b&a
BRASILIANO & ASSOCIADOS

REVISTA ELETRÔNICA 36ª

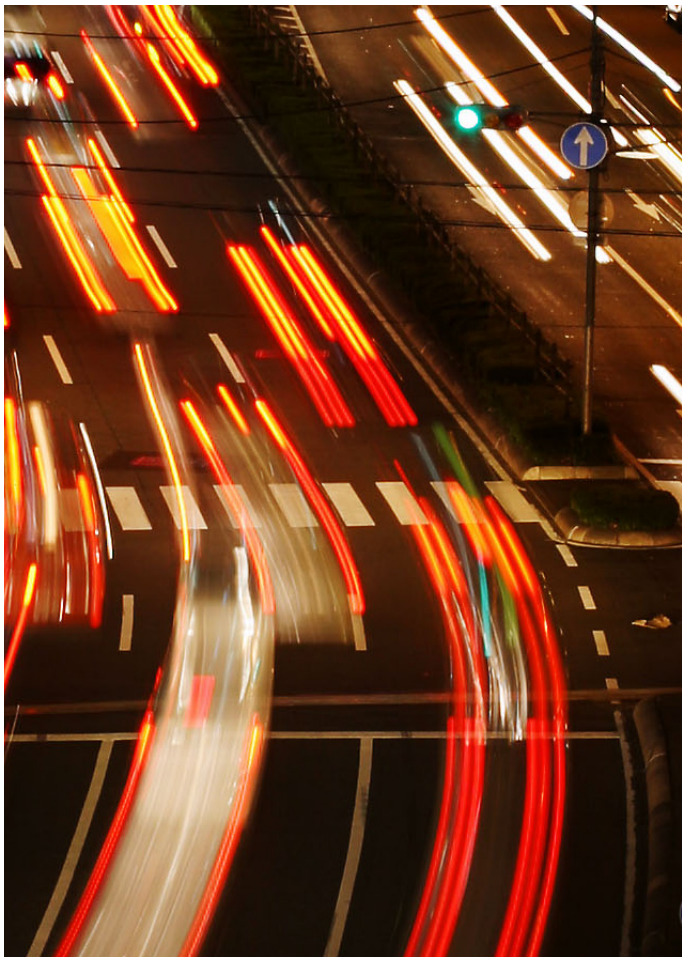
FUGA de INFORMAÇÃO e DESINFORMAÇÃO

www.brasiliano.com.br

ISSN 1678-2496N

Maio - Junho 2008 | Edição 36ª

SUMÁRIO



A Revista Eletrônica Brasiliano &
Associados nº36 é uma publicação
bimestral.

Diretor Executivo: Antonio Celso Ribeiro Brasiliano
Diretora de Treinamento: Enza Cirelli
Projeto Gráfico e Editoração: Marina Brasiliano
e-mail: mabrasiliano@gmail.com
Credito da foto Capa: (c)Tomo.Yun (www.yunphoto.net/pt/)

INOVAÇÃO NA SEGURANÇA EMPRESARIAL: EXISTE??

"Não existe nada mais difícil de fazer, nada mais perigoso de conduzir, ou êxito mais incerto do que tomar a iniciativa de introduzir uma nova ordem das coisas, porque a inovação tem inimigos em todos aqueles que se têm saído bem sob as condições antigas, defensores não muitos entusiásticos entre aqueles que poderiam sair-se bem na nova ordem das coisas"

Como consultor há amais de 18 anos de mercado, sinto-me motivado a iniciar este editorial com a reflexão pelos desafios e obstáculos à introdução de inovação e mudanças em nosso setor de atuação. Conforme a analogia ao texto acima, escrito por Maquiavel em seu famoso livro – O Príncipe, que aliás está cada dia mais atual. A resistência ao novo e ao desconhecido tem instigado nossos executivos das empresas prestadoras de serviço e os gestores das empresas tomadoras de serviço a persistirem num enfoque sistemático e pragmático, visando garantir seus posicionamentos. Quando toma-se esta atitude, optar só pelo pragmatismo, é o mesmo que acreditar que o futuro pode ser previsto como uma projeção de crescimento ajustado sobre um passado conhecido. Neste caso é o mesmo que olhar pelo espelho retrovisor!

Isto explica de forma clara o porque que nosso segmento ainda não avalia o risco de perder espaço no organograma empresarial, ainda não somos estratégicos, estamos posicionados no nível tático e operacional. Só 14% das empresas tomadoras de serviço possuem gerência de segurança corporativa!! Diretoria de Segurança corporativa menos que 4%, isso mesmo,, e ainda em 2008 perdemos mais uma diretoria em uma empresa de grande porte com atuação em território brasileiro e internacional!! A resposta está na reação natural das pessoas e empresas em optarem pelo mais fácil e prático, ao invés de enfrentar os desafios do nosso ambiente. Walter Longo, evengelista da agência de publicidade Young & Rubican disse em entrevista na Revista HSM Management que é preciso que as empresas possuam executivos com coragem e visão de longo prazo. Ele ressalta que os executivos de hoje administram empresas mais preocupados com o fim do mês do que com que com o fim do mundo. O mundo se acovardou!!Hoje ninguém mais se arrisca. Parece que a aventura humana chegou ao fim. As empresas são guiadas por uma visão utilitarista, em vez do empreendedorismo.

Vejam só!! SE isto está acontecendo em outros segmentos empresariais, imaginem no nosso!! Somos extremamente conservadores!! Para enfrentar esta turbulência, "O NOVO",

os profissionais de segurança e riscos necessitam possuir fortes valores para suportar esta pressão, é necessário quebrar regras, é necessário acreditar em superação, coragem e pioneirismo. Não pode ter medo do novo, de ousar de forma coerente e técnica.

Cair não é o problema, mas sim não levantar. Victor Hugo falava que acreditar em um sonho é construir o nosso futuro. Queremos que nosso segmento sonhe grande e ouse fracassar!

Espero que vocês, leitores, passem a refletir sobre o novo e a inovação e que possam de forma direta quebrar regras e ousar, tudo isso visando abrir caminho para a nossa subida no organograma empresarial.

Termino este editorial com a citação de Karlfriend Graf Von Durckheim:

"Quando se está realmente no caminho, o homem que deparar com tempos difíceis no mundo não se voltará para um amigo que lhe ofereça refúgio e consolo, estimulando a sobrevivência da sua velha personalidade. Pelo contrário, buscará alguém que, fiel e inexoravelmente, o ajude a se arriscar para superar o sofrimento e ultrapassá-lo com valentia, transformando-o na "balsa que vai à margem mais distante". Somente na medida em que o homem se expõe repetidamente às aniquilações do mundo surgirá nele aquilo que é indestrutível.

Nisso repousa a dignidade do ousar. A prática deve ensinar o homem a deixar-se assaltar, perturbar, empurrar, insultar, quebrar e golpear, ou seja, animá-lo a abandonar seu anseio fútil pela harmonia, pela ausência de dor e por uma vida cômoda e assim descobrir, lutando contra as forças opostas, aquilo que o aguarda além do mundo das polaridades. A primeira exigência é ter coragem para enfrentar a vida, para encontrar tudo o que há de mais perigoso no mundo..Quanto mais um homem aprende a enfrentar incondicionalmente o mundo ameaçador, mais se revelam as profundidades da Natureza Essencial do Ser e mais se abrem as possibilidades de uma nova vida em contínua Transformação."

Será que podemos tentar ser assim?? Reflitam!!!!

Boa leitura e sorte!

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

b&a
BRASILIANO&ASSOCIADOS

RISCO HUMANO: A IMPORTÂNCIA DO RECRUTAMENTO E DA SELEÇÃO NA SEGURANÇA EMPRESARIAL

Mauro Baier de Carvalho*

Ainda somos constantemente questionados sobre qual a melhor forma de selecionar um profissional para o preenchimento de uma vaga ou mesmo qual o critério para uma indicação coerente. Muitos desses questionamentos se dão pela própria forma como se tratam os processos de recrutamento e seleção nas empresas.

A dificuldade do gestor de segurança em declarar exatamente o que ele precisa aliada à inexperiência do departamento de recursos humanos em selecionar esta mão-de-obra acabam sendo as maiores causas de insucesso.

É de suma importância que o gestor de segurança transmita a sua necessidade de contratação de forma clara e específica. Os requisitos devem ser entendidos pelo profissional de RH e checados durante todo o processo seletivo. Desta forma, o primeiro passo da seleção de pessoal está na correta descrição do cargo, que deve atender os seguintes itens:

- Missão do cargo- o que se espera da pessoa contratada frente às necessidades da empresa
- Principais desafios- de forma ampla e holística prevêem o cenário a ser encontrado pelo novo contratado e como se espera que ele atue
- Dimensões do cargo- para quem ele responde, quais os seus subordinados e como o departamento de segurança está inserido no contexto da empresa
- Principais produtos e serviços- descrever frente às rotinas da função quais são as responsabilidades / obrigações, clientes internos / externos, requisitos dos clientes e medições (indicadores de qualidade)
- Formação exigida para o cargo- nível técnico, acadêmico etc
- Salário e benefícios- se houver oportunidade de influenciar neste quesito, o gestor deve recomendar a prática de mercado referente ao segmento do negócio da empresa, ou seja, comparar o que é aplicado entre empresas do mesmo ramo
- Experiência e recomendação- são importantes e devem ser consideradas.

De posse destas informações, o gestor de segurança e o RH podem seguir para o próximo passo, que é a procura pelos candidatos e seleção de currículos.

É preciso ressaltar a importância da participação do gestor neste momento, pois ainda é uma área nova e as atividades são desconhecidas por muitos recrutadores. Lembre-se de colocar a isca no lugar certo. Não adianta procurar funções administrativas em academias de formação ou buscar um especialista acadêmico na operação.

b&a
BRASILIANO&ASSOCIADOS

Após a seleção prévia dos currículos, vêm a hora das entrevistas que devem ser realizadas primeiramente pelo RH e depois pelo solicitante da vaga, no caso o gestor de segurança.

Se possível, envolva outras áreas com as quais a segurança possua sinergia. É importante o envolvimento de outros gestores e suas opiniões sobre o candidato de forma a gerar cumplicidade na tomada de decisão e promover o relacionamento entre as áreas da empresa.

Aprovado nesta fase, o candidato deverá se submeter a testes de conhecimento sobre os serviços e atividades que exercerá. Se estiver selecionando para a área operacional, foque os testes em atividades práticas. Se for para área tática e/ou estratégica, prefira a aplicação de um "case", forçando a utilização de ferramentas do pacote Office, metodologias de análise de riscos e ferramentas gerenciais. Ao final, peça para que o trabalho seja apresentado para o grupo avaliador.

É de suma importância não decidir sozinho, gere o sentimento de cumplicidade entre os envolvidos no processo. Não deixe que a sua opinião se sobreponha frente aos demais. O ideal é ter uma decisão coletiva com a sua recomendação.

Riscos no processo

O risco negativo neste momento é a escolha da pessoa errada ou a demora para encontrar o perfil desejado. No primeiro caso, soma-se o retrabalho e os custos diretos e indiretos do processo. No segundo, o acúmulo de tarefas e o tempo de resposta aos clientes internos e externos.

Utilizando o processo descrito, a probabilidade de uma contratação indesejada é pequena, porém o seu impacto ainda pode ser catastrófico se todo o fluxo não for seguido na íntegra.

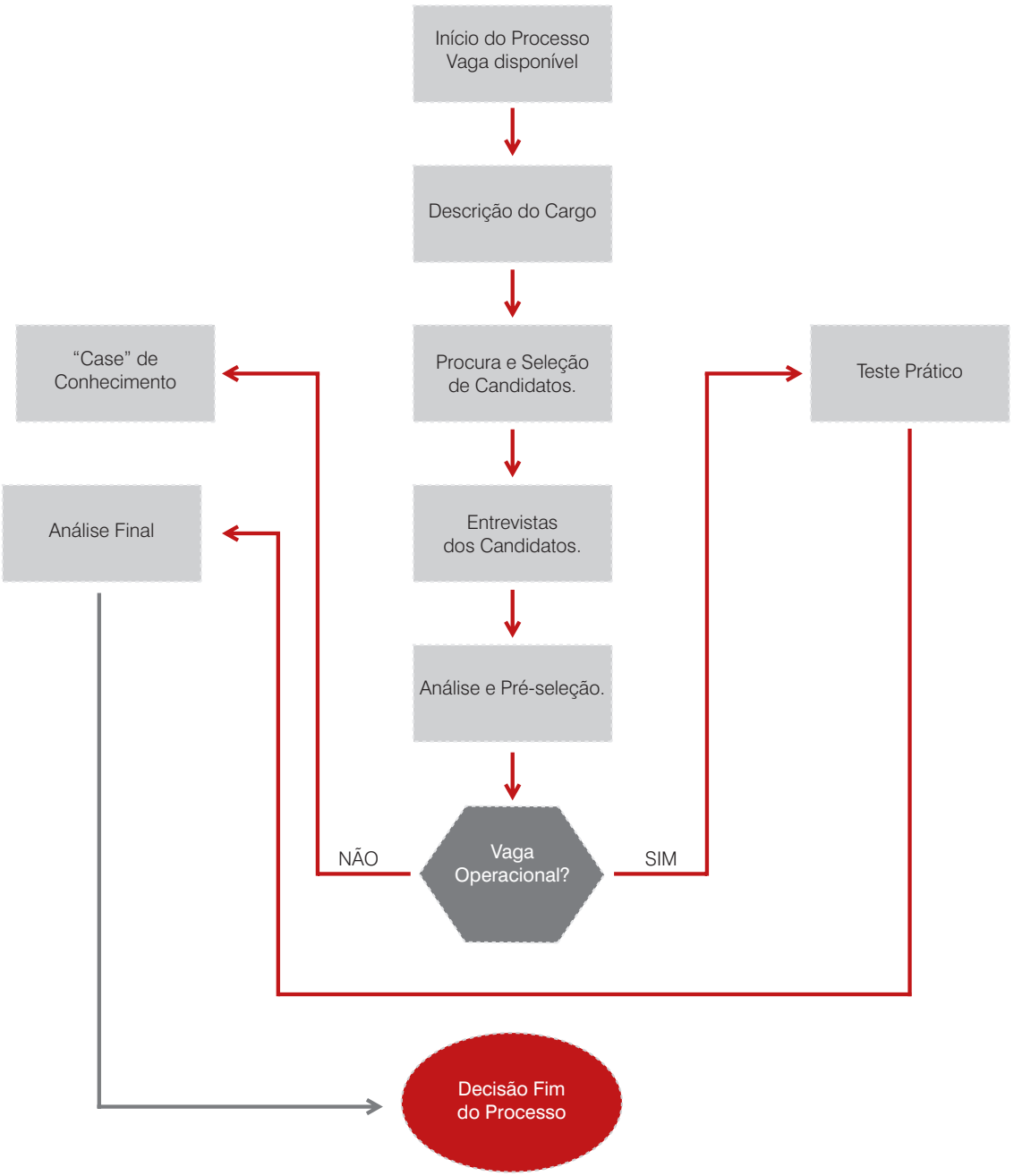
Consideramos também o risco positivo como uma possibilidade de demonstrar aos demais departamentos de uma organização que a segurança empresarial possui os seus métodos e processos estruturados e condizentes com o objetivo do negócio da empresa, onde a prevenção e antecipação aos eventos futuros são tratadas de forma profissional.

Meios auxiliares

Definimos como meios auxiliares os elementos de suporte ao processo e que de forma indireta contribuem para o êxito da tarefa de recrutamento e seleção. Muitos já são conhecidos, mas poucos são utilizados. Destacam-se:

- Benchmark
- Divulgação das vagas em associações de segurança, universidades, cursos de formação e demais entidades de classe
- Network, troca de informações entre gestores de segurança
- Bom relacionamento com RH e demais áreas envolvidas no processo
- Levantamento sócio-funcional

Fluxograma do Processo



Mauro Baier de Carvalho é bacharel em Administração, MBA em Gestão de Segurança Empresarial - Fecap, professor nos Cursos de Extensão Universitária da Fecap/ B&A e coordenador de Segurança da Boehringer Ingelheim do Brasil.

O PERIGO VEM DE DENTRO

Hugo Ferreira Leitão*

Nos dias de hoje, todas as informações estão ou passam pelos computadores. Sejam elas dados sigilosos, informações de clientes, faturamento da empresa ou até uma simples conversa para combinar o jantar. Em um mundo tão globalizado e dinâmico, todos estes computadores estão em rede, sejam nas redes internas como aquelas que criamos em nossas empresas, ou conectadas a tão falada Internet, a grande rede mundial de computadores interconectados.

Por isso é fácil para um usuário com algum conhecimento de informática invadir uma rede privativa e acessar dados sigilosos que deveriam estar guardados a sete chaves. Assim, empresas investem um bom dinheiro em programas que fecham as portas de entrada de suas máquinas (os chamados firewalls) e em antivírus, programas especiais que detectam e excluem os programas infiltrados pelos invasores.

Só que apenas isso não resolve. Pode parecer um contra-senso para alguns, mas o maior risco para os sistemas de Tecnologia da Informação (TI) não são os invasores externos, mas sim os internos. Sim, o maior perigo vem de dentro da própria empresa.

Há casos de invasores que se valem da chamada engenharia social, que consiste do mais antigo truque para enganar alguém: vale-se da boa vontade do usuário. Por isso é comum aquele já manjado e-mail que pede para clicar em algum link para abrir uma foto ou documento, mas que na verdade abre as portas do computador ao invasor. Para este perigo não bastam apenas os programas antivírus ou proteções contra invasões, mas sim a instrução de todos os funcionários para quem saibam como agir nestes casos.

Existe também outro risco. Muitas informações consideradas sigilosas estão ao alcance de qualquer funcionário, deixando a possibilidade que tais dados sejam usados de forma indevida. E não é necessário ir muito longe, já que até mesmo as informações necessárias para o colaborador exercer a sua função podem ser

utilizadas dessa forma. Por isso, é necessário que o empresário invista em uma boa análise de risco para que possa identificar as informações consideradas sigilosas, quem as acessa, qual a ferramenta que existe para identificar estes acessos e mensurar o impacto do roubo da informação. Só assim haverá um tiro certeiro que protegerá os dados e tornará possível a identificação de um possível invasor.

Entre outras ferramentas de segurança, a análise de risco consiste em identificar e classificar todos os processos do negócio, verificando o funcionamento da empresa, como é feita essa operacionalização pelos seus colaboradores, por quais sistemas as informações passam, quem acessa os bancos de dados, incluindo uma identificação das informações sigilosas. Após esta primeira análise, é necessário também verificar quais dados estão vulneráveis e acessíveis a possíveis usuários maliciosos, ou até mesmo àqueles que podem soltar a informação acidentalmente, e quais os riscos que a empresa sofre. A partir daí são implantadas soluções como a proteção das informações e a identificação dos usuários.

Infelizmente, muitas empresas não percebem a necessidade do investimento em Segurança da Informação. A pressão por resultados é muito grande e quase sempre é necessário que a empresa faça girar o capital e obtenha lucro o mais rápido possível, deixando os cuidados em segurança para segundo plano. Só que esse descaso pode ocasionar um bom prejuízo depois se informações sigilosas forem acessadas.

Um caso famoso, que ocorreu em meados de 2007, foi o de um administrador de banco de dados de uma empresa subsidiária da processadora de serviços financeiros FIS (Fidelity National Information Services), que juntou dados de mais de dois milhões de pessoas cadastradas na corporação e os vendeu para companhias de marketing. Com os dados, um imenso mailing contendo informações como nome, endereço, datas de nascimento, informações sobre contas bancárias e cartões de crédito foi criado e parcialmente revendido para outras empresas de marketing. Mesmo que estas informações não sejam utilizadas para crimes, com certeza os clientes da FIS não ficaram nada satisfeitos ao saber que seus nomes e telefones agora estão nas mãos de inúmeras empresas de marketing ativo.

Até empresas que trabalham diretamente na Internet não percebem o perigo de algumas atitudes, que nem sempre são cometidas por má-fé. Em agosto de 2006, o site de buscas Yahoo!, um dos mais antigos da rede, liberou sem maiores cuidados uma lista de registros de buscas efetuadas no site durante três meses. Eram dados de centenas de milhares de assinantes, que foram disponibilizados para pesquisa não-comercial, mas que estavam acessíveis para qualquer um. A situação foi tão crítica que dois repórteres do jornal norte-americano The New York Times conseguiram até localizar um desses usuários apenas com os dados divulgados pelo Yahoo!. Apesar das informações terem sido retiradas do ar rapidamente, é impossível calcular agora quantas pessoas em todo o mundo as acessaram e gravaram em suas próprias máquinas. Isto mostra como é importante saber o que fazer e como fazer quando se trata de segurança.

Por isso é importante não ficar para trás. A falta de segurança hoje pode trazer muita dor de cabeça amanhã.

Hugo Ferreira Leitão é especialista em Segurança da Informação, diretor técnico e fundador da Foco Security - www.focosecurity.com.br

DESINFORMAÇÃO: ARMA DA CONTRA INTELIGÊNCIA

Joffre Coelho Chagas Júnior *

A desinformação é uma medida de caráter ofensivo onde à empresa através do seu departamento de Contra-Inteligência irá iludir a concorrência sobre suas atividades e principalmente sobre o lançamento de seus produtos e/ou serviços.

Lembrando que a Contra-Inteligência é o ramo da Atividade de Inteligência responsável em salvaguardar o Sistema da Empresa, contra as ações dos seus concorrentes. É uma atividade permanentemente exercida e executada com o objetivo de proteger conhecimentos vitais para a empresa, seu pessoal e instalações contra as atividades desenvolvidas pelo Serviço de Inteligência da concorrência.

Para atender o que está descrito no conceito acima, a Contra-Inteligência conta com dois segmentos:

- Segurança Orgânica e
- Segurança Ativa.

A Segurança Orgânica é o conjunto de medidas passivas com o objetivo de prevenir e até mesmo obstruir as ações do serviço de Inteligência da concorrência. Para isso conta com os seguintes grupos de atividades:

- Segurança de Pessoal;
- Segurança da Documentação;
- Segurança das Comunicações;
- Segurança da Informática e
- Segurança das suas Áreas e Instalações.

A Segurança Ativa é a atividade desenvolvida pelo serviço de Inteligência da empresa, com o objetivo exclusivamente ofensivo visando detectar, identificar, avaliar e neutralizar as ações desenvolvidas pelo serviço de Inteligência da concorrência. Essa atividade é desenvolvida através das seguintes ações:

- Contra-Espionagem;
- Contrapropaganda e
- Desinformação.

b&a
BRASILIANO&ASSOCIADOS

Ao meu ver, a atividade que pode traduzir em um ganho significativo para a empresa, tornando-a mais competitiva nesse mundo globalizado, onde o risco está presente em todas as suas atividades, seja ela de produto ou serviço, é a Desinformação.

Buscando mostrar sua importância vamos fazer uma viagem ao passado, mais precisamente na década de 40 (quarenta), durante a Segunda Grande Guerra, onde uma Operação do Serviço de Inteligência Britânico confundiu a Inteligência Alemã, obtendo êxito na invasão da Europa.

Conhecida como a mais bem sucedida Operação de Desinformação da Segunda Guerra Mundial, surge a Operação "Mincemeat – Recheio".

Após o sucesso da invasão da África do Norte, os Estrategistas aliados queriam definir o próximo passo: avança da África para a Europa através da Sicília, pelo estreito de Messina. É claro que os alemães, por certo, esperavam por isso e iriam concentrar suas forças na região. Como convencê-los do contrário, induzindo-os a dispersar suas tropas para outros pontos do continente europeu? A partir daí é que entra em ação o Intelligence Service britânico, quando um de seus membros pensa numa Operação de Desinformação.

Como os alemães sabiam que oficiais ingleses sobrevoavam a costa espanhola rumo à África do Norte, por que não lançar ao mar um cadáver com documentos falsos, como se fosse vítima fatal de um acidente aéreo, exatamente nas imediações do litoral espanhol?

A Operação foi planejada nos mínimos detalhes desde a escolha do cadáver que deveria ter como causa mórtis as características de um afogamento para confundir os alemães, pois fatalmente isso seria verificado pelo Serviço de Inteligência Alemão, bem como todo o resto da Estória de Cobertura. Foi criado um passado para o major William Martin, que na verdade era um súdito inglês que morrera de pneumonia e a família havia cedido seu corpo ao Estado desde que sua identidade jamais fosse revelada. Várias ligações fizeram para o major William inclusive lhe arrumaram uma namorada para dar mais realidade a história e a ela criar maior poder de convencimento aos alemães. Cartas e documentos foram dobrados e desdobrados várias vezes para parecer que tinham sido lidos diversas vezes.

O major Martin conduzia ainda chapas de identificação, um relógio de pulso, cigarros, bilhetes antigos de ônibus e chaves. Em sua última noite na Inglaterra, teria levado a noiva ao teatro e tinha no bolso a metade de dois ingressos para uma peça no dia 22 de abril de 1942.

Em suma, o plano de certa forma simples, baseava-se nos seguintes pontos:

Martin levaria numa pasta uma carta do general Sir Archibald Nye, subchefe do Estado-Maior Imperial, ao general Alexander, comandante do Grupo de Exércitos da África, com uma explicação, entre amigos, dos motivos pelos quais Alexander não estava recebendo do chefe do Estado-Maior, tudo o que queria. Por inferência, chegava-se a conclusão que se planejava atacar o Mediterrâneo Ocidental. Os possíveis pontos seriam um na Grécia e o outro, não muito bem identificado, mas não era a Sicília.

O major levava ainda um comunicado do Lorde Louis Mountbatten ao almirante de Esquadra, Sir Andrew Cunninghan, comandante-e-chefe no Mediterrâneo, explicando sua missão e concluindo: "Creio que Martin é o homem que lhe serve. Queira mandá-lo de volta logo que termine o assalto. E não se esqueça de dar-lhe mais sardinhas. Elas estão aqui racionadas".

A palavra "sardinhas" servia apenas para indicar aos alemães a Sardenha como objetivo do ataque. Estava assim em grosso modo preparada, a Operação Recheio.

O cadáver de Martin seria transportado pelo submarino Seraph, sob o comando do tenente Jewell, e lançado ao mar próximo a Huelva.

O próprio Churchill deu sua aprovação e ordenou para que o general americano Eisenhower, no comando da invasão da Sicília, fosse informado.

A operação foi desencadeada e na manhã do dia 30 de abril de 1943, um pescador espanhol avistou o corpo perto da praia e avisou as autoridades. Após autópsia, constatou-se asfixia por imersão no mar.

Como os britânicos imaginavam, os documentos caíram nas mãos de um conhecido espião nazista operando na Espanha, que depois de fotografá-los enviou as fotos para a Alemanha.

Nesse ínterim, um agente alemão estava na Inglaterra verificando o passado de Martin, investigando os dados relativos a sua vida. Tudo que procurou achou e se convenceu que tudo era verdadeiro, informando a seus superiores na Alemanha, sem saber que a Contra-Inteligência havia seguido seus passos.

Como resultado o Alto Comando Alemão transferiu uma Divisão Blindada da França para o Peloponeso (região da Grécia) e também foram colocadas minas ao longo do litoral grego.

No oeste, o marechal-de-campo Wilhelm Keitel assinou uma ordem determinando o reforço da Sardenha.

Mesmo depois de iniciado o ataque principal à Sicília, os alemães continuavam pensando tratar-se apenas de uma manobra secundária. O êxito da missão pode ser avaliado nas palavras do marechal-de-campo, Erwin Rommel, cujos documentos pessoais revelam que, quando os aliados invadiram a Sicília, as defesas alemãs achavam-se dispersas em conseqüência do encontro do cadáver de um mensageiro diplomático nas costas da Espanha.

É obvio que a Operação tinha muito mais detalhes do que os aqui mencionados, porém, nosso objetivo não é o detalhamento da Operação e, sim, mostrar a importância do Serviço de Inteligência e Contra-Inteligência para sua empresa, em particular a atividade de Contra-Inteligência que se utiliza de meios valiosíssimos para garantir a sua empresa a sustentabilidade nesse mercado globalizado, agressivo e competitivo, como a DESINFORMAÇÃO.

Joffre Coelho Chagas Júnior* é gerente da Superintendência de Averiguação de Sinistro da Empresa GPS Logística e Gerenciamento de Risco (PAMCARY). Mestre em Operações Militares, tem MBA de Gestão de Segurança Empresarial pela FECAP - SP; Gestión de Seguridad Empresarial Internacional pela Universidad Pontificia Comillas de Madrid; especialista em Segurança – ABSO e cursos de Investigação de Roubo de Cargas; Gerenciamento de Risco no Transporte Rodoviário de Cargas; Segurança e Criminalidade. É professor convidado da FECAP/Brasiliano & Associados para cursos de Investigações & Fraudes Empresariais e no MBA de Gestão de Segurança Empresarial, além de coordenador técnico dos Cursos da Brasiliano & Associados.