seu âmago conceitos, plenamente, alinhados com a ISO 31000 (Gestão de Riscos Corporativos) e recomenda, explicitamente, que sejam alinhados seus requisitos com outras certificações como a ISO 9001:2008 e a ISO 14000:2004.

Através da compreensão estratégica do negócio e do alinhamento desses sistemas de gestão, a formulação e implementação de modelos de gestão de riscos na Cadeia Logística ganham probabilidades exponenciais de sucesso.

Assim a Gestão de Riscos e práticas de Segurança passam a ser integradas aos processos da própria Cadeia Logística e não mais se comportam como apêndices das atividades principais da empresa.

Ou seja, a Gestão de Riscos passa a ser um elemento que gera valor para o negócio.

Gerenciando Riscos nos Processos Logísticos

As empresas trabalham seus processos para melhorar indicadores de produtividade, garantir o nível de qualidade prometido ou exigido pelos clientes, reter o conhecimento, permitir a existência de métricas para seus modelos de gestão e outros motivos que poderíamos citar.

Contudo, o foco de desenvolver e melhorar processos passa, basicamente, sob a ótica de duas dimensões: tempos e custos. O que é plenamente correto e consagrado.

Agora temos uma nova oportunidade... A oportunidade de após essa análise e definição dos processos, sob as dimensões de tempos e custos, de avaliar esses processos sob a dimensão do risco.

Ou seja, avaliar os processos buscando identificar rupturas, existentes ou potenciais, que afetem os Fatores Críticos de Sucesso e por sua vez possam impactar os Objetivos do Negócio.

Essa abordagem cria um novo cenário para os gestores de logística, porque agora podem, inteligentemente, avaliar suas decisões sob uma ótica de custo benéfico para o negócio, quando tratarem dos requisitos de segurança.

Assim os investimentos financeiros ou em energia nos assuntos de segurança sobem de nível na pirâmide de gestão, porque passam a ser tratados, na verdade, com assunto de riscos.

Na prática o que devemos fazer, após as fases de entendimento do contexto e de estruturação dos planos de comunicação e consulta, é aplicar os conceitos da Auditoria Baseada em Riscos para mapear os processos logísticos e demais processos que tenham interfaces com os objetivos a atingir.

Este mapeamento exige uma análise dos modelos adotados, dos fluxos operacionais e de operações, do nível de aderência dos controles previstos, do emprego das tecnologias e das questões ligadas às pessoas.

O resultado esperado é identificar os chamados *red flags*, ou seja, pontos de atenção reais ou potenciais que poderiam até mesmo ser classificados como pequenas falhas. Pequenas falhas essas que passam a compor fatores de riscos. E para que este trabalho seja executado com sucesso a aplicação de metodologia se torna crucial.

Sem método, sem processo, apenas com a experiência ou força de vontade se tendência a alongar os trabalhos, dificultar a organização das informações e obscurecer as análises. Logo aplicar o framework da ISO 31000 aliado aos requisitos da ISO 28000 dá ao trabalho a tecnicidade necessária para alcançar bons resultados.

Supply Chain Risk Management - SCRM

A gestão de riscos da cadeia logística – Supply Chain Risk Management (SCRM) integra a organização, clientes, fornecedores e seu ambiente empresarial, reduzindo a dependência e promovendo a sinergia. Desta forma o gerenciamento contínuo dos riscos na cadeia logística passa a ser fonte de vantagem competitiva para todos neste processo.

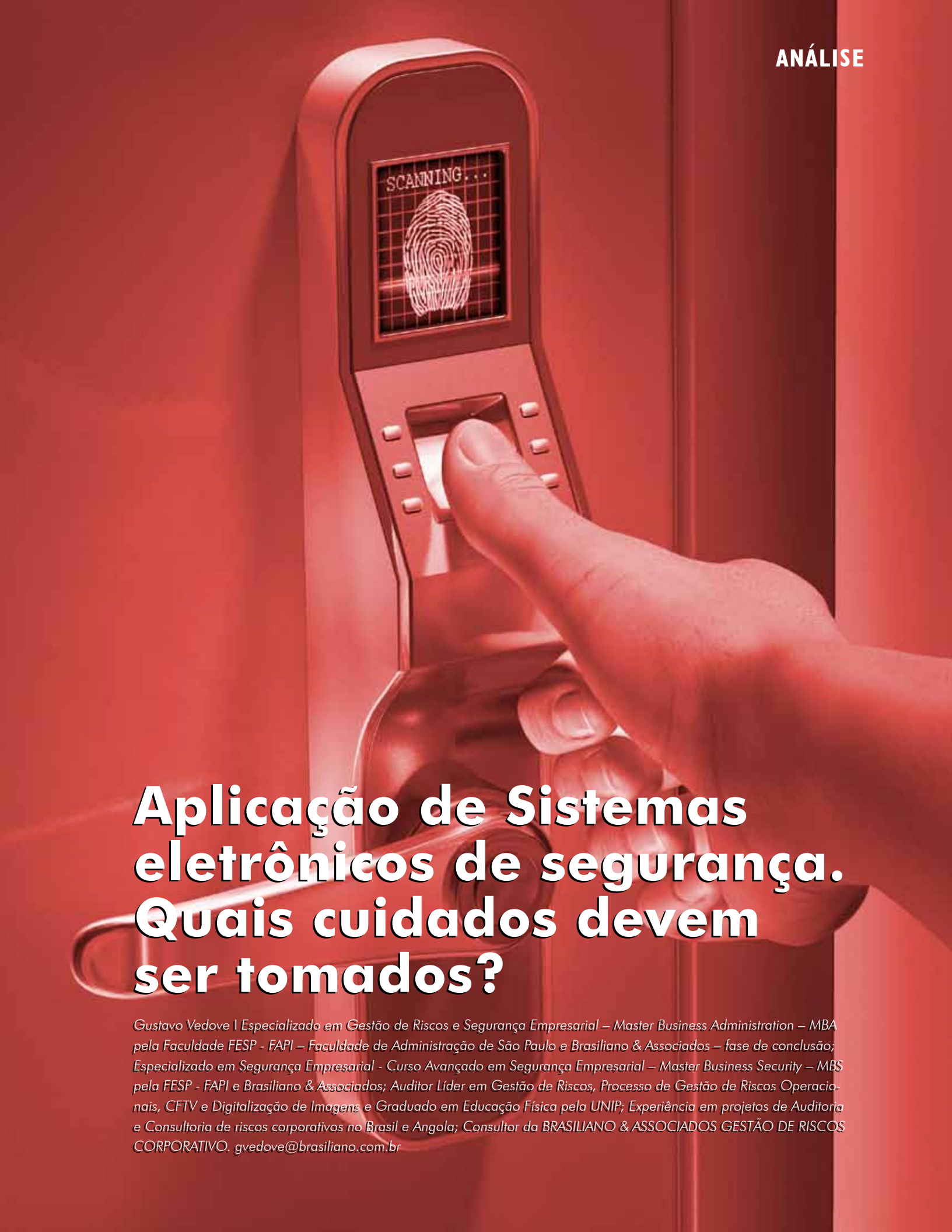
Os riscos na cadeia logística podem afetar uns ou vários dos processos operacionais, podendo influenciar negativamente os objetivos de negócio. A gestão de riscos da cadeia logística é estruturado e sinérgico, aperfeiçoando a estratégia, os processos, os recursos humanos e a tecnologia. O foco é controlar, monitorar e avaliar o risco da cadeia logística visando garantir a continuidade o processo Supply Chain e aumentar sua resilência.

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

- Implantação do Processo de Gestão de Riscos, com base na ISO 28000, 28002 e 31000;
- Elaboração no todo ou em partes do processo de Identificação, Análise e Avaliação e Tratamento dos Riscos na Cadeia Logística, com base na ISO 28000, 28002 e 31000;
- Elaboração e Implantação de Política de Gestão Riscos e da Gestão da Segurança para a Cadeia Logística, seguindo os preceitos da ISO 28000, 28002 e 31000;
- Elaboração e Implantação de Manuais de Contingência e Continuidade das Operações, seguindo os preceitos da ABNT NBR 15999, ISO 28000, 28002 e 31000;
- Elaboração de Processo de Comunicação e Consulta, incluindo as técnicas e ferramentas de sensibilização e conscientização para o público interno e externo;
- Preparação para a Certificação da ISO 28000.

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

b&a
BRASILIANO&ASSOCIADOS



Aplicação de Sistemas eletrônicos de segurança. Quais cuidados devem ser tomados?

Gustavo Vedove | Especializado em Gestão de Riscos e Segurança Empresarial – Master Business Administration – MBA pela Faculdade FESP - FAPI – Faculdade de Administração de São Paulo e Brasiliano & Associados – fase de conclusão; Especializado em Segurança Empresarial - Curso Avançado em Segurança Empresarial – Master Business Security – MBS pela FESP - FAPI e Brasiliano & Associados; Auditor Líder em Gestão de Riscos, Processo de Gestão de Riscos Operacionais, CFTV e Digitalização de Imagens e Graduado em Educação Física pela UNIP; Experiência em projetos de Auditoria e Consultoria de riscos corporativos no Brasil e Angola; Consultor da BRASILIANO & ASSOCIADOS GESTÃO DE RISCOS CORPORATIVO. gvedove@brasiliano.com.br

Os objetivos deste artigo são: Mostrar situações de aplicação e dar algumas dicas para o comprador solicitar ao fornecedor.

Parece até comum e automático a implantação de sistemas eletrônicos em empresas, escolas, residências, condomínios, industriais, entre outros, mas, qual critério para averiguar a necessidade de instalar sistemas eletrônicos como Circuito Fechado de Televisão, Alarmes, Controle de Acesso, entre outros?

Proteção Perimetral: A pergunta é: O que queremos identificar ou evitar?

Queremos identificar apenas uma pessoa pulando a cerca e ou o muro e temos meios de reação para atuar? *Então por que gastar como sistemas perimetrais, tipo cerca elétrica e ou infravermelho ativo (IVA)*? *Se análise de riscos mostra que a segurança no local pode ser feita com meios de reação e o apetite ao risco da empresa assume esta invasão, é possível economizar no gasto com sistema de detecção. Com um gasto menor é possível monitorar o perímetro apenas com uma câmera tendo a lente adequada para abranger toda extensão, já que a intenção é identificar apenas que alguém pulou e não seu rosto.*

E quando o foco é impedir a entrada? No caso de condomínios horizontais, onde a extensão perimetral é uma das maiores criticidades de segurança, as dicas são: Proteger a parte superior do muro com concertina dupla e realizar manutenção preventiva e verificação através de rondas constantemente, pois os agressores deste tipo de condomínio costumam preparar a ação, ou seja, por vezes, os mesmos danificam o perímetro para voltar no outro dia, sendo: o corte e ou abertura de intervalos na própria concertina ou arame, além de buracos nos blocos pelo lado externo para possibilitar a subida.

Estruturando a proteção superior, é preciso avaliar a estrutura do corpo do muro deixada pela incorporadora do residencial. O ideal seria a incorporada ter previsto uma cerca a 1,20 de altura chapiscada de cimento pelo lado interno junto aos blocos para evitar a abertura de buracos para passagem, mas, como este investimento quase nunca acontece, fica sob a responsabilidade de o condomínio investir para proteção deste nível do perímetro, pois este modus operandi para entrada, ocorrem frequentemente em condomínios destas características que se situam em áreas florestais, o que ajuda os meliantes.

O terceiro nível de proteção do perímetro seria a plantação de sanção do campo, que é um arbusto de rápido crescimento e apresenta vantagens que o tornam ideal para a formação de cerca viva, com espinhos semelhantes aos da roseira, funcionando como uma barreira contra invasores no perímetro interno do condomínio.

O investimento é alto, mas, é uma estratégia de proteção funcional, diferentemente de sistemas eletrônicos como cerca elétrica e IVA, que não evitam a entrada, além de proporcionar alta manutenção e alarmes falsos considerando a aplicação neste tipo de conjuntura, necessitando

ainda de alto investimento em infraestrutura para funcionamento e monitoramento dos sistemas.

Condomínios verticais: A grande porcentagem de aplicação em proteção perimetral neste tipo de condomínio se resume em cerca elétrica e infravermelho ativo (IVA), agora, qual sistema é o mais ideal? Novamente a análise de risco é de suma importância para decisão entre um sistema e outro. Características do bairro, índice de criminalidade na região, estudo de modus operandi, poder aquisitivo dos moradores, nível de segurança nos condomínios vizinhos, poder de reação do condomínio e policia da região, entre outros, devem ser consideradas no estudo.

Ambos os sistemas oferecem vantagens e desvantagens, simplificadamente sendo:

Cerca elétrica:

Maior gasto com manutenção, maior inibição por se tratar de uma barreira física, é mais ostensivo, há quem ache agressivo e gera a impressão de uma prisão e há quem não se importa com tal aparência e o gasto é maior, principalmente em grandes distâncias.

IVA (infravermelho ativo):

É mais discreto, menor gasto com manutenção, menor tempo de instalação, principalmente em grandes distâncias, não é uma barreira física e o custo é menor.

A determinação de qual sistema utilizar é sempre com base na análise de riscos, que depende também do nível de percepção de segurança dos condôminos. O fato é que um sistema de detecção surge em apoio aos meios humanos. Através dos recursos tecnológicos as identificações de situações críticas poderão ser monitoradas e até evitadas. As ferramentas aperfeiçoarão o suporte aos recursos humanos, que por sua vez oferecem o meio de reação. A reação é a resposta pronta e efetiva ao risco.

Neste caso o condomínio pode contratar o monitoramento deste alarme, replicar o sinal nos apartamentos e exigir pronta resposta da empresa contratada.

Dicas em Geral

- Procurar empresas conhecidas no mercado, que ofereçam garantia do serviço, ou seja, empresas com know how.
- Conhecer um projeto feito pela empresa antes da contratação.
- Para indústrias e empresas de médio e grande porte, na intenção de implantar sistema IP de CFTV, procurar sempre contar com apoio e auxilio da área de T.I, caso contrário dificilmente o projeto será aprovado, pois influenciará diretamente na rede da empresa, que deve estar preparada para receber este tipo de sistema, por isso o responsável

pela T.I deve ter fundamental participação. Aperfeiçoar os recursos da rede através da qualidade de serviço (QoS), priorizando conforme a necessidade o tráfego de dados do sistema de segurança, com objetivo de melhora da performance de transmissão.

- Realize análise custo x benefício.
- Prever contingências para os sistemas: Caminhões distintos de cabeamento
- O dimensionamento do no-break deve levar em consideração todos os equipamentos do sistema, câmeras, estações de monitoramento, monitores, etc. Tudo deve funcionar mesmo sem energia. O fornecedor deve se responsabilizar pelo correto dimensionamento levando em conta o consumo dos equipamentos propostos.
- Para as câmeras, distâncias acima de 150 metros, usar fibra ótica multímodo.
- Para as câmeras interligadas por fibra ótica multímodo, ou seja, as que estiverem a uma distância acima de 150 metros do switch de distribuição, usar um par de conversores de mídia.
- Até 150 metros utilizar cabo UTP: Cabo UTP categoria 6.
- Cabeamento do Switch Core para os Switches de Distribuição – Usar fibra ótica multímodo.
- Cabeamento do No-break para os Switches de Distribuição – Usar Cabo PP+T 3x2, 5mm, antichama.
- Colocar os switches no no-break e o no-break no gerador.
- Deixar sempre 10% das portas dos switches livres para serviços de manutenção.
- Redundância da fonte de alimentação dos switches de distribuição. Utilizar no-break local para alimentar os switches.
- Instalar os switches em local seguro e restrito, podendo ser em AT (área técnica) e ou shaft.
- Realizar manutenções preventivas.
- Atentar-se a temperatura do ambiente e capacidade da câmera. Se necessário usar meios auxiliares como caixa de proteção com ventilação.
- Todo projeto de CFTV tem que possuir diferentes câmeras com lentes de acordo com aplicação.
- Na aplicação de lentes auto Iris obrigatoriamente a câmera tem que ter a função que irá acionar esse dispositivo (auto Iris). A função de circuito eletrônico que interliga é o controle de vídeo Iris.
- Para aperfeiçoar recurso e usar apenas uma câmera para monitorar dois ambientes, é preciso

a função EDR (eletronic dinamic range). Ex: monitora dentro do bar pegando a janela monitorando parte da rua. Muito utilizado em tuneis.

- É necessário fazer a integração de câmeras x lente x iluminação do ambiente por que o escrito na especificação de 0,01 lux na realidade não atende por que existe um * que mostra a real necessidade da câmera em iluminação.
- Microcâmera - Aplicação: elevadores e salas pequenas (média de 7 x 5 m). Motivo: lente grande angular 90°, o que é preciso para ambientes pequenos onde se necessita identificar as pessoas.
- Alimentação das câmeras: Mais recomendado trabalhar com 24V AC. Motivo: proteção contra raios.
- Para todas as soluções, o ideal é avaliar a empresa em termos de sobrevivência de mercado, pós venda e reposição de peça.
- Toda proposta deve prever proteção de surto/transientes. Protetor de surto MPS 1-15 e protetor de surto para o cabo de sinal de CFTV.
- Toda proposta deve prever o item proteção elétrico do sistema, sendo aterramento.
- Nunca instalar os DVR's na portaria. O local deve ser protegido e restrito, além de prever ar condicionado.
- Na utilização de cabo coaxial para dar impedância utilizar: RG59 até 300 mts e RG6 e RG11 até 700 mts.
- Os cabos coaxiais suportam as seguintes distâncias para transmissão de sinal de vídeo colorido: Cabo minicoaxial – até 100 metros, Cabo da série 59 – até 228 metros, Cabo da série 6 – até 304 metros e Cabo da série 11 – até 457 metros.
- Para aplicação em prédios, na vertical, é viável utilizar cabo UTP (par trançado).

Em meio a tantas opções no mercado, o ideal é alinhar a necessidade realizando um custo benefício frente ao nível de risco da empresa, indústria, escola, condomínio, entre outros. A mensuração da probabilidade e o impacto do risco que darão a diretriz para implementação, que deve agregar valor nos processos de segurança, permitindo a otimização de recursos, meios de proteção, detecção e reação.

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

RISCOS NO AMBIENTE DE TRABALHO, O QUE FAZER QUANDO ELE ESTÁ PRESENTE?

Os riscos ambientais estão dentro das organizações e muitas delas não sabem como descobrir certos riscos que podem trazer grandes impactos Ana Paula Deodato – anapaula@brasiliano.com.br

Sabemos que não vivemos em mundo livro dos riscos, sempre vamos deparar com tipos de riscos diferentes, que podem causar diferentes impactos na sociedade, nas organizações e em diferentes tipos de ocasiões quando não tratado o risco corretamente, e sempre é preferível um pequeno risco se um risco maior puder ser evitado. Quando falamos de riscos ambientais estamos tratando de um assunto que gera três diferentes círculos de riscos, o risco na segurança, acidentes de alta consequência e sua probabilidade pode ser nomeada como baixa, tendo em vista a segurança do trabalhador e na prevenção de perdas. Os ricos sobre a saúde é considerado de alta probabilidade, e com menor consequência, mas a relação de causa e efeito, trazendo problemas na produtividade da organização e ara a saúde dos colaboradores. Já o risco ecológico dentro de todos os riscos neste circulo, o resultado pode ainda trazer uma complexidade de riscos para o meio ambiente, causando danos para a população, para comunidade e no ecossistema, onde o impacto pode ser grande gerando diferentes consequências.

Os riscos ambientais são alargados de várias formas e divididos em cinco categorias de riscos, onde classificamos os agentes como riscos físicos, químicos, riscos biológicos, riscos ergonômicos e riscos de acidentes, onde estão existentes em todos nos locais de trabalho e que podem causar danos à saúde dos colaboradores e o desempenho da organização. Sem as prevenções correta de riscos, o aumento da capacidade de gerar danos às organizações é grande, quando a organização não sabe dos riscos que ela está exposta a probabilidade de acontecer praticamente inevitável, é necessário que a organização esteja completamente prevenida das ameaças dos riscos, para que isso não aconteça, a necessidade de entender quais riscos cada empresa pode enfrentar é um dos passos importantes para evitar perdas.

Toda organização deve estar dentro dos padrões de normas para que não ocorram acidentes que possam denegrir a imagem da empresa, o importante é separar o perigo e o risco, pois o perigo são condições quem podem causar danos às pessoas, propriedades e meio ambiente, já o risco é quando um perigo pode se transforma em um acidente. É necessária uma análise concreta dos cenários para evitar esses tipos de eventos que possam ocorrer certas variações que chegue a causar consequências nas empresas.

É necessário, conhecer os que estão expostos, identificar os fatores de riscos, fazer uma listagem de perigos, conhecer as condições dos processos estudados, classificar os perigos de acordo com a política e critérios estabelecidos no contexto estratégico.

Esses riscos resultam em situações que são indesejáveis onde sabemos que sem um gerenciamento é de fato o que pode acontecer, quando é mapeado o riscos, e ele vir a acontecer, será gerado uma situação que

de uma forma será aceitável, sabendo que essa situação de uma forma será aceita e assumida, assim a organização saberá que estava gerenciada de acordo com os riscos onde ela saberia que poderia ser causado de alguma forma.

Os riscos ambientais estão sempre expostos em todas as organizações, que são eles:

Riscos Físicos

São fatores que estão relacionados com: luz, barulho, temperatura, umidade, ventilação, radiações, ruído, calor, pressões e altura.

Riscos Químicos

São fatores relacionados à: poeira, gases, vapores, aerossóis, aerossóis sólidos, fumaças e combustível em geral.

Riscos Biológicos

Esses fatores são: vírus, bactérias, protozoários, bacilos, animais peçonhentos, suor e águas residuais e efluentes.

Riscos Ergonômicos

Os fatores são: local de trabalho inadequado, levantamento de peso impropriado, jornada prolongada, desconforto e treinamento inadequado.

Riscos de Acidentes

Máquina sem proteção, choques elétricos, equipamentos, ferramentas inadequadas, perigo de incêndio, material fora de especificação e edificação perigosas.

Consequências

O ruído atua diretamente sobre o sistema nervoso, com efeitos diversos: fadiga nervosa; alterações mentais: perda de memória, irritabilidade, hipertensão; modificação do ritmo cardíaco; diminuição da visão noturna; dificuldade na percepção de cores. Além destas consequências, o ruído atinge também o aparelho auditivo causando a perda temporária ou definitiva da audição. As consequências das vibrações se diferem problemas nas articulações das mãos e braços; osteoporose.

Absorver radiações no organismo pode causar diversas lesões, sendo ela radiação ionizante ou não ionizante - Radiações ionizantes: os operadores de raios-X e radioterapia e radiações não ionizantes: já se trata da radiação infravermelha, radiação ultravioleta como a gerada por operações em solda elétrica, ou ainda raios laser, micro-ondas,

Temperaturas elevadas ou baixas podem causar diferentes tipos de consequências com: desidratação; erupção da pele; câimbras; fadiga física; as temperaturas baixas causam feridas; rachaduras e necrose na pele; doenças reumáticas.

Muitas atividades os colaboradores estão exposto a pressões ambientais acima ou abaixo das pressões normais, diferente da pressão atmosférica a que normalmente estamos acostumados diariamente. A exposição a pressões anormais pode causar a ruptura do tímpano quando o aumento de pressão for brusco e a liberação de nitrogênio nos tecidos e vasos sanguíneos e morte.

Lugares em que as atividades ou local de excussão de trabalho sejam em locais alagados, com umidade, situações em que colocam o colaborador nesta situação, podem ter problemas que agravam a saúde do mesmo, à umidade pode ocasionar doenças do

aparelho respiratório, quedas, doenças de pele, doenças circulatórias, entre outras.

O perigo da química está quando o colaborador está exposto ao manipular produtos químicos que podem causar danos físicos ou prejudicar a saúde. Os danos físicos relacionados à exposição química vão desde irritação na pele e olhos, passando por queimaduras leves, chegando até podendo causar incêndio ou explosão. Os danos à saúde podem advir de exposição de curta ou longa duração o contato de produtos químicos tóxicos com a pele e olhos e também a inalação de seus vapores, podem resultar em doenças respiratórias crônicas, doenças do sistema nervoso, doenças nos rins e fígado, e até mesmo alguns tipos de câncer.

Os riscos biológicos ocorrem por meio de micro-organismos onde em contato com o homem, podem provocar inúmeras doenças. Muitas atividades profissionais podem ocasiona para que o colaborador por sua vez se contamine. É os casos de indústrias de alimentação, hospitais, limpeza pública, laboratórios, entre outros. As doenças em que os colaboradores estão em riscos são: tuberculose, brucelose, malária, febre amarela.

Os riscos ergonômicos: esforço físico, levantamento de peso, postura inadequada, controle rígido de produtividade, situação de estresse, trabalhos em período noturno, jornada de trabalho prolongada, monotonia e repetitividade, imposição de rotina intensa, podendo deixar o colaborador com problemas físicos e psicológicos.

Os principais riscos mecânicos em que os colaboradores estão expostos as atividades de trabalho, quando essas atividades dependem de maquinarias os cuidados devem ser maiores, onde a maioria dos acidentes acontece quando a proteção é ínfima, quando as condições de trabalho são precárias, erros de comando, ferramentas em mal estado e falta de manutenção. As principais consequências que o colaborador pode enfrentar são: arrastamento, aprisionamento, corte, decepamento, esmagamento, choque, perda de estabilidade ou perfuração.

Manter a organização fora dos riscos:

- O cumprimento das normas de segurança.
- A disponibilidade e uso adequado de equipamentos de proteção.
- Programas de treinamento.
- Manutenção preventiva de equipamentos de trabalho.
- A disponibilidade de extintores e outros dispositivos de combate a incêndios.
- Treinamento de combate a incêndio e em situações de emergência.
- Mapa de risco obrigatório e sinalização adequada das áreas de riscos e das rotas de fuga.
- A disponibilidade de sistema de emergência.
- Planos de contenção quando ocorrem situações de emergência (derramamentos, vazamentos, contaminações, explosões).

- Planos de emergência para enfrentar situações críticas como falta de energia elétrica, água, incêndio e inundações.
- Sistema de registro dos testes de segurança e desempenho dos equipamentos de urgência.

O estudo e o Gerenciamento dos riscos

Em geral o estudo de risco se inicia em quatro fases importantes para seu objetivo final, sendo:

1. Identificação das fontes de perigo
2. Estimativa da resposta do perigo
3. Estimativa da exposição
4. Caracterização do risco

O estudo de risco separado do gerenciamento de risco e baseado em cima dos dados de risco recolhidos, todas as informações adquiridas são importantes para o desenvolvimento de opções alternativas para o desenvolvimento das soluções dos riscos envolvidos. Para a consultoria avaliar à estimativa dos riscos, os resultados da análise de probabilidades e consequências são sobrepostos, assim obtêm a classificação do risco, definindo sua origem, a probabilidade de acontecer e as consequências geradas do perigo.

Independente do seguimento das organizações, tendo um porte pequeno, médio ou grande, os riscos estão presentes, mas o importante é reduzir o mínimo o nível do risco, planejar corretamente para que não aconteçam acidentes que podem trazer grandes prejuízos, neste caso a análise de risco, busca a informação e detecta o perigo existente.

Os objetivos de detectar os riscos que as organizações estão expostas, ajuda com que o rendimento e a produtividade do trabalho sejam progressivos e com que a empresa não tenha perdas, reduzindo quando os riscos já estão presentes nas empresas. Os riscos aumentam a degradação pelo trabalho, diminui a produtividade e, em consequência, a qualidade final do produto.

RISCOS AMBIENTAIS

GRUPOS								
AGENTES QUÍMICOS	I VERVELHO	POEIRA	FUMOS METÁLICOS	NÉVOAS	VAPORES	GASES	PRODUTOS QUÍMICOS EM GRAL	SUBSTÂNCIAS COMPOSTOS OU PRODUTOS QUÍMICOS EM GERAL
AGENTES FÍSICOS	II VERDE	RUÍDO	VIBRAÇÃO	RADIAÇÃO IONIZANTE E NÃO IONIZANTE	PRESSÕES ANORMAIS	TEMPERATURAS EXTREMAS	FRIO CALOR	UMIDADE
AGENTES BIOLÓGICOS	III MARROM	VÍRUS	BACTÉRIA	PROTOZOÁRIOS	FUNGOS	BACILOS	PARAZITAS	INSETOS, COBRAS, ARANHAS, ETC
AGENTES ERGONÔMICOS	IV AMARELO	TRABALHO FÍSICO PESADO	POSTURA INCORRETAS	TREINAMENTO INADEQUADO INEXISTENTE	JORNADAS PROLONGADAS DE TRABALHO	TRABALHO NOTURNO	RESPONSABILIDADE E CONFLITO TENSÕES EMOCIONAIS	DESCONFORTO MONOTONIA
AGENTES MECÂNICOS	V AZUL	ARRANJO FÍSICO DEFICIENTE	MAQUINAS SEM PROTEÇÃO	MATÉRIA PRIMA FORA DE ESPECIFICAÇÃO	EQUIPAMENTOS INADEQUADOS DEFEITUOSOS OU INEXISTENTES	FERRAMENTAS DEFEITUOSAS INADEQUADAS OU INEXISTENTES	ILUMINAÇÃO DEFICIENTE ELETRICIDADE	INCÊNDIO EDIFICAÇÕES ARMAZENAMENTO

Leis e Normas

De acordo com a PORTARIA MTB Nº 3.214, DE 08 DE JUNHO DE 1978, NR-9 é necessário que todas as organizações estejam dentro da norma para evitar tipos de acidentes que possam trazer prejuízos para as mesmas.

9.1. Do objeto e campo de aplicação.

9.1.1. Esta Norma Regulamentadora - NR estabelece a obrigatoriedade da elaboração e implementação, por parte de todos os empregadores e instituições que admitam trabalhadores como empregados, do Programa de Prevenção de Riscos Ambientais - PPRA, visando à preservação da saúde e da integridade dos trabalhadores, através da antecipação, reconhecimento, avaliação e consequente controle da ocorrência de riscos ambientais existentes ou que venham a existir no ambiente de trabalho, tendo em consideração a proteção do meio ambiente e dos recursos naturais. (109.001-1 / I2)

9.1.2. As ações do PPRA devem ser desenvolvidas no âmbito de cada estabelecimento da empresa, sob a responsabilidade do empregador, com a participação dos trabalhadores, sendo sua abrangência e profundidade dependentes das características dos riscos e das necessidades de controle. (109.002-0 / I2)

9.1.5. Para efeito desta NR, consideram-se riscos ambientais os agentes físicos, químicos e biológicos existentes nos ambientes de trabalho que, em função de sua natureza, concentração ou intensidade e tempo de exposição, são capazes de causar danos à saúde do trabalhador.

9.1.5.1. Consideram-se agentes físicos as diversas formas de energia a que possam estar expostos os trabalhadores, tais como: ruído, vibrações, pressões anormais, temperaturas extremas, radiações ionizantes, radiações ionizantes, bem como o infrassom e o ultrassom.

9.1.5.2. Consideram-se agentes químicos as substâncias, compostos ou produtos que possam penetrar no organismo pela via respiratória, nas formas de poeiras, fumos, névoas, neblinas, gases ou vapores, ou que, pela natureza da atividade de exposição, possam ter contato ou ser absorvido pelo organismo através da pele ou por ingestão.

9.1.5.3. Consideram-se agentes biológicos as bactérias, fungos, bacilos, parasitas, protozoários, vírus, entre outros.

NR 9.2.1 O Programa de Prevenção de Riscos Ambientais deverá conter, no mínimo, a seguinte estrutura:

a) planejamento anual com estabelecimento de metas, prioridades e cronograma; (109.003-8 / I1)

b) estratégia e metodologia de ação; (109.004-6 / I1)

c) forma do registro, manutenção e divulgação dos dados; (109.005-4 / I1)

d) periodicidade e forma de avaliação do desenvolvimento do PPRA. (109.006-2 /I1)

Bibliografia

Leis - NR 9 - PROGRAMA DE PREVENÇÃO DE RISCOS AMBIENTAIS (109.000-3). Disponível em < http://www010.dataprev.gov.br/sislex/paginas/05/mtb/9.htm>

Informações sobre a biossegurança. Disponível em < http://www.fiocruz.br/biosseguranca/Bis/StartBIS.htm>

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

Claudio Peixoto

Brasileiros se reúnem para combater a FRAUDE

ACFE
Association of Certified Fraud Examiners

Claudio Peixoto é diretor de investigação da Ernest & Young Terco e presidente da ACFE – Association of Certified Fraud Examiners Brasil, a maior organização do mundo de combate à fraude, contando com mais 55 mil membros em todo o mundo, composto por investigadores de fraudes, contadores, auditores, advogados, empresários, professores, onde engloba e associam seus conhecimentos para enriquecer os conhecimentos de todos e gerando novas oportunidades para acabar com a fraude nas organizações, com a experiência de todos a facilidades de desenvolver o combate à corrupção é eficaz.

Em fevereiro de 2011, um grupo que já participava do programa resolveram trazer a associação para o Brasil, criando uma filial com o mesmo objetivo, além de ensinar novos associados a praticar a anticorrupção e a antifraude. Fundada com 60 associados, hoje a associação já conta com 185, todos com a mesma intuição, o número de associados é favorável no crescimento da ACFE no Brasil, o caminho está correto com os conhecimentos dos membros da associação, formalizando recursos e ferramentas para a descoberta da frauda antes que aconteça e traga prejuízos às organizações.

No exterior a ACFE já existe há mais tempo e neste ano abriu seu Capítulo no Brasil. Qual o principal objetivo da associação e o que representa a abertura do Capítulo brasileiro?

Em 1988, Joseph T. Wells decidiu criar o ACFE com o principal objetivo de compartilhar o seu vasto conhecimento na prevenção e combate à fraude, como consequência, muitos profissionais

"a melhor forma de prevenir fraudes dentro de uma empresa é o exemplo que vem da alta administração"

se capacitaram e hoje, os EUA possui um ótimo índice sobre a percepção global da fraude (7,1) dessa forma, nós acreditamos que a criação do capitulo brasileiro contribua, no médio e longo prazo, para melhorar a percepção global da corrupção no Brasil, que atualmente é de 3,7, à medida que cada vez mais profissionais se tornem capazes de auxiliar as empresas onde trabalham na prevenção e combate a fraude.

Mundialmente a ACFE possui mais de 55.000 associados e oferece diversos tipos de suporte ao mercado. Quais são as principais ações e metas previstas para o Brasil?

Acreditamos que em breve disponibilizaremos uma série de treinamentos para nossos associados com o objetivo principal de combater fraudes nas empresas, incluindo treinamentos preventivos e treinamentos detectivos, isso inclui uma parceria que já está em desenvolvimento com uma das melhores universidades do País e a realização de um congresso sobre o combate a fraudes em 2012. Adicionalmente, pretendemos trabalhar em conjunto com outras organizações, como órgãos de classe relacionados (ex.: OAB, CRC e outros) para conscientizar esses profissionais e tornarmos ponto de referencia para apoia-los nos diversos programas de combate a fraude e, caso necessário, ajuda-los em investigações especificas e/ou em questões legais.

Como a ACFE ajuda as organizações no combate às fraudes?

Como ela pretende atingir o seu público-alvo? Atualmente a ACFE reúne um grupo seleto de profissionais. Pretendemos fomentar a interação desses profissionais através do compartilhamento de experiências exposição de temas relevantes por profissionais de destaque no combate a fraude, portanto acreditamos que atingiremos os objetivos de nossos associados capacitando-os a combaterem às fraudes dentro das organizações.

A capacitação e o adequado preparo são importantes aliados no combate às fraudes. O que a ACFE oferece aos interessados no sentido da capacitação profissional?

Em breve, disponibilizaremos um programa de estudo para obtenção da certificação em exame de fraudes (CFE) que atestará a capacidade técnica do profissional na prevenção e no exame de fraudes. Esse certificado tem reconhecimento internacional e inclui conhecimentos de técnicas forenses, contabil-financeiro, legislação e ética.

Qual a melhor forma de prevenir fraudes dentro das empresas?

Acredito que a melhor forma de prevenir fraudes dentro de uma empresa é o exemplo que vem da alta administração. Nenhuma empresa onde a alta administração age de maneira questionável pode esperar uma conduta diferente de seus funcionários, mas isso isoladamente não previne fraudes, portanto recomendo a criação e manutenção de um programa de combate a fraudes que contemple pelo menos as seguintes atividades: conscientização continua de todos os funcionários, monitoramento do ambiente de controles, disponibilização de um canal de comunicação de situações suspeitas, com a possibilidade de denuncias anônima e apuração de todas as denuncias, aplicação das sanções cabíveis ao fraudador, aprimoramento do ambiente de controles internos.

As forças motivadoras fazem com que as algumas pessoas apliquem fraudes. Quais são os principais fatos geradores da ocorrência de fraudes nas organizações?

Segundo Donald Cressey, há três principais fatos geradores da ocorrência de fraude nas organizações:

1) pressão, que pode ser a pressão financeira, metas abusivas, pressão social, ou ate mesmo vícios, como jogos, drogas e outros.

2) oportunidade, observamos que o fraudador é uma pessoa que possuía confiança, autoridade para agir, e abusando desses poderes, decide

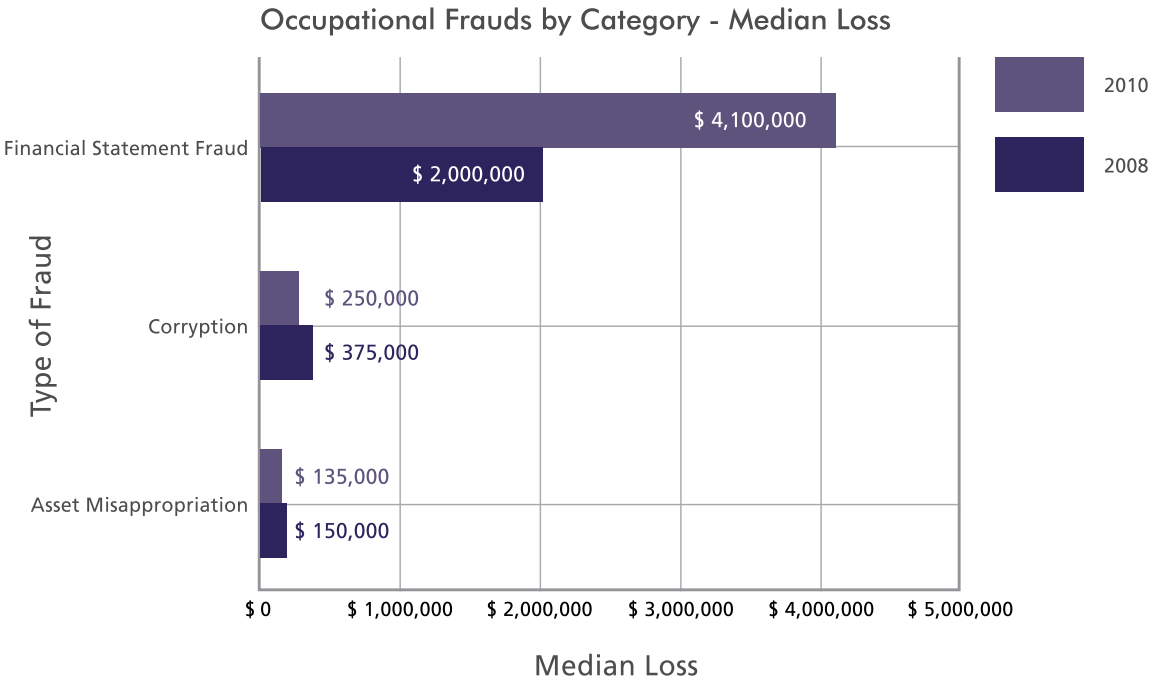
3) racionalizar o ato fraudulento, falsificando documentos que suportem a fraude, obtendo vantagens para si ou para um determinado grupo.

Como reconhecer um fraudador dentro da empresa?

Observamos algumas características comuns aos fraudadores, porém precisamos ter a consciência de que essas caracterizam não são evidencias de fraude, mas apenas um alerta: Estilo de vida incompatível com sua renda, vícios, tais como jogo, drogas, álcool, problemas financeiros, insatisfação com o trabalho.

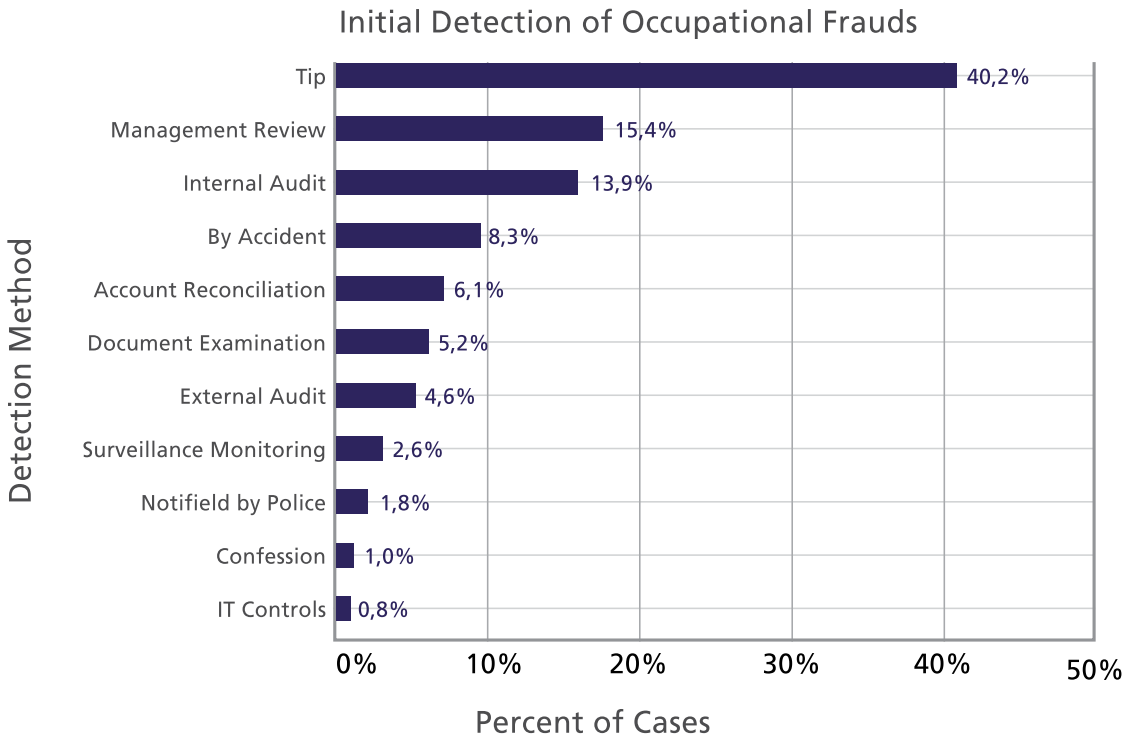
Qual o tipo de fraude que traz mais prejuízos para as organizações?

Segundo pesquisa global realizada pelo ACFE em 2010, as fraudes nas demonstrações financeiras ultrapassam, na média, USD 4bilhões em 2010.



Qual a forma mais ágil de detectar uma fraude?

Segundo pesquisa global realizada pelo ACFE em 2010, 40% das fraudes detectadas foram através do canal de denúncias.



Qual o golpe mais aplicado nas organizações quando o fraudador é um colaborador?

Nossas pesquisas indicam que o tipo de fraude mais cometida nas organizações são as relacionadas à corrupção, que contempla os conflitos de interesse; pagamento de propina; gratificações ilegais; falsificação de licitações.

Qual o perfil do fraudador de empresas? Que medidas eficazes podem ser tomadas para identificá-los e inibir sua ação?

Tipicamente, o perfil do fraudador é: homem, com idade entre 36 e 45 anos, trabalha na área contábil ou operacional, porém as principais características comportamentais do fraudador são: Viver além de suas posses; dificuldades financeiras; dificuldade em compartilhar tarefas; problemas familiares; recusam-se a tirar férias; excesso de pressão, entre outras.

Entre apurar uma fraude até as últimas consequências e pensar na preservação da imagem institucional o que os administradores devem fazer?

Essa é uma pergunta muito interessante, pois muitos administradores tem essa dúvida. Até que ponto apurar a fraude compromete a imagem institucional da empresa? Entendo que em todos os casos, sem exceção, a empresa deve apurar a fraude justamente para poder preservar sua imagem institucional. Quando uma empresa deixa de apurar uma suspeita de fraude, ela passa uma mensagem para seus colaboradores (internos e externos) que não esta preocupada com

"No início dos anos 1920, Charles Ponzi iniciou um esquema onde utilizava o dinheiro de novos investidores para remunerar os investidores mais antigos, esquema esse conhecido no Brasil como "pirâmide" e mundialmente conhecido como "esquema Ponzi"

a questão e que tolera atitudes como essa, assim os demais colaboradores podem entender que não serão punidos por cometer atos ilícitos, portanto apurar a fraude significa preservar a imagem institucional da empresa e transmite o nível de tolerância a atos ilícitos para todos seus colaboradores.

E as fraudes conhecidas como golpes populares. Porque, mesmo batidas, elas se perpetuam?

Essa é uma pergunta interessante, uma característica comum às fraudes ocorridas nas empresas e os golpes populares é a confiança que é depositada no fraudador. No início dos anos 1920, Charles Ponzi iniciou um esquema onde utilizava o dinheiro de novos investidores para remunerar os investidores mais antigos, esquema esse conhecido no Brasil como "pirâmide" e mundialmente conhecido como "esquema Ponzi". As pessoas entregavam dinheiro a Charles Ponzi, pois confiavam nele. Essa fraude foi mundialmente divulgada. Recentemente, observamos a aplicação do mesmo esquema por Bernard Madoff numa fraude bilionária com perdas superiores a USD 18 bilhões. As pessoas deixaram ser enganadas, pois confiaram nos fraudadores, iludidos por um ganho relevante e rápido.

Na sua visão em que medida leis ou regulamentos anticorrupção (FCPA - Foreign Corruption Practices Act/EUA) e antilavagem de dinheiro (Lei 9.613/98 Brasil), por exemplo, ajudam a inibir a ação dos fraudadores?

Acredito que o que mais contribui para inibir a ação dos fraudadores é a ação dos órgãos reguladores, por exemplo, o Departamento de Justiça americano (DOJ) vem, a cada ano, intensificando as ações de fiscalização. No Brasil, o DRCI também vem intensificando seus trabalhos e firmando acordos bilaterais para recuperação de ativos com origem ilícita.

Como atual Presidente do ACFE/Brasil, como você imagina que estará a associação no Brasil daqui a 5 anos?

Estamos confiantes que a nossa associação será capaz de influencias positivamente nosso ambiente corporativo, suportando as organizações na prevenção e no combate às fraudes, dessa forma, gostaria que o nosso país passasse a ser reconhecido internacionalmente como um país que combate esse tipo de crime.

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

Ana Paula Deodato

Ação de Gestão de Riscos no Metrô de Belo Horizonte

Saiu na última edição do jornal interno Acontece Metrô BH, uma nota sobre a Ação de Gestão de Riscos, que a empresa irá adotar no Plano Estratégico em 2012. Antonio Celso Ribeiro Brasiliano participou da reunião que escolheu o projeto piloto das estações Eldorado e Central, onde serão implantadas em todas as 19 estações.

Brasiliano esclareceu relatos importantes para o Plano Estratégico, onde os trabalhos de consultoria estão em fase final de detalhamento. "Já foram elencados os principais riscos e as medidas de contingência necessárias. Agora é definir prazos e atribuir responsáveis, que trabalharão em planos de ação específicos por área, permitindo que cada um deles seja devidamente tratado e que a classificação dos riscos emergentes seja priorizada, monitorada e requalificada permanentemente".

Além do presidente do Comitê, Alexandre Resende, lembrar o apoio da Superintendência no acompanhamento das ações e também destacou que a utilização do mapeamento, como ferramenta complementar à elaboração do planejamento estratégico, dará maior efetividade à implementação e cumprimento da política de gestão do risco.

Lançamento dos livros

Noite de autógrafos - Guia Prático para a Gestão de Continuidade de Negócios – GCN e As fraudes contra as Organizações e o papel da Auditoria Interna

Antonio Celso Ribeiro Brasiliano junto com o Professor Humberto Ferreira Orlá Filho, lançaram seus livros na Livraria Cultura do shopping Market Palce, São Paulo, no dia 27 de Julho. Brasiliano, lançou Guia Prático para a Gestão de Continuidade de Negócios – GCN -, com o principal objetivo de criar, manter ou incorporar um plano de ação dentro das organizações, um Guia completo com todas as informações que as organizações precisam estar por dentro da Gestão de Continuidade de Negócios eficaz, com um processo lógico, além do guia trazer uma fácil capacidade de formular um gerenciamento completo, abordando diferentes acontecimentos para uma elaboração ativa PCN, que ajudará o Gestor a ter uma linguagem fácil e didática para seus conhecimentos e aprendizagem.

Ana Paula Deodato

A obra do Humberto, **As fraudes contra as Organizações e o papel da Auditoria Interna**, tem como objetivo chegar às organizações a informações que as fraudes podem ser evitadas juntamente a uma Auditoria Interna eficiente, que tem a principal função de prevenir qualquer tipo de fraude que possa estar dentro das organizações, detecta-las antes do prejuízo, o auditor precisa de um instrumento de controle, bem como uma administração cumprindo suas estratégias, projetos e metas.

A noite foi teve um exclusivo lançamento com autógrafos com os autores, que receberam convidados e amigos, que fizeram deste evento uma grandiosa noite, além do lançamento, o autor Humberto Ferreira Oríá Filho, palestrou sobre As Fraudes Contra as Organizações e o Papel da Auditoria Interna, ressaltando itens como: Missão da Auditoria, Riscos que estão nas organizações, Fraude: conceitos, fraudes rotineiras, hipótese de ocorrência, Identificação das fraudes, características do fraudador, detecção da fraude pela auditoria interna e outros itens que fizeram a diferença na palestra, confira as fotos!

Cursos

Curso de Extensão em Gestão de Riscos e Compliance

Foram realizados na Faculdade FESP/FAPI, no final do mês de julho dois diferentes cursos, nos dias 27, 28 e 29 de julho Curso de Exensão em Gestão de Riscos e Compliance, ministrado pelo professor Nilton dos Santos, com o principal objetivo de certificar os alunos no estudo do processo de gestão de riscos e o campo de complice, a integração de conhecimentos para contribuir na governança corporativa.

O programa do curso tratava de assunto que enriqueceram os conhecimentos de todos que participaram, abordando os principais assuntos: Contextos e conceitos de Gestão de Riscos, Compliance,

Ana Paula Deodato

Governança Corporativa, Ética nas organizações; Conceito e aplicações da Gestão de Riscos Corporativos, com a visão da ISO 31000: estrutura da gestão de riscos integrada, identificação, análise e avaliação de riscos, plano de resposta aos riscos, monitoramento de riscos; Sistema de Controles Internos: função do sistema de controles internos, metodologia para análise do ambiente do controle interno; COSO, autogestão de controles – CSA – Control Self Assessment; Função de Compliance: Teoria da conformidade, compliance em instituições financeiras e não financeiras, programa de compliance, abrangência do programa, compliance e direitos humanos; Regulações Nacionais e Internacionais: SOX, Basiléia, Resoluções do BACEN, entre outras; Fronteiras do Compliance: auditoria, jurídico, ombudsman, controles internos e riscos corporativos; Estudo de casos: análise de dados e discussão das estruturas de gestão de riscos e compliance.

A Brasiliano & Associados contou com a participação das empresas: Tecban; Moto Honda; Accor Hotéis; Petrobras; Copel; Total distribuidora; Promon Engenharia e Anglo Ferrous.

Curso de Extensão em Como Proteger as Organizações dos Riscos Corporativos

Nos dias 28 e 29, o profissional na área de comunicação, Flávio Schmidt, forneceu aos interessados, o Curso de Extensão em Como Proteger as Organizações dos Riscos Corporativos e Acabar com as Crises de Comunicação, a finalidade principal desses dois dias de curso foi capacitar o profissional na área de comunicação que atuam nos níveis de direção, gerenciais ou na administração interna e externa de uma organização, focalizando também diretores e executivos que operam na área marketing, vendas,

Ana Paula Deodato

mercado, administração, administração de recursos humanos e nas áreas específicas de engenharia, segurança, planejamento estratégico e gerenciamento de continuidade de negócios, controle de riscos e desastres, meio ambiente e sustentabilidade.

O professor dividiu o curso no primeiro dia passando contextos; definições; modelo e desenvolvimento de crise; o gerenciamento tradicional da crise e estudo de cases. No segundo dia Flávio, finalizou o curso com um programa de prevenção de crises; o círculo – mapeamento dos riscos, definição de cenários, riscos potenciais, medidas preventivas, elaboração de procedimentos; classificação e severidade de riscos; campanha de comunicação e consulta; estratégia e manual de prevenção.

Participaram do curso as empresas: Globo; RAF Comunicação; Klabin; Graber Sistema de Segurança; HSBC; Grupo Liberdade Banco do Brasil; Condomínio Conjunto Nacional e Marconi & Associados.

Brasiliano votado como diretor na ACFE do Brasil!

No começo de fevereiro de 2011, profissional especializado em combate a fraude como advogados e auditores resolveram trazer para o Brasil, a ACFE – Association of Certified Fraud Examiners, associação criada em 1988, com a intenção de combater a fraude, hoje mundialmente participam da associação mais de 55 mil profissionais com a mesma intenção combater a fraude.

Ana Paula Deodato

Antonio Celso Ribeiro Brasilaino, foi eleitor com diretor da associação, com o maior privilegio de entrar nesta entidade para combater a corrupção e as fraudes que atingem as organizações de todo o Brasil. Ás entidades, organizações e associações estão investindo para a prevenção e investigações que estão cada vez maiores para acabar com essas fraudes.

1° Congresso de Combate e Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo

Nos dias 26 e 27 de setembro a FEBRABAN – Federação Brasileira de Bancos realiza o 1° congresso de combate e Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, em São Paulo.

As melhores práticas de prevenção à lavagem de dinheiro e ao financiamento do terrorismo nas instituições reguladas, avaliação do poder judiciário e do GAFI sobre as ações de PLD no Brasil e o resultado das investigações e das fiscalizações sobre o crime de lavagem de dinheiro, são alguns dos temas que estarão em debate.

Os participantes terão a oportunidade de fazer perguntas e tirar dúvidas sobre a PLD com os representantes do Banco Central, do COAF, da CVM e da SUSEP.

Confira alguns palestrantes confirmados: Joaquim da Cunha Neto, Coordenador-Geral de Análise – COAF: Conselho de Controle de Atividades Financeiras; Roberto Troncon Filho, Superintendente – DPF SP: Departamento da Polícia Federal em São Paulo; Carlos Donizeti Macedo Maia, Chefe do DESUP: Departamento de Supervisão de Bancos e Conglomerados Bancários – Banco Central do Brasil.

Acesse HYPERLINK www.febraban.org.br e confira a programação! Faça sua inscrição até 31/08 e garanta 20% de desconto!

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

Engenharia Social – A Arte de Enganar

Egle Dorminda Cascino | Pós-graduada em Gestão de Tecnologia da Informação, cursando MBA em gestão de Riscos e Fraudes Empresariais pela Brasiliano & Associados (FAPI). egledc@hotmail.com e Wander Steves Carbone | Formado em Administração de empresas pela UNIP, cursando MBA em gestão de Risco e Fraudes Corporativas pela Brasiliano & Associados (FAPI) wscarbone1@gmail.com

Resumo

A engenharia social é um dos meios mais utilizados na obtenção de informações sigilosas e importantes, tudo isso se torna mais fácil porque ela explora com muita sofisticação as "falhas de segurança dos humanos" enquanto as empresas investem fortunas em tecnologias de segurança de informações e protegem fisicamente seus sistemas, mas a maioria ainda não possui métodos que proteja seus funcionários das armadilhas dos engenheiros sociais, estes ataques são muito frequentes e não apenas pela internet, mas no dia-a-dia das pessoas, uma vez que ainda nos tempos de hoje mesmo com toda tecnologia o método mais simples, eficiente e mais utilizado ainda é o de "perguntar", na maioria das vezes, o engenheiro social se aproxima da vitima, faz perguntas sem maiores objetivos ou mantém conversas despretensiosas, apenas com o intuito de ganhar a confiança da outra parte, então somente depois que já se estabeleceu a relação de confiança é que o engenheiro parte para obter as informações que realmente lhe interessam, existem vários perfis de engenheiros sociais, várias ferramentas e métodos utilizados pelos mesmos, mas também existem várias formas e maneiras de nos protegermos destes ataques.

Introdução

Com o crescente avanço da tecnologia, as empresas têm despendido boa parte do tempo e muitos investimentos em TI para solucionar os problemas técnicos de segurança, preocupando-se com a proteção de seus sistemas contra os ataques de hackers e novos vírus que possam surgir. Porém, esquecem-se das informações que estão de posse dos seus empregados, que, via de regra, não recebe treinamento, política de segurança ou qualquer outro mecanismo que sirva de proteção contra o ataque de engenheiros sociais.

Neste artigo, apresentaremos o que é a engenharia social, como ela se apresenta no nosso cotidiano, qual o perfil do engenheiro social e as ferramentas por ele utilizadas. Bem como a arte do engenheiro social, suas formas de abordagem e suas artimanhas.

Desenvolvimento

A Engenharia Social

Antes de entendermos como a engenharia social funciona, é fundamental compreender o seu conceito, bem como o conceito de informação.

Conceito de Informação

É de suma importância definir "o que é informação", pois se as definições forem vagas, haverá espaço para diversas interpretações da legislação dos direitos autorais da informação, prejudicando os reais autores.

Informação, segundo o Aurélio, significa: "ato ou efeito de informar ou informar-se; dados acerca de alguém ou de algo; conhecimento, participação; comunicação ou notícia trazida ao conhecimento de uma pessoa ou do público; instrução ou direção".[1]

Para as organizações, as informações têm grande representatividade, estão contidas em relatórios financeiros, de produtividade, de desempenho, nos fluxos e processos operacionais, nas campanhas de lançamento de novos produtos, "nos segredos" de fabricação. Permeiam, portanto, todo o ambiente corporativo, apresentando-se em papel, em arquivos eletrônicos ou simplesmente arquivados na mente das pessoas que participam da cadeia produtiva das empresas (Empregados, parceiros, fornecedores, entre outros). Porém, são negligenciadas pelas organizações, uma vez que a maioria das pessoas que as manipulam desconhecem o seu real valor ou a melhor maneira de defendê-las.

Definição de Engenharia Social

Podemos dizer, em linhas gerais, que engenharia social é o termo utilizado para designar a obtenção de informações importantes de uma empresa, através de seus usuários e colaboradores. Essas informações podem ser obtidas pela ingenuidade ou confiança. Em outras palavras, a engenharia social pode ser considerada a "arte de enganar", iludir ou persuadir pessoas. Os engenheiros sociais são perspicazes, e através dos diversos perfis da psicologia humana, conseguem encontrar "os pontos fracos" de suas vítimas, alcançando seus objetivos.

Engenharia Social "é a arte de coletar informações de indivíduos inocentes, perguntan-

1 Aurélio Buarque de H. FERREIRA, Novo Dicionário Básico da Língua Portuguesa, p. 361

do-lhes questões aparentemente inofensivas ou fingindo ser alguém que não é".[2]

Engenharia porque constrói táticas de acesso a sistemas e informações sigilosas de forma indevida; social porque se utiliza de seres humanos que, por natureza, são gregários, vivendo e trabalhando em grupos organizados.

Perfil Do Engenheiro Social

O engenheiro social geralmente é uma pessoa educada, cordial, solícita, agradável, carismática, envolvente, determinado, curioso e altamente criativo. É um bom observador, conhece as facetas humanas, sabe reconhecer a melhor forma de abordagem, sendo paciente na espera do momento oportuno para o ataque. É uma "arte" que pode ser utilizada, tanto para o bem quanto para o mal, existem pessoas que, para cumprirem sua rotina de trabalho diária com bom desempenho, necessitam receber treinamentos específicos a fim de adquirirem formação técnica nessa arte. "Entre eles podemos citar os investigadores dos comandos especiais da polícia, detetives particulares, agentes especiais do governo, entre outros".[3] Existem outros, que desenvolvem ou aperfeiçoam suas habilidades pessoais para aplicar golpes, tirarem vantagem ou, simplesmente, se exibirem perante suas comunidades. "Mas, dentro do contexto da engenharia social, dois personagens merecem destaque: Frank W. Abagnale Jr. e Kevin D. Mitnick."[4]

Frank William Abagnale Jr. ficou famoso por tornar-se o maior fraudador e falsário da história dos Estados Unidos. Conseguindo roubar milhões de dólares através de cheques falsificados com perfeição, também se passou por professor, piloto de avião, médico e advogado. Após ser preso, foi recrutado para trabalhar no setor de fraudes do FBI. Posteriormente, tornou-se um dos melhores e mais bem pagos consultores de segurança contra fraudes.

Kevin David Mitnick considerado um dos "cibercriminosos" mais famosos, responsável pela invasão de diversos computadores como, Motorola, Novell, Nokia, Sun Microsystems e da Universidade da Califórnia, entre outros. Aos 25 anos de idade, foi condenado a um ano de prisão por invasão de sistema e furto de software da DEC. Ao sair da prisão, continuou a cometer invasões, e como estava sendo vigiado pelas autoridades, resolveu "desaparecer", utilizando-se de identidade falsa. Em 1995, foi novamente apanhado pelo FBI, graças a engenhosidade de Tsutomu Shimomura, um grande especialista em segurança do Centro Nacional de Supercomputadores de San Diego, que teve seu computador pessoal (que estava conectado via Internet com o Centro Nacional) invadido por Mitnick. Cumpriu cinco anos de prisão, até 2000, quando foi liberado com a condição de manter-se longe de computadores, celulares e telefones

2 Dan VERTON, Confissões de Hackers Adolescentes, p. 20

3 Idéia extraída do livro a Arte de Hackear Pessoas de Antonio Marcelo e Marcos Pereira, p. 5 e 6

4 Mário César P. PEIXOTO, Engenharia Social e Segurança da Informação, p 5

portáteis pelo período de três anos. Atualmente, é consultor de segurança para corporações em vários países e co-fundador da Defensive Thinking, empresa de consultoria em Los Angeles.

Suas Ferramentas e Aplicações[5]

Muitas são as táticas e artifícios aplicados para se obter acesso indevido às informações, estejam elas em meios eletrônicos, impressas ou armazenadas em qualquer outro formato. Para tanto, o engenheiro social faz uso de suas habilidades pessoais e de algumas ferramentas como as descritas abaixo:

- Telefone ou VOIP
- Internet
- Intranet
- E-mail
- Chats
- FAX
- Cartas / correspondências
- Lixos (Vasculha documentos)
- Pessoalmente
- P2P (Peer-to-Peer)
- "Surfar" sobre os ombros

5 Baseado no livro: Mário César P. PEIXOTO, Engenharia Social e Segurança da Informação, p 5 a 7

Percebemos que dois fatores favorecem o sucesso da engenharia social. São eles: a falta de consciência das táticas de engenharia social utilizadas e o excesso de autoconfiança das pessoas, por não se considerarem ingênuas a ponto de serem manipuladas.

Formas Usuais de Abordagens

Da mesma forma como as tecnologias tem evoluído ao longo dos anos, o mesmo ocorre com a engenharia social, que passa por constantes transformações a fim de manter seu caráter inovador, responsável pela conquista de seu objetivo. Mas, apesar da necessidade de inovações na arte de enganar, o engenheiro social utiliza-se de alguns aspectos clássicos de ataques, como os descritos a seguir:

- Ataque Direto
- Criando a confiança
- Posso Ajudar?
- Você Pode Me Ajudar?

Assim, fica cada vez mais evidente que não se pode depender apenas da proteção de firewalls de rede como meio de salvaguardar as informações. Pois a maior vulnerabilidade, nos ambientes empresariais, está no elo mais fraco – as pessoas, e para elas a melhor proteção é conscientização e treinamento.

Engenharia Social na Internet

A Internet é uma grande aliada dos engenheiros sociais, que a utilizam para coleta de dados ou para incrementar a finalização de ataques, através de sites clonados, e-mails falsos, salas de bate-papo. Para evitar que o atacante se utilize desses artefatos, e através de programas maliciosos domine a sua máquina, esteja atento: não abra anexos ou clique em links sem ter certeza

absoluta da sua procedência. Sempre que estiver navegando, ou seja, visitando algum site, verifique se a conexão está autenticada e criptografada. Muito cuidado com a questão de segurança, sites de WEB que não utilizem um protocolo seguro, não são passíveis de receber informações confidenciais, tais como endereço, telefone, nome, número de cartões de crédito, entre outras.

Ao falarmos de segurança no ambiente da Internet existe outra regra básica a ser lembrada: ter um antivírus instalado, deixando também o firewall ativado, que deverá ser atualizado diariamente. Digamos que completamente seguro ninguém está, mas podemos dificultar a entrada de vírus, trojans e outros inconvenientes, a fim de preservarmos um pouco a privacidade dos dados que julgamos ser confidenciais.

O CERT.br (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil), em sua Cartilha de Segurança para Internet, parte IV[6], aborda o tema Fraudes na Internet, explicando que devido à dificuldade em atacar e fraudar dados em um servidor de uma instituição bancária ou comercial, os atacantes concentram esforços na exploração de fragilidade dos usuários para realizar fraudes através da Internet.. Na maioria dos casos, o usuário é induzido a instalar algum código malicioso ou acessar uma página clonada, possibilitando o furto de dados pessoais, como senhas bancárias e números de cartões de créditos.

Fraudes mais usuais via Internet:

- Scam – é qualquer tipo de esquema ou ação enganosa e/ou fraudulenta que tem como finalidade obter vantagens financeiras.
- Phishing – também conhecido como phishing scam, é uma forma de engenharia social, onde pessoas mal intencionadas se passam por outras, ou por instituições conhecidas como um banco, empresa ou sites populares procurando induzir os usuários a acessarem páginas falsificadas.
- Orkut - O atacante consegue, através do furto via phishing, o login e senha do Orkut de algum usuário e, posteriormente, deixa recados para "todos os conhecidos" dessa vítima.

Pontos Fracos Explorados Pelo Engenheiro Social

Qualquer instituição, por mais segura que esteja sempre tem um fator que pode desequilibrá-la, sempre existe um elo mais fraco: o ser humano. São essas pessoas que detêm todos os "segredos" e "macetes" desse império e estão totalmente desprotegidas e vulneráveis. E este fato não passa despercebido ao engenheiro social, ao contrário, esta é a sua ferramenta de trabalho fundamental. Enquanto os engenheiros de segurança se preocupam em "salvaguardar" os softwares e os hardwares, as informações podem estar "vazando" num simples "telefonema" feito a algum funcionário.

6 Cartilha de Segurança para Internet CERT.br disponível em http://cartilha.cert.br, acesso em 13/08/2010

Checando as Informações

Todas as organizações que primem pela segurança, tanto de suas informações quanto de seus clientes, devem executar a checagem das informações.

A maioria das empresas possui um Call Center, que detém informações cadastrais dos clientes e dos produtos que este possui. Por exemplo, o Call Center de um Banco tem em seu cadastro o número do RG, CPF, número de cartão de crédito, número da conta corrente, seu saldo bancário, sua movimentação bancária, seu endereço, entre outras informações.

No cenário corporativo temos outras vulnerabilidades que podem ser exploradas, tanto por um engenheiro social como por um funcionário insatisfeito:

- Mesas de escritório e armários abertos;
- Papéis adesivos: (post it)
- Pool de Impressoras:
- Correio Eletrônico:

Funcionário Demitido ou Insatisfeito

Um ex-funcionário, assim como funcionários insatisfeitos ou desmotivados, por se sentirem injustiçados, são fatores de risco sob o aspecto da seguridade e disponibilidade das informações internas da empresa. Sabemos que nem todos os "injustiçados" irão utilizar de seus conhecimentos referentes aos processos internos para ajustar suas diferenças com as empresas, porém as estatísticas apontam que a maior ameaça vem de dentro das organizações.

Gestão da Segurança da Informação

As ameaças e o perigo existem, e as empresas devem adotar um Programa de Segurança Empresarial, de forma abrangente, para proteger a informação como um todo, não apenas as que estão armazenadas em sistemas computacionais.

"A gestão da segurança está apresentando a arte de formular, implementar e avaliar linhas de ação multidepartamentais, referentes às interações da organização com o seu ambiente, tentando garantir o seu principal patrimônio que é a informação, para atingir seus objetivos de longo prazo, relativos a seus produtos, mercado, clientes, concorrentes, sociedade, etc". [7]

A Segurança da Informação "deve ser interpretada como a segurança física dos meios de comunicação – cabos, linhas de transmissão, ondas de radiofreqüência, links com satélites; segurança física dos meios computacionais; segurança lógica dos Sistemas de Tecnologia da Informação; a segurança do fluxo da Informação – formal ou informal e por último a segurança de quem lida – as pessoas – com informações estratégicas e críticas no que concerne ao desempenho da empresa". [8]

Os conceitos básicos da segurança são:

- Confidencialidade
- Integridade
- Disponibilidade

---

7 Texto extraído do site: http://www.trueaccess.com.br/downl_artigos/artigo%20%20atividades%20da%20gestao%20corporativa%20de%20seguranca.pdf, acesso em 26 Out 2006

8 Antonio Celso RIBEIRO BRASILIANO, A (in)Segurança nas Redes Empresariais, p. 75

"é primordial que as empresas invistam em instrução e conscientização dos funcionários sobre o real valor das informações que são geradas e manuseadas diariamente"

Devemos conhecer, também, os conceitos de ameaça e de vulnerabilidade, uma vez que a compreensão de ambas facilitará a compreensão dos incidentes de segurança, que servirão como subsídios para a análise dos riscos. As ameaças podem ser:

- Naturais
- Involuntárias
- Voluntárias

E a vulnerabilidades é o ponto onde qualquer sistema é suscetível a um ataque.

Norma Sobre Segurança

Nbr Iso / Iec 17799

O grau de dependência tecnológica que o mercado atingiu, motivou a elaboração de uma norma específica para orientar e padronizar a gestão da segurança da informação. A ela foi dado o nome de BS 7799. A Brithish Standart 7799 é uma norma de segurança da informação, sendo que a versão brasileira dessa norma é a NBR ISO / IEC 17799, homologada pela ABNT em 2001 e abrange os seguintes aspectos:

1. Política de segurança;
2. Segurança organizacional;
3. Classificação e controle dos ativos de informação;
4. Segurança de pessoas;
5. Segurança física e do ambiente;
6. Gerenciamento das operações e comunicações;
7. Controle de acesso;
8. Desenvolvimento manutenção de sistemas;
9. Gestão da continuidade do negócio;
10. Conformidade (com normas, regulamentos, legislação, etc.)

Conclusão

A potencialidade intelectual e mental, ao mesmo tempo em que ajuda a edificar e construir o império do conhecimento, também pode colocá-lo em risco iminente. Portanto, tudo é uma questão de bom senso e de ética profissional, alinhados à cultura organizacional e das regras sociais vigentes.

Por isso, é primordial que as empresas invistam em instrução e conscientização dos funcionários sobre o real valor das informações que são geradas e manuseadas diariamente, e da forma como os engenheiros sociais atuam com o objetivo de roubá-las.

Outro aspecto importante a ser ressalto sobre a segurança da informação, é que quanto mais fortes forem as barreiras físicas e lógicas de proteção, mais suscetível a empresa estará aos ataques de Engenharia Social. A Internet dividiu o nosso cotidiano entre dois mundos: o real e o virtual. Necessitamos de tecnologia para estarmos integrados ao mundo, mas essa tecnologia ao mesmo tempo em que nos faz evoluir, também pode nos prejudicar. A empresa, ao mesmo tempo em que necessita se proteger, também precisa se utilizar das inovações tecnológicas, como forma de obter vantagens competitivas, o que implica em segurança, que por sua vez demanda

investimento. Contra a Engenharia Social, não basta apenas instalar antivírus e firewalls, é necessário uma transformação cultural e organizacional na empresa, que irão refletir na conduta dos funcionários. Para isso, as empresas devem implementar um Programa de Segurança Organizacional, treinar e conscientizar seus funcionários, devendo enfatizar as maneiras pelas quais os atacantes costumam abordar suas vítimas e, quais as estratégias de proteção mais adequadas para cada tipo de ataque. Portanto, as Políticas de Segurança, assim como os procedimentos operacionais devem ser compostos por ações fáceis de serem implementadas, e que funcionem como barreiras às artimanhas dos engenheiros, a fim de que estes não consigam explorar a ingenuidade e a fragilidade dos funcionários. Os responsáveis pela segurança da informação devem estar atentos ao surgimento das novas tecnologias, para saber utilizá-las e ao mesmo tempo defendê-las, além de elaborarem um Programa de Segurança Empresarial que inclua as Políticas de Segurança, Classificação e Controle dos Ativos, Segurança das Pessoas, Segurança Física e do Ambiente, Controle de Acesso, Gestão da Continuidade do Negócio, sendo que todas essas implementações deverão estar em conformidade com a legislação vigente.

Referências

VERTON, Dan. Confissões de Hackers Adolescentes. São Paulo: Berkeley, 2002

BRASILIANO, Antonio Celso R, A (in) Segurança nas Redes Empresariais. São Paulo: Sicurezza, 2002.

PEREIRA, Marcos & MARCELO, Antonio. A Arte de Hackear Pessoas. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2005.

PEIXOTO, Mário César P. Engenharia Social e Segurança da Informação na Gestão Corporativa. Rio de Janeiro: Brasport Livros e Multimídia Ltda, 2006.

CARTILHA de Segurança para Internet, CERT.br - Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil.

Disponível em:

http://cartilha.cert.br/. Acesso em 13 Agosto 2010

Atividades de Gestão da Segurança da Informação.

Disponível em:

http://www.trueaccess.com.br/downl_artigos/artigo%20%20atividades%20da%20gestao%20corporativa%20de%20seguranca.pdf. Acesso em 26 Outubro 2006

Ler & Saber

Ana Paula Deodato

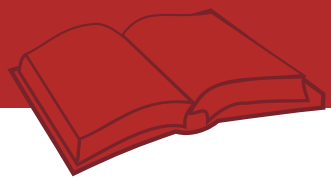
O Capital Baseado em Risco Uma Abordagem para Operadoras de Planos de Saúde

Nem todas as operadoras de saúde sabem quais são os riscos que elas estão expostas, e quando surge um imprevisto não sabem como agir. O mais importante é agir de uma forma que não prejudique seus beneficiários e nem as prestadoras de serviços, para isso é necessário que as operadoras façam um estudo dos riscos que estão expostas na operação de planos privados de assistência à saúde.

Obra de Renata Gasparello de Almeida - Mestre em Engenharia de Produção pela UFF (Universidade Federal Fluminense) - Pós-Graduada em Engenharia Econômica e Financeira pelo Latec - UFF - Graduada em Ciências Atuariais pela UFRJ (Universidade Federal do Rio de Janeiro) - Especialista em Regulação de Saúde Suplementar da Agência Nacional de Saúde Suplementar (ANS) - Representante da ANS na International Association of Insurance Supervisors (IAIS) e membro do Subcomitê Técnico de Solvência e Atuária da IAIS - Representante da ANS na Câmara Nacional de Atuária - câmara consultiva da Superintendência Nacional de Previdência Complemetar - Previc (órgão regulador dos fundos de pensões) - Membro do Instituto Brasileiro de Atuária (MIBA 1013) - Membro do Instituto dos Actuários Portugueses (reg 609).

Todas as informações necessárias estão nesta obra que foi elaborada através de muita pesquisa e conhecimentos para que o leitor fique ciente de todos os riscos, e das informações complementares que ajudam no desenvolvimento desse tipo de organização.

Ler & Saber



Editora Sicurezza, trazendo a informação!!
CONFIRA AS PUBLICAÇÕES

Coleção Auditoria e Fraude

- As Fraudes contras as Organizações e o papel da Auditoria Interna

Coleção Cenários Prospectivo

- A Importância da Comunicação de Risco para as Organizações
- Cenários Prospectivos em Gestão de Riscos Corporativos: um Estudo de Caso Brasileiro
- Gestão da Continuidade de Negócios - GCN
- Gestão da Continuidade de Negócios e a Comunicação em Momentos de Crise

Coleção Consultoria e Gestão

- Gestão Estratégica do Sistema de Segurança. Conceitos, Teorias, Processos e Prática
- Guia Prático para Elaboração de Fluxograma

Coleção Gestão de Riscos

- Gestão de Risco Operacional em Shopping Center a Segurança que o Cliente não vê
- Gestão de Riscos Operacionais para um Sistema de Abastecimento de Água
- Gestão de Risco Positivo
- Gestão e Análise e Riscos Corporativos: Método Brasiliano Avançado

Coleção Segurança da Informação

- O Valor Probatório do Documento Eletrônico

Coleção Segurança Empresarial

- Dicas e Macetes do Gestor de Segurança
- Processos e Métodos em: Prevenção de Perdas e Segurança Empresarial

Coleção Segurança Pessoal

- Guia de Procedimentos Segurança Pessoal
- Dicas de Segurança
- Guia Prático do Agente de Segurança

Coleção Segurança Pública

- As Formas do Crime
- A Questão da Segurança Privada
- Corrupção: um Efeito Sobre a Taxa de Juros
- Mobilização de micro comunidades : Vizinhança e Segurança pública

Coleção Tecnologia da Segurança

- Controle de Acesso: Conceitos, Tecnologias e Benefícios

para comprar acesse: www.sicurezzaeditora.com.br

SICUREZZA editora


20 anos de credibilidade na área de capacitação
Nossos Cursos Proporcionam a Evolução na sua Carreira Profissional
Pós Graduação I MBA em Gestão de Risco e Fraudes Empresariais
MBA em Gestão de Risco Corporativos
Extensão Universitária I Gestão de Continuidade de Negócios
Gestão e Análise de Risco Estratégica ISO 31000
Auditoria Baseada em Risco
Gerenciamento de Crises de Comunicação
Gestão de Risco Cadeia Logística -
ISO 28000 e 28002
b&a
BRASILIANO&ASSOCIADOS
info@brasiliano.com.br
www.brasiliano.com.br
11 5531 6171
convênio:
FAPI FACULDADE DE ADMINISTRAÇÃO SÃO PAULO
FESP FACULDADE DE ENGENHARIA SÃO PAULO