UNIVERSIDADE DE LISBOA

FACULDADE DE LETRAS

Conselhos de segurança anti-terrorismo para hotéis e restaurantes: tradução e respectivo comentário

Relatório do estágio realizado no Instituto Superior de Ciências Policiais e Segurança Interna

Raquel Rodrigues Milho

MESTRADO EM TRADUÇÃO

2013

UNIVERSIDADE DE LISBOA

FACULDADE DE LETRAS

Conselhos de segurança antiterrorismo para hotéis e restaurantes: tradução e respectivo comentário

Relatório do estágio realizado no Instituto Superior de Ciências Policiais e Segurança Interna

Raquel Rodrigues Milho

Orientadora: Professora Doutora Anabela Gonçalves

MESTRADO EM TRADUÇÃO

2013

AGRADECIMENTOS

Em primeiro lugar, agradeço à Professora Doutora Clotilde Almeida e ao Subintendente Sérgio Felgueiras por me terem concedido a possibilidade de estagiar no ISCPSI.

À doutora Cristina Reis pela orientação do estágio no ISCPSI.

À Professora Doutora Anabela Gonçalves pela orientação e pela disponibilidade que sempre mostrou.

Ao ISCPSI e a todos os dele fazem parte, desde o corpo administrativo ao pessoal da cafetaria e das limpezas. Um agradecimento especial à chefe Ana Robalo pela simpatia e pelos convites para dois dedos de conversa e um café.

Às minhas companheiras de estágio, a Andreia Sousa e a Susana Silvestre, pela ajuda e por entenderem melhor do que ninguém os meus desabafos.

Finalmente, aos meus pais e aos meus amigos por me fornecerem distracções quando este relatório tornava inexistente a minha vida social.

RESUMO

O presente relatório de estágio tem como objectivo a descrição e análise do trabalho de tradução realizado no Instituto Superior de Ciências Policiais e Segurança Interna, em Lisboa, no âmbito do estágio profissionalizante do Mestrado em Tradução.

Este estágio teve como objectivo a tradução de textos da área técnica e foi uma oportunidade para colocar em prática os conhecimentos adquiridos ao longo do primeiro ano do Mestrado.

O relatório está dividido em três partes. A primeira parte é dedicada à apresentação da entidade de acolhimento, com uma menção breve à sua história, à descrição do próprio estágio e à apresentação dos textos traduzidos, com uma referência às diferenças entre os mesmos.

A segunda parte tem como intuito dar a conhecer o que é a tradução no seu sentido genérico, pretendendo-se apresentar algumas questões relacionadas quer com o trabalho do tradutor quer com o próprio trabalho de tradução. Ainda neste capítulo é dada especial atenção à tradução de textos técnicos, uma vez que os documentos traduzidos no estágio se incluem nesta área da tradução.

A terceira e última parte do relatório foca-se na análise de um dos documentos traduzidos, um manual de segurança anti-terrorismo para hotéis e restaurantes. Primeiramente, são apresentadas questões de tradução relacionadas com questões lexicais, como a terminologia, sendo depois analisadas questões sintácticas e questões relativas à modalidade e à coesão referencial, finalizando-se com questões de carácter cultural.

Palavras-chave: tradução, tradução técnica, sintaxe, terminologia

ABSTRACT

This report aims to describe and analyse the translation work carried out at Instituto Superior de Ciências Policiais e Segurança Interna in Lisbon as part of my professional internship for a Master in Translation.

The aim of this internship was the translation of technical texts and the putting into practice of the knowledge acquired during the first year of the Master's program.

The report is divided in three sections. The first section features a description and brief history of the institute and of the internship itself, along with the introduction of the translated texts and their differences.

The second part aims to inform what translation is in general, with a reference to some matters of the translator and the translation work. In this part there is a chapter about the translation of technical texts, as the documents translated in the internship belong to this category of translation.

The third and last part of this report focuses on the analysis of one translated documents, a guide of counter terrorism protective security advice for hotels and restaurants. Firstly we will explore the difficulties concerning lexical aspects, like terminology, and sintactical aspects. After there will be a chapter about the analysis of examples related to modality and another concerning referential cohesion. Lastly we will focus examples of cultural aspects present in the translation.

Keywords: translation, technical translation, syntax, terminology

LISTA DE SIGLAS

CEPOL – Collège Européen de Police/Colégio Europeu de Polícia

CPNI – Centre for the Protection of National Infrastructure

ESP – Escola Superior de Polícia

FLUL – Faculdade de Letras da Universidade de Lisboa

ISCPSI – Instituto Superior de Ciências Policias e Segurança Interna

NaCTSO – National Counter Terrorism Security Office

UEFA – Union of European Football Associations

ÍNDICE

INTRODUÇÃO[1]

A minha experiência na área da Tradução começou no momento em que iniciei o estudo de outras línguas, num instituto, quando não tinha mais do que oito anos. Porém, nessa altura, ainda não sabia que o que fazia na minha cabeça e depois passava para o papel se chama *traduzir*. Foi nesse instituto que tive o primeiro contacto a minha primeira experiência com a língua inglesa, que esteve presente ao longo da minha educação e dos meus tempos-livres.

A decisão de ir para o curso de Línguas, Literaturas e Culturas, variante em Línguas Modernas, da FLUL, deveu-se ao facto de querer prolongar o estudo de línguas estrangeiras – não só de Inglês e Alemão, que à data também já começara a estudar. Esta opção revelou-se vantajosa, porque me deu a conhecer o Italiano e o Espanhol. No entanto, quando finalizei o primeiro ciclo de estudos do Ensino Superior, ponderei o Jornalismo como a próxima etapa. O engano foi descoberto nos primeiros meses e percebi que o meu lugar era junto das línguas, pelo que ingressei no Mestrado em Tradução.

Este Mestrado possibilitou-me crescer como tradutora, saber o que está certo e o que se deve evitar numa tradução; todavia, o trabalho de um tradutor nunca pára. Como em todas as outras profissões, estamos sempre a aprender, sempre a crescer e a saber mais.

A opção da realização do estágio surgiu aquando da inscrição para o mestrado, sem saber ainda se seria ou não aceite para a realização do mesmo e se haveria alguma vaga para um estágio. Não estava nos meus planos escrever uma tese ou traduzir e analisar uma obra por mim escolhida, porque queria algo que me abrisse horizontes e que me permitisse o contacto com um ambiente exterior ao da Faculdade. Pretendia com o estágio algo que se assemelhasse a uma experiência profissional. A primeira opção foi a tradução audiovisual, mas, uma vez que não abriu qualquer vaga para um estágio nesta área, o Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI) revelou-se, sem qualquer dúvida, a melhor opção.

[1] Este relatório não segue as regras do Acordo Ortográfico de 1990. Porém, os exemplos retirados do manual traduzido, que está redigido tendo por base o dito acordo, não foram modificados aquando da sua utilização neste relatório.

O estágio no ISCPSI proporcionou-me a utilização de competências e conhecimentos que adquirira no primeiro ano do Mestrado. Por outro lado, a instituição em questão, pela sua importância no que diz respeito à formação de oficiais de polícia e à comunicação com organismos estrangeiros relacionados com a polícia, tem um estatuto importante no panorama nacional e internacional, razão que muito pesou na minha candidatura a este estágio. A tradução do texto técnico, pela sua especificidade e dificuldade, foi mais um desafio que me foi colocado neste Mestrado e todas as razões havia para que o último ano tivesse como base este campo da tradução.

O relatório que se apresenta de seguida está dividido em três capítulos principais. O primeiro capítulo pretende dar a conhecer o ISCPSI, bem como apresentar uma descrição do estágio e dos textos traduzidos. No segundo capítulo procede-se a uma breve reflexão teórica acerca da tradução, com particular referência à tradução técnica, visto ter sido esta a área da tradução em que se inscrevem os documentos trabalhados no estágio. Por fim, o terceiro capítulo do relatório será dedicado à análise de um dos textos traduzidos, o manual de conselhos de segurança anti-terrorismo para hotéis e restaurantes, o que permitirá justificar as opções de tradução que foram tomadas em alguns dos casos que considerámos mais relevantes.

Neste relatório apenas se procede a uma reflexão relativamente ao manual e não ao outro texto também trabalhado. A justificação para tal é apresentada mais à frente no início do terceiro capítulo.

CAPÍTULO UM

1. CARACTERIZAÇÃO DO ESTÁGIO

1.1 Entidade de acolhimento

O ISCPSI é um estabelecimento de Ensino Superior público policial misto que funciona no antigo Convento do Calvário, na Rua 1º de Maio, nº 3, em Lisboa.

Em 1966, o edifício foi atribuído à Escola Prática de Polícia, vindo depois a ser ali instalada a Escola Superior de Polícia (ESP). As instalações anexas foram inauguradas no ano lectivo de 1994/95. Em 1999, a Escola Superior de Polícia passou a chamar-se Instituto Superior de Ciências Policiais e Segurança Interna.

A ambição do Instituto, aquando da sua criação em 1979, era a preparação e formação de oficiais de Polícia com o Curso Superior de Formação de Oficiais de Polícia, para que se procedesse à substituição progressiva dos oficiais do Exército a prestar serviço na Polícia de Segurança Pública. Porém, em 1984, na sequência do Decreto-Lei n.º 129-B/84, publicado no Diário da República n.º 98, 1ª série, de 27 de Abril, passou a ser da competência da ESP fornecer outros dois cursos. Assim, no ano lectivo de 1984/85 e nos seguintes, "passa a pertencer à Escola Superior de Polícia ministrar os cursos de formação de comissários e chefes da Polícia de Segurança Pública" (artigo 1º do mesmo Decreto-Lei), ou seja, foi naquele ano lectivo que foram pela primeira vez ministrados não só o Curso de Formação de Oficiais de Polícia, mas também o Curso de Promoção a Comissário e o Curso de Promoção a Chefe de Esquadra.

O instituto funciona em regime interno e os alunos usam uma farda com as divisas do ISCPSI e do ano que frequentam. Concluída a licenciatura em Ciências Policiais, o aluno passa ao posto de Subcomissário e torna-se, na maioria das vezes, Comandante de Esquadra.

Actualmente, o instituto não ministra apenas a Licenciatura em Ciências Policiais (Curso de Formação de Oficiais de Polícia), mas também cursos intensivos de Anti-Terrorismo, de Direito Disciplinar, de Direito e Segurança e de Contratação e Finanças Públicas. Também da sua competência são os cursos de Pós-Graduação em Procedimento Contra-Ordenacional, Gestão Civil de Crises, Segurança Interna e Gestão Municipal da Segurança e os Mestrados nas áreas de Ciências Policiais, Segurança Interna, Gestão da Segurança, Criminologia e Investigação Criminal, Gestão Municipal da Segurança e Gestão Civil de Crises.

Para além dos cursos, o ISCPSI realiza também conferências e seminários, quer para alunos quer para profissionais da Polícia. É, igualmente, parte integrante de projectos de investigação e desenvolvimento relacionados com a segurança interna, nomeadamente através da realização, coordenação ou colaboração nos mesmos e um ponto de contacto para o Colégio Europeu de Polícia (CEPOL – *Collège Européen de Police*). Finalmente, o ISCPSI promove, ainda, acções de formação na área da segurança, nas quais será utilizada a tradução levada a cabo durante o nosso estágio (formação sobre segurança hoteleira e turística).

1.2 Descrição do estágio

O estágio profissionalizante decorreu entre Setembro de 2012 e Maio de 2013, nas instalações do ISCPSI. Os dias de trabalho eram as segundas-feiras e as quartas-feiras, das 8h30 às 12h30, e cada semestre de estágio teve a duração de 120 horas. A orientação, no local, foi feita por parte do Subintendente Sérgio Felgueiras e da Dr.ª Cristina Reis, tradutora do Instituto. À nossa disposição estava uma sala com duas mesas e várias cadeiras, bem como Internet *wireless*. Foi utilizado um computador portátil próprio, dada a impossibilidade de o ISCPSI o disponibilizar.

As línguas de trabalho foram o Inglês e o Português, e foi apenas realizado trabalho de tradução da primeira para a segunda.

A tradução dos documentos foi amparada pela consulta de dicionários, em papel ou, mais comummente, na Internet, e de glossários, como os realizados em algumas disciplinas ao longo do primeiro ano do Mestrado e o de Cruz (2012). Nos casos em que a primeira pesquisa nos referidos dicionários e glossários não era bem-sucedida, era

feita uma busca em *sites* de entidades ou empresas com reconhecida importância nas áreas em questão. Não foram utilizados programas de tradução automática, embora, por vezes, o tradutor automático do Google tenha ajudado na compreensão de algumas frases, sendo-lhe, como é óbvio, dada a devida margem de dúvida.

Quando já tinha procedido à tradução de algumas páginas do manual, enviava-as à Dr.ª Cristina Reis para que esta as corrigisse. Em função dessas correcções, cabia-me actualizar o texto final, após o que procedia a uma revisão do mesmo. Este trabalho foi apoiado pelo cruzamento de informações com a outra estagiária da mesma língua, Susana Silvestre.

O manual referido constitui o *corpus* de análise deste relatório e encontra-se, na sua versão traduzida, em anexo (Anexo B).

2. DESCRIÇÃO GERAL DOS TEXTOS TRADUZIDOS

O estágio consistiu na tradução de um manual de conselhos de segurança anti-terrorismo para hotéis e restaurantes, originalmente escrito em Inglês e produzido pelo *National Counter Terrorism Security Office* (NaCTSO), unidade policial que faz parte do *Centre for the Protection of National Infrastructure* (CPNI); este manual foi descarregado do *site* do próprio NaCTSO, tendo sido escrito pela *Association of Chief Police Officers* (ACPO) em 2008. A tradução deste documento foi interrompida durante a quase totalidade do mês de Outubro para que fosse realizada a tradução de um outro documento em Inglês, produzido pelo CEPOL para ser utilizado num projecto de policiamento em eventos de futebol organizados pela UEFA. Este texto foi-me entregue pessoalmente pela Dr.ª Cristina Reis, em formato electrónico.

Ambos os textos traduzidos foram redigidos seguindo o Acordo Ortográfico de 1990, por opção do ISCPSI.

Os dois documentos são textos técnicos, em Inglês, e pertencem à área de segurança em espaços públicos.

O manual tem 70 páginas e um *design* apelativo devido à presença de imagens e títulos coloridos. Tem como objectivo aconselhar o público-alvo (os gerentes,

proprietários ou responsáveis pela segurança em hotéis e restaurantes) sobre as medidas a tomar para assegurar a protecção dos espaços. Este documento dirige-se a um único destinatário, um gerente de um hotel ou de um restaurante, não se adaptando, quer pelo seu tamanho quer pelo seu registo linguístico, a um auditório, uma vez que seriam necessárias várias horas para que a totalidade do texto fosse lida. O destinatário está fortemente presente, como é possível verificar nos exemplos (1) a (4).

(1) You know what is important to you and your business.

(2) You should be aware of the need to modify them to take into account any changes in your hotel or restaurant.

(3) Your planning should incorporate the seven key instructions applicable to most incidents.

(4) Try to ensure that your procedures, while effective, are not needlessly disruptive.

Os parágrafos não são muito extensos e alternam entre texto normal, caixas de texto (com informação importante para o leitor) e marcas ou numeração. As frases são maioritariamente imperativas e alternam entre frases curtas (uma linha) e frases longas (três ou mais linhas). A terminologia do manual é relacionada com o Direito, com a indústria, com as forças policiais, com a actividade económica, com a energia, com o emprego, com a informática e com organismos do Reino Unido. Em anexo (Anexo A), existe uma lista de termos do manual, com as respectivas traduções. Alguns exemplos desses termos encontram-se reunidos em (5) a (13):

(5) Criminal prosecution – Acção criminal

(6) Business continuity planning – Planos de continuidade das actividades

(7) Tenant – Locatário

(8) P45 – Código de referência de um formulário com quatro partes intitulado *Details of employee leaving work*, relativamente a cessação de contrato e que deve ser entregue pela entidade empregadora.

(9) Strategic Commander – Comandante estratégico

(10) Publicly-funded compensation scheme – Regime de indemnização financiado por fundos públicos

(11) Disability Discrimination Act – Lei para a não-discriminação da deficiência

(12) Trade bodies – Organizações empresariais

(13) Home Office Scientific Development Branch (HOSDB) – Gabinete para o Desenvolvimento Científico do Ministério da Administração Interna

Por seu lado, o texto da UEFA pretende formar as forças policiais em contexto de jogos de futebol e promover a cooperação policial internacional, tendo como destinatários comandantes policiais. O texto deverá ser lido por um orador, numa palestra. É constituído por cinco páginas e encontra-se dividido em parágrafos com várias extensões (mínimo de uma linha e máximo de sete). As diferentes secções que o integram são iniciadas por títulos em maiúsculas e, em diversas ocasiões, somos confrontados com expressões em negrito ou em maiúsculas, para que se dê mais relevância àquela informação durante a palestra. A terminologia deste texto é relacionada com o Direito, com as forças policiais e com o futebol, como é possível perceber através dos exemplos (14) a (17).

(14) Law enforcement services – Serviços responsáveis pela aplicação da lei

(15) Justice & Home Affairs Minister – Ministro da Justiça e dos Assuntos Internos

(16) National Football Information Point (NFIP) – Pontos nacionais de informação sobre futebol

(17) Riot police – Polícia de intervenção

As frases são predominantemente curtas e imperativas (*You need to define precisely how they fit into your plans.*), mas também se encontram diversas frases interrogativas, que funcionam, essencialmente, como estratégia de organização do texto (a resposta à questão é dada no próprio texto, como no caso da questão *What is realistic for you as commanders in the host cities to expect from colleagues in other countries in Europe?* à qual se segue a resposta *We need to make sure you are clear in your understanding of how the legal powers in other countries support you*.). Neste texto, encontram-se alguns problemas de escrita, nomeadamente de pontuação, verificando-se, por exemplo, a presença de vírgulas a separar o sujeito do predicado; os erros foram corrigidos na tradução.

CAPÍTULO DOIS

1. BREVE REFLEXÃO SOBRE A TRADUÇÃO

A **tradução** é uma actividade que envolve várias áreas, incluindo textos literários, técnicos, científicos, informativos, entre outros, bem como produções audiovisuais. Tal actividade remonta há muitos séculos, sendo as versões *Vetus Latina* e alexandrina da Bíblia, datadas do século II e III respectivamente, as primeiras traduções conhecidas. No glossário da obra de Crystal (1997: 439), a definição de tradução é a que se segue:

> *Translation (gen): 1. Conversion from one language into another.*
> *2. Conversion of written texts from one language into another.*

Esta definição não é totalmente satisfatória, uma vez que faz apenas referência explícita a textos escritos. Ora, é do conhecimento geral que a tradução não envolve unicamente textos escritos: a legendagem, a áudio-descrição e a sonorização são elas próprias formas de tradução e não envolvem necessariamente textos escritos.

A utilização da palavra *conversão* (*conversion* na citação acima) é uma boa forma de explicar o que é uma tradução, porque o tradutor deve adaptar a sua tradução à língua para a qual está a traduzir, quer se trate de uma língua falada, escrita ou gestual. Há expressões e palavras que não fazem sentido numa língua que não seja a original se forem traduzidas à letra. Tome-se como exemplo as expressões *it's raining cats and dogs* e *está a chover a potes*. Uma e outra significam o mesmo em línguas diferentes e fazem parte do conhecimento dos falantes dessa língua. Traduzi-las à letra não faria qualquer sentido, uma vez que os falantes do Português estranhariam a expressão *está a chover cães e gatos*. Neste sentido, a definição de tradução apresentada em Newmark (1988: 5) é mais rigorosa: "rendering the meaning of a text into another language in the way that the author intended the text". Por outras palavras, o tradutor tem que ser capaz de fazer a tradução do sentido do texto, tendo por base o que o autor queria dizer com o mesmo.

Roman Jakobson (1959) define três categorias distintas na tradução:

- *Tradução intralingual* ou reformulação

- *Tradução interlingual* ou tradução propriamente dita
- *Tradução intersemiótica* ou transmutação

A tradução intralingual consiste na interpretação dos elementos verbais por meio de outros elementos da mesma língua e acontece quando se recorre a outra palavra, mais ou menos sinónima, ou a uma perífrase. A tradução interlingual consiste na interpretação dos elementos verbais por meio de uma outra língua. Por fim, a tradução intersemiótica consiste na interpretação dos elementos verbais por meio de sistemas de elementos não-verbais, como acontece aquando da tradução de um texto escrito para um meio audiovisual. Ainda no mesmo ensaio, Jakobson aborda a questão da equivalência e refere que não há uma equivalência total entre as línguas do mundo, porque, embora possa existir a mesma palavra em todas elas, essa palavra não terá certamente o mesmo significado.

Uma perspectiva distinta da linguística estruturalista de Jakobson foi apresentada pela linguista alemã Katharina Reiss (1971). Trata-se uma visão funcionalista que defende que o que determina uma tradução não é o assunto do texto, mas sim a função do mesmo. É graças a Reiss (1984) e Vermeer (1986) e à sua *Skopostheorie* (teoria do *skopos*, ou finalidade, da tradução) que percebemos que nunca "será possível uma tradução sem objectivo bem definido e é este que, em todos os casos, determina a estratégia a adoptar para que tal objectivo seja obtido da melhor maneira possível nas circunstâncias de chegada. Não é o texto de partida o factor determinante, não o é a fidelidade a este, mas a 'fidelidade' ao objectivo, à intenção ao destino que se dá ao texto de chegada. O factor central de cada tradução é o texto de chegada." (Vermeer, 1986: 8). O tradutor assume, deste modo, mais importância no processo de tradução, servindo de mediador e tendo em consideração a finalidade da tradução, não apenas o texto de partida ou a lealdade ao mesmo.

A teoria de Vermeer e Reiss foi continuada e desenvolvida por Christiane Nord (1991), para a qual todas as traduções são instrumentais, embora se faça a distinção entre tradução documental e tradução instrumental. A tradução documental "serves as a document of a source culture communication between the author and the source text (ST) recipient" (Nord 1991: 72), ou seja, o destinatário apercebe-se de que o texto que lhe está a ser transmitido é uma tradução. Pelo contrário, a tradução instrumental "serves as an independent message transmitting instrument in a new communicative

action in the target culture, and is intended to fulfill its communicative purpose without the recipient being conscious of reading or hearing a text which, in a different form, was used before in a different communicative situation" (Nord, 1991: 73). Dito por outras palavras, nesta segunda acepção de tradução, o texto traduzido deve ser entendido como um original na língua de chegada. O destinatário do texto traduzido não se deve aperceber de que se trata realmente de um texto cujo original pertence a outra língua, mas deve lê-lo como um texto escrito na sua própria língua.

A tradução não é apenas a passagem de um texto de uma língua para outra sem se ter em atenção o conhecimento daqueles que serão os destinatários da obra traduzida. Por exemplo, na tradução portuguesa do livro *Harry Potter and the Philosopher's Stone* (Harry Potter e a Pedra Filosofal), a tradutora decidiu adicionar uma nota de rodapé para a referência Bonfire Night, uma festividade da Grã-Bretanha durante a qual se fazem fogueiras e lançam foguetes, que pode ser desconhecida para os leitores não britânicos se nessas culturas não existir um evento equivalente. O tradutor deve ter a preocupação de traduzir o significado das palavras e não apenas a sua tradução literal, devendo também ter em conta o contexto do texto e o sentido que o texto tem nesse contexto.

Todas as línguas conseguem traduzir tudo, nada é intraduzível. Porém, pode acontecer que o tradutor tenha que recorrer a empréstimos ou a notas de tradutor para que a compreensão do texto não seja perturbada. Cabe ao tradutor, enquanto mediador entre a língua/cultura de partida e a língua/cultura de chegada, fazer com que o sentido e a conotação atribuídas a um nome ou a uma expressão seja igualmente convertida para a língua para a qual se traduz. Por esta razão, Yebra (2004) considera que "la actividad del traductor consta de dos fases: la fase de la comprensión del texto original, en que el traductor trata de captar o entender el contenido del texto que se dispone a traducir, y la fase de la expresión del mismo contenido en la lengua terminal".

Ainda sobre o mesmo tema, Rónai (1956: 21) defende que "o tradutor deve conhecer todas as minúcias semelhantes da língua de seu original a fim de captar, além do conteúdo estritamente lógico, o tom exato, os efeitos indiretos, as intenções ocultas do autor". Segundo o mesmo autor, "a fidelidade alcança-se muito menos pela tradução literal do que por uma substituição contínua" (*ibid*.). Por isto, Rónai considera que "para ser fiel, o tradutor, além do indispensável conhecimento dos dois idiomas, precisa sobretudo de imaginação" (*ibid*.: 23).

O tradutor tem que ter conhecimento do destinatário do texto, para saber se a tradução daquele texto passa pela utilização de estrangeirismos com que o público-alvo já está familiarizado ou se pela procura de um equivalente, no caso de o haver, e pela utilização de notas de tradutor.

Para além de conhecer o destinatário do texto a traduzir, o tradutor tem que conhecer o tipo de texto com que trabalha. Para Adam (1992), um texto é composto por várias sequências, com autonomia relativa e que estabelecem entre si relações hierárquicas. Cada sequência tem uma organização interna própria e pode decompor-se em partes que se podem relacionar entre si e com a totalidade da unidade textual. Este autor propõe uma tipologia onde cada texto é uma unidade com várias sequências textuais que podem coexistir dentro do mesmo texto:

Estrutura	Objectivos/funções	Características	Exemplos
Narrativa	Relatar acontecimentos reais ou fictícios	Elementos de sucessão causal e temporal; deícticos temporais; verbos no presente de narração ou pretérito perfeito; mecanismos de introdução e manutenção dos referentes	Romances, novelas, notícias, relatórios
Descritiva	Dar uma imagem rigorosa e fiel de objectos, pessoas, ambientes ou situações não visíveis pelo leitor	Elementos de localização espacial e temporal; figuras de estilo; verbos estativos no presente e imperfeito; forte modificação nominal; predomínio de coordenação e justaposição.	Guias turísticos, descrição de um romance ou novela
Argumentativa	Defesa de uma opinião ou a persuasão do receptor	Verbos declarativos e acusativos; frases negativas, declarativas e interrogativas (retóricas); conectores lógicos; subordinação adverbial.	Teses, debates, editoriais
Explicativa	Intenção comunicativa e função informativa e didáctica	Verbos no presente; vocabulário de especialidade; perífrases; frases declarativas; sinónimos; aposições.	Manuais, artigos de divulgação, enciclopédias
Dialogal -conversacional	--------	----------	Diálogos numa peça de teatro, conversas telefónicas

Na tradução do manual de aconselhamento de segurança anti-terrorismo para hotéis e restaurantes, co-existem sequências descritivas e explicativas, sendo as características mais comuns a utilização de estruturas de coordenação e de justaposição,

como em (18), bem como forte presença de léxico especializado e de perífrases, como no exemplo (19):

(18) Os alvos mais prováveis são os locais de grande afluência de pessoas, lugares que sejam considerados simbólicos e instalações importantes onde pode ocorrer um elevado número de vítimas. (página 126, primeiro parágrafo) – No original: *The most likely targets are mass casualty crowded places, symbolic locations and key installations.*

(19) Treine-os para abrir o correio com abre-cartas (e com o mínimo de movimentos), para manter as mãos afastadas do nariz e da boca e para lavar sempre as mãos após o manuseamento da correspondência. (página 105) – No original: *Train them to open post with letter openers (and with minimum movement), to keep hands away from noses and mouths and always to wash their hands afterwards.*

A Internet é cada vez mais uma ferramenta importante para um tradutor, qualquer que seja a sua área de trabalho. Este instrumento permite ao tradutor a consulta de dicionários e enciclopédias aos quais poderia não ter acesso tão rápido se os mesmos apenas existissem em papel. Tomem-se como exemplos os casos de dicionários de calão ou dicionários de universidades e editoras conceituadas como a Oxford University Press, a Longman, a Mcmillan Publishers e a Merriam-Webster. Para além disto, a Internet possibilita ao tradutor a consulta de bases de dados e de bases terminológicas, bem como o contacto com especialistas da área do texto que se está a traduzir ou, inclusive, com outros tradutores, que podem nem se encontrar no mesmo país ou continente em que estamos. Permite igualmente a consulta de *sites* que disponibilizam *online* textos idênticos aos que o tradutor está a trabalhar (os chamados textos paralelos), o que se torna particularmente útil nos casos em que a tradução envolve designações de organismos ou termos técnicos, entre outros.

Há tradutores que se especializam nas diversas áreas da tradução e em domínios diferentes dentro dessas mesmas áreas, ou seja, um tradutor para legendagem pode

especializar-se em séries e documentários relacionados com a Medicina, mas não necessariamente em todos os textos sobre Medicina. É sobre uma das áreas da tradução, a tradução técnica, que nos debruçaremos em seguida.

2. A TRADUÇÃO TÉCNICA

Os textos técnicos estão presentes em diferentes áreas do conhecimento, desde a Medicina à Linguística, passando pelas Belas-Artes e pelo Direito.

Gamero Perez (2001: 28) afirma que os textos técnicos, bem como os textos científicos, são utilizados "para transmitir el conjunto de saberes proprios de una disciplina a los especialistas en formación o, en algunos casos, para divulgar unos conocimientos básicos entre el público general". O mesmo afirma Byrne (2006: 3), de acordo com a qual a tradução técnica é particularmente relevante nos domínios que lidam com a aplicação do conhecimento que provém da investigação em ciências naturais. Por isto, encontramos, como exemplos de textos técnicos, notícias, artigos científicos, enciclopédias, relatórios, correspondência e manuais de instruções, entre outros.

A **tradução técnica** pretende fazer com que o destinatário tenha um fácil acesso à informação do texto de partida, sem, no entanto, reproduzir o texto de partida no que diz respeito ao estilo ou à linguagem: "The purpose of technical translation is to present new technical information to a new audience, not to reproduce the source text, per se, or reflect its style or language. Technical translation is a communicative service provided in response to a very definite demand for technical information which is easily accessible (in terms of comprehensibility, clarity and speed of delivery)" (Byrne, 2006: 11).

Porém, a tradução técnica é normalmente vista como o "parente pobre" (*poor cousin*, em Byrne, 2006: ix) da "verdadeira" tradução (nas palavras da autora, *real translation*), sendo até vista como um tipo de tradução básica e fácil. Muito do trabalho realizado na área tem-se restringido a questões terminológicas ou técnicas, pelo que a tradução técnica é uma avenida de investigação teórica mais promissora do que se imagina (Byrne, 2006: 1).

Todos os tipos de tradução têm as suas especificidades e a tradução técnica não é excepção. A terminologia, característica saliente dos textos técnicos, é um elemento fundamental na tradução. No caso dos termos, em grande parte dos casos é possível encontrar equivalentes terminológicos. No entanto, quando se trata de denominações de leis ou cargos, por exemplo, o tradutor tem frequentemente de desenvolver pesquisa no sentido de encontrar o equivalente na língua de chegada, que pode ser idêntico à expressão da língua de partida ou não, caso em que é necessário encontrar estratégias que permitam ao leitor reconhecer as denominações em questão. Assim, por exemplo, uma lei com um nome equivalente em dois países (como o Reino Unido e Portugal) não é necessariamente igual no seu conteúdo, ou seja, pode ser mais ou menos extensa e referir ou não a mesma informação. A título ilustrativo, no Reino Unido, a *Data Protection Act* de 1998[2] faz referência à protecção de dados, sem especificar se estes são pessoais ou não[3]. Por seu lado, Portugal possui a Lei de Protecção de Dados (Lei n.º 67/98 de 26 de Outubro de 1998[4]) que se aplica apenas aos dados pessoais. O tradutor tem que pesquisar que lei se aplica no mesmo caso em Portugal ou manter a denominação do original, servindo-se de outros meios, como notas de tradutor, para deixar claro aos leitores a que se refere a dita lei.

Em todos os textos traduzidos, é importante fazer os possíveis para que os destinatários não se apercebam de que aquela é uma tradução. Porém, esta necessidade é ainda mais visível nos textos técnicos, porque "in the case of technical translation, all readers are concerned about is getting the information they need and being able to understand and use it effectively in order to do something else, usually some task relating to their day to day work" (Byrne, 2006: 15). O mesmo nos é dito por DeGeorge (1984: 1), que afirma que o público-alvo dos textos técnicos tem como principal interesse a capacidade do tradutor técnico de transmitir a informação com clareza e precisão e não a inteligibilidade do texto traduzido. Assim:

> "*the translation needs to function in precisely the same way as any other text in the target language. Readers are unlikely to show mercy to a translation that is obviously a translation just because it is a translation. This serves only to distract them from*

[2] Disponível em http://www.legislation.gov.uk/ukpga/1998/29

[3] Foram criadas várias disposições posteriores a esta lei e referentes a dados pessoais, mas que fazem sempre referência à *Data Protection Act*.

[4] Disponível em http://www.cnpd.pt/bin/legis/nacional/LPD.pdf

their primary concern: finding the information they need in the document and using it." Byrne (2006: 15)

Os textos técnicos são escritos por um especialista e podem destinar-se a outro especialista ou ao público em geral. Podem ser em formato escrito, audiovisual ou oral e têm características linguísticas variadas[5]:

- Forte presença de siglas e abreviaturas[6]
  - (20) CPNI (Centre for the Protection of National Infrastructure)
  - (21) MAI (Ministério da Administração Interna)
- Utilização de latinismos e estrangeirismos
  - (22) *per se*
  - (23) *download*
- Modificação pré e pós-nominal pesada
  - (24) Independent and impartial counter terrorism advice and guidance
  - (25) Materiais químicos, biológicos ou radiológicos
- Nominalizações
  - (26) Failure (de *fail*)
  - (27) Preocupação (de *preocupar*)
- Frases longas e complexas
  - (28) Managing the risk of terrorism is only one part of a hotel or restaurant manager's responsibility when preparing contingency plans in response to any incident in or near their premises which might prejudice public safety or disrupt normal operations.
  - (29) Sempre que possível, estabelecer o ponto de controlo de acessos de veículos distante do local protegido, implementando patrulhas regulares e instruindo o pessoal para que vigie alguém com um comportamento suspeito.
- Uso abrangente da passiva
  - (30) Extensive research has been carried out on the effects of blast on glass.
  - (31) Esta brochura foi desenvolvida pelo CPNI.

[5] A este propósito consultar Baakes (1994), Hoffmann (1991) e Zethsen (1999).

[6] Alguns dos exemplos que se seguem são retirados do manual traduzido no âmbito do estágio a que o presente relatório se reporta.

Os textos técnicos, no seu original e numa versão traduzida, têm uma função pragmática, porque pretendem comunicar algo a um destinatário e levar esse destinatário a realizar determinadas acções; cabe ao tradutor conhecer os objectivos do texto. Estão presentes nos mais diversos locais, desde empresas, escritórios e fábricas até manuais escolares e publicidade. De facto, os textos técnicos não se cingem a uma só área ou a um só tipo. Podemos encontrá-los em enciclopédias, relatórios, folhetos informativos, correspondência, especificações técnicas de produtos e processos, actas, manuais de instruções de uso, etc.

No século XX, devido à industrialização e à internacionalização da cooperação e do comércio, os textos técnicos e a tradução dos mesmos aumentaram significativamente. Todos os dias nos deparamos com novas traduções de todas as áreas, mas, mesmo que não nos apercebamos, estima-se que a tradução técnica equivale a 90% da percentagem total de traduções anuais (Byrne, 2006: 2).

Na tradução técnica, estão envolvidos textos precisos e é de extrema importância aquilo que se pretende transmitir. Se um tradutor técnico traduzir erradamente uma indicação referente a um procedimento científico ou militar, o seu lapso pode ter consequências desastrosas e dar azo à descredibilização desse mesmo tradutor.

Não é raro pensar-se que o tradutor deve ser um especialista em todas as áreas que traduz. É óbvio que, quanto maior for o conhecimento de um tradutor acerca de uma área, mais facilidade poderá ter em lidar com a terminologia dessa área, mas nem todos os tradutores técnicos traduzem textos de uma área apenas e muito dificilmente conseguiriam tornar-se em especialistas de todas essas áreas. Como afirma Byrne (2006: 5), baseando-se em Robinson (2003), "the translator should have enough knowledge either to know how to deal with the text or to be able to acquire whatever additional information is needed". Ainda segundo Byrne (2006: 6), o tradutor deve ter conhecimento da área, competências de escrita e de pesquisa, conhecimento dos géneros e tipos textuais e competências pedagógicas, e deve 'personificar' o autor original, que, muitas vezes, é um especialista numa determinada área. Por isto, o tradutor precisa de transmitir a mesma autoridade que esse especialista aquando da tradução, pelo que o desafio para o tradutor técnico é a pesquisa que este tem que realizar num determinado campo, quer no que diz respeito à terminologia quer relativamente ao modo de escrita dos especialistas desse campo.

A utilização de ferramentas de tradução assistida por computador, como o TRADOS e o Wordfast, permitem que o tradutor tenha um acesso rápido a traduções que já realizou e que possuem o mesmo termo ou, inclusive, as mesmas frases, sem que tenha a necessidade de traduzir essas mesmas frases uma segunda vez ou de procurar esse mesmo termo a Internet ou num glossário por si construído.

Nos últimos anos, as novas tecnologias têm provado ser um excelente apoio aos tradutores. A consulta de uma base terminológica, como o IATE (InterActive Terminology for Europe), que nos apresenta termos dos mais variados domínios, desde desde o Direito à indústria agro-alimentar, ou de um dicionário que envolva bases de dados (como o Linguee, que vai pesquisar os termos de consulta aos *sites* europeus EurLex e Europarl, de legislação da União Europeia e do Parlamento Europeu, respectivamente) em muito facilita a tradução de um texto técnico.

Alguns autores consideram que não existem diferenças entre textos técnicos e textos científicos. Embora ambos os tipos de textos possuam léxico especializado e sejam obra de um especialista, é aqui que acaba a semelhança entre eles. Gamero Perez (2001: 28) defende que os textos científicos "tienen la funcionalidad de difundir ampliamente los resultados de la investigación entre la comunidad de especialistas; por ejemplo a través de artículos, ponencias en congresos, o conferencias", algo que não acontece com os textos técnicos, cujo "ámbito de uso (…) es mucho más amplio, e incluye la producción de textos con el fin de contribuir a la organización de los procesos industriales (plan de producción, solicitud de desarrollo del producto, etc.), ofrecer información al usuario de los productos (manual de instrucciones, prospecto de medicamento), anunciar productos (publirreportaje, anuncio técnico, etc.), y otros muchos más". A mesma distinção é feita por Byrne (2006: 8), que refere que a tradução científica se refere apenas à parte teórica da ciência, enquanto a tradução técnica diz respeito à aplicação do conhecimento científico.

CAPÍTULO TRÊS

ANÁLISE DO MANUAL *CONSELHOS DE SEGURANÇA ANTITERRORISMO PARA HOTÉIS E RESTAURANTES*

Neste capítulo, serão apresentadas e comentadas algumas opções de tradução do manual de conselhos de segurança anti-terrorismo para hotéis e restaurantes, que, pela sua extensão, oferece mais possibilidades de análise do que o documento da UEFA sobre segurança em eventos futebolísticos. O capítulo está dividido em cinco grandes secções: questões lexicais, questões sintácticas, a expressão da modalidade, aspectos de coesão referencial e questões culturais.

Algumas ocorrências são mais recorrentes do que outras. No caso das primeiras, não será feita uma listagem exaustiva de todas as ocorrências daquela mesma situação, o que em alguns casos se tornaria impraticável.

1. QUESTÕES LEXICAIS

Nesta secção, serão apresentados e comentados exemplos de questões lexicais com que me deparei ao longo da tradução do manual. Primeiramente, serão apresentados problemas com o léxico especializado. Em seguida, apresentar-se-ão problemas relacionados com o léxico não especializado, nomeadamente no que diz respeito a formas de tratamento, perífrases, polissemia e falsos amigos e sinonímia. Na última secção, far-se-á referência à tradução de denominações e siglas.

1.1 Léxico especializado: a terminologia

O léxico comum distingue-se do léxico especializado pelo facto de pertencer à língua comum, que "é caracterizada pela polissemia, ambiguidade, redundância, multiplicidade situacional e temática" (Contente, 2008: 33). Pelo contrário, o léxico

especializado pertence à língua de especialidade, que "é um conjunto de meios linguísticos utilizados numa situação de comunicação de uma determinada especialidade, a fim de assegurar a comunicação entre os seus pares" (*ibid*.). Contente acaba esta matéria citando Wimmer, que refere que a língua de especialidade difere "da língua comum através dos seguintes aspectos: precisão, univocidade denominativa, economia, relação matéria/objecto" (Wimmer, 1982: 17, *apud* Contente, 2008: 33). Esta definição de língua especializada é particularmente clara em Cabré (1998: 59):

> *"We speak of special or specialized languages to refer to a set of subcodes (that partially overlap with the subcodes of the general language), each of which can be specifically characterized by certain particulars such as subject field, type of interlocutors, situation, speakers' intentions, the context in which a communicative exchange occurs, the type of exchange, etc. Situations in which special languages are used can be considered as marked."*

As áreas técnicas e científicas têm duas coisas em comum no que diz respeito ao vocabulário que delas faz parte: todas elas utilizam palavras do léxico comum e todas têm a sua própria **terminologia**. Como nos diz Newmark (1998: 152), "the central difficulty in technical translation is usually the new terminology". A terminologia pode ser entendida como "las palabras propias de un campo de especialidad, que caracteriza y diferencia a un determinado colectivo o grupo de profesionales frente a otro, aparte de las peculiaridades específicas en lo que a estilística y estructura formal del texto se refiere" (San Salvador, 1998).

Os textos técnicos, sendo ricos em terminologia, fazem com que os tradutores dos mesmos necessitem de ter acesso a esse vocabulário, para que o texto traduzido chegue aos especialistas da área da mesma forma que o original. Devido a isto, Cabré (1998: 48) refere que a "terminology prepared for translators must contain contexts that provide information on how to use the term, and, ideally, provide information about the concept in order to ensure translators use the precise term to refer to a specific content".

A unidade terminológica é o termo, que "corresponde teoricamente apenas a um conceito" (Contente, 2008: 35). Note-se, no entanto, que, mesmo que apenas haja um

termo na língua de partida, esse mesmo termo pode ter várias acepções na língua de chegada, pelo que a informação acerca do conceito a que Cabré (1998) faz referência na citação do parágrafo anterior é importante para que o tradutor – e em especial o tradutor técnico – saiba que acepção desse mesmo termo na língua de chegada deve escolher para a sua tradução. Porém, não podemos esquecer que "a unidade terminológica apresenta, por vezes, os traços comuns com as palavras do vocabulário corrente" (Contente, 2012: 60).

Como qualquer outro tradutor, o tradutor técnico tem que ter um conhecimento profundo das línguas com que trabalha, sejam as de partida ou as de chegada. Não pode apenas apoiar-se em dicionários comuns para a sua tradução, porque não sabe se o termo que aparece no original tem mais alguma tradução do que a que aparece nesse dicionário.

A tradução do manual fez com que fosse necessária a pesquisa de terminologia de diversas áreas, como se ilustra de seguida:

- Direito
  - (32) Legal action – Via judicial
  - (33) Criminal injury – infracção penal
- Indústria
  - (34) Flying glass – estilhaços de vidro
  - (35) Pulping – Desfibração
- Defesa
  - (36) Mortar – morteiro
  - (37) Reconnaissance – reconhecimento
- Actividade económica
  - (38) Outsourcing – externalização
  - (39) Trade bodies – organizações empresariais
- Emprego
  - (40) Pre-employment check – verificação dos antecedentes laborais
  - (41) Recruitment – selecção do pessoal
- Energia
  - (42) Uninterrupted power supply (UPS) – Unidades de alimentação ininterruptas

- Informática
    (43) Trojan – *trojan*
    (44) Disk drive – unidade de disco
- Transportes
    (45) Traffic-calming – redução do ruído de trânsito
    (46) Maintenance hatch – escotilha de manutenção

As traduções apresentadas não foram todas conseguidas nas mesmas fontes. A maioria dos termos (como os dos exemplos (32), (35), (36), (37), (38), (44) e (45)) foram traduções encontradas no IATE. Foram também encontradas traduções no EurLex e no Europarl, através do Linguee (cf. (33) e (39)); outros termos, como os dos exemplos (34) e (40), foram obtidos através da consulta do glossário de Cruz (2012). Alguns termos foram propostos pela Dr.ª Cristina Reis, como aconteceu com os exemplificados em (41) e (46). Foi ainda feita pesquisa de termos em revistas da especialidade (PCGuia) e em *sites* de instituições relacionadas com os assuntos abordados no manual (Bernardo da Costa (Comércio de Equipamentos de Segurança) e ActiveCard).

1.2 Léxico não especializado

Como já vimos, o léxico especializado coloca diversos problemas à tradução. Porém, o mesmo acontece com o léxico não especializado, por diversos factores que se prendem com "o seu sentido literal (denotação), (…) o seu sentido expressivo, ou seja, os valores que pode invocar (conotação), a sua capacidade polissémica, o grau de ocorrência com outras palavras (colocações), assim como a influência que o contexto exerce sobre [uma palavra]" (Sá, 2012: 50).

Nesta secção sobre léxico não especializado, começaremos por abordar as diferenças entre as formas de tratamento na língua de partida e na língua de chegada; em seguida, serão apresentados casos em que foi necessária a tradução por perífrase;

trataremos as palavras polissémicas e os falsos amigos, sendo a secção finalizada com uma subsecção sobre sinonímia.

1.2.1 Formas de tratamento

As formas de tratamento podem colocar problemas aquando de uma tradução, porque estão dependentes de determinados estilos ou registos, "com características específicas a nível fonológico e prosódico, lexical, morfológico e sintáctico" (Duarte, 2000: 356). Estes estilos e registos, por sua vez, são condicionados por factores não linguísticos que nos levam a utilizar *V. Ex.ª* em contextos onde não utilizaríamos uma forma mais impessoal, como *tu*. Entre esses factores não linguísticos estão a situação, a relação social entre os participantes e o grau de proximidade ou de distância entre eles. (*ibid*.).

O pronome pessoal de segunda pessoa em Inglês, *you*, não pode, no contexto da tradução em questão, ser traduzido como *tu* ou *você*, os equivalentes directos em língua portuguesa, porque ambos são muito informais. A opção mais frequente foi a de eliminar a utilização de um pronome expresso, obtendo-se frases com sujeito nulo, construção permitida pela gramática do Português, como é possível verificar nos exemplos (47) a (51).

(47) Contudo, se considerar que está vulnerável a um atentado, deve aplicar medidas de segurança apropriadas para reduzir o risco ao mínimo possível. (página 88) – No original: *If, however, you assess that you are vulnerable to attack, you should apply appropriate protective security measures to reduce the risk to as low as reasonably practicable*.

(48) Quaisquer que sejam as circunstâncias, deve dizer à polícia, tão rapidamente quanto possível, o que vai fazer. (página 108) – No

original: *Whatever the circumstances, you should tell the police as soon as possible what action you are taking*.

(49) Se levou a cabo uma avaliação dos riscos da segurança do pessoal, isto ajudá-lo-á a decidir quais os níveis de controlo apropriados para os diferentes postos. (página 113, separador 'Política de controlo dos antecedentes laborais') – No original: *If you have conducted a personnel security risk assessment then this will help you to decide on the levels of screening that are appropriate for different posts.*

(50) Se utilizar adjudicatários, [deve] assegurar-se de que o equipamento e os procedimentos estão de acordo com as normas. (página 121, caixa de texto) – No original: *If you use contractors, ensure that their equipment and procedures are up to standard*.

(51) O que pode fazer (página 121, caixa de texto) – No original: *What you can do*

Quando a construção de sujeito nulo não se revelou a opção mais adequada, como em (52), a decisão de tradução pendeu sobre a inserção de expressões nominais que remetem directamente para os destinatários do manual, como *o leitor*.

(52) Este guia (…) destaca o papel vital que o leitor pode desempenhar na estratégia do Reino Unido contra o terrorismo. (página 85, primeiro parágrafo) – No original: *This guide (…) highlights the vital part you can play in the UK counter terrorism strategy.*

Veja-se que, em (52), a opção por um sujeito nulo daria lugar a uma interpretação inadequada, visto que, nesse caso, o pronome relativo *que* seria interpretado como sujeito da relativa e teria como antecedente o SN *Este guia*. Ora, a interpretação

pretendida é a de que o leitor do guia (e não o guia) pode desempenhar um papel vital na estratégia contra o terrorismo.

A questão da pessoa a utilizar reflectiu-se, também, na escolha dos determinantes e pronomes possessivos que remetem para o leitor. Se compararmos as gramáticas do Inglês e do Português, verificamos que o determinante possessivo é obrigatório na primeira língua, em contextos em que a segunda pode dispensá-lo. Colocar na tradução deste manual todas as ocorrências de determinantes possessivos faria com que o texto se identificasse pouco com as regras de uso dos possessivos em Português. Assim, sempre que tal não afectava a interpretação requerida, decidiu-se pela eliminação dos determinantes possessivos na tradução, como nos exemplos (53) a (56).

(53) O que é que o serviço de polícia local lhe pode dizer sobre delitos e outros problemas na sua área? (página 89, quinta marca) – No original: *What can <u>your</u> local Police Service tell you about crime and other problems in your area?*

(54) Deve monitorizar constantemente as imagens captadas pelo sistema de CCTV. (página 100, segundo parágrafo) – No original: *You should constantly monitor the images captured by <u>your</u> CCTV system*

(55) Mantenha as cassetes durante 31 dias, pelo menos. (página 101, sexta marca) – No original: *Keep <u>your</u> tapes for at least 31 days.*

(56) Procure o aconselhamento do CTSA da polícia local acerca da ameaça e de medidas defensivas. (página 104, Planeamento dos procedimentos de tratamento de correspondência) – No original: *Seek advice from <u>your</u> local police Counter Terrorism Security Adviser (CTSA) on the threat and on defensive measures*.

Nos casos em que o pronome é necessário por questões de interpretação, como em (57) e (58), optou-se pela tradução através do determinante possessivo de terceira pessoa com referência a segunda pessoa.

(57) É possível que o seu hotel ou restaurante possa vir a estar envolvido num incidente terrorista. (página 85, terceiro parágrafo) – No original: *It is possible that your hotel or restaurant could be involved in a terrorist incident.*

(58) Em casos excepcionais, a polícia pode insistir na realização da evacuação, embora deva fazê-lo sempre em conjunto com o seu gestor de segurança. (página 108, quinto parágrafo) – No original: *In exceptional cases they may insist on evacuation, although they should always do so in consultation with your security manager.*

Em (58), especificamente, decidiu-se manter o pronome possessivo porque, na sua ausência, podia considerar-se que apenas havia um gestor de segurança para todos os estabelecimentos daquela zona, o que não corresponde à realidade.

1.2.2 Perífrase

Segundo Fawcett (1997: 45), a perífrase, a que o autor chama *amplification*, é uma estratégia que devemos utilizar para "providing explanations rather than making cultural adaptations as a strategy for bridging anticipated gaps in the target-language audience's knowledge". Esta estratégia é sobretudo utilizada quando um tradutor não se pode servir de notas de rodapé para explicitar o que o autor pretende com o emprego de uma determinada palavra ou expressão. O mesmo autor dá-nos o exemplo de um tradutor que utilizou a frase *fazia lembrar a Jangada da Medusa*[7], muito embora haja

[7] A Jangada da Medusa é um quadro de Theodore Géricault que retrata o naufrágio da fragata real Medusa e a luta dos sobreviventes numa pequena jangada.

leitores que não sabem o que significa (*ibid*.), para nos explicar que, antes de se recorrer a uma tradução literal, o tradutor deve procurar mais a fundo o significado da expressão com que se deparou.

Em (59) e nos exemplos seguintes, foi necessário proceder-se à introdução de palavras que não constavam no original, quer como forma de explicitação quer como forma de evitar a ambiguidade[8].

(59) Aconselhe-se junto do CTSA da polícia local sobre o que devem ser estas barreiras e sobre outras medidas que pode tomar, como a vigilância eletrónica, incluindo o ANPR e a proteção contra estilhaços de vidro. (página 123, caixa de texto) – No original: *Seek the advice of your local Police Counter Terrorism Security Adviser (CTSA) on what these should be and on further measures such as electronic surveillance including Automatic Number Plate Recognition (ANPR) and protection from flying glass.*

Em (59), a decisão pela utilização da perífrase deveu-se à necessidade que parecia haver de explicitar que o CTSA deveria ter conhecimento não de todas as medidas mas sim das medidas que o leitor pode tomar para aumentar a protecção do seu hotel ou restaurante.

Veja-se agora o exemplo (60):

(60) Considere os pontos seguintes quando fizer o planeamento relativamente a um incidente com instrumentos de ataque/armas de fogo: (página 128, Planeie) – No original: *Consider the following when planning for a firearms/weapons incident:*

[8] Os casos que requereram uma modificação da frase pela utilização de constituintes com propriedades de selecção específicas (e que poderão fazer com que seja necessária a adição de outros constituintes) serão tratados mais à frente.

Também em (60) se decidiu explicitar a frase na língua de chegada, adicionando-se informação que não constava do original. Acrescentar o substantivo *pontos* teve como objectivo esclarecer que *seguinte* se referia aos pontos que se seguiam e não ao restante texto.

Por seu lado, no exemplo (61) optou-se pela utilização de uma perífrase para evitar a ambiguidade. Se se tivesse mantido apenas *depois*, o leitor podia entender esse *depois* como referindo o momento posterior àquele em que se localiza a situação denotada por *manter as mãos afastadas do nariz e da boca* ou o momento posterior ao do manuseamento da correspondência. Como a primeira não era de todo o que se pretendia com o texto original, decidiu-se pela expansão da frase na tradução.

(61) Treine-os para abrir o correio com abre-cartas (e com o mínimo de movimentos), para manter as mãos afastadas do nariz e da boca e para lavar sempre as mãos <u>após o manuseamento da correspondência</u>. (página 105) – No original: *Train them to open post with letter openers (and with minimum movement), to keep hands away from noses and mouths and always to wash their hands <u>afterwards</u>.*

No caso do exemplo (62), por sua vez, a perífrase teve como objectivo ajudar à compreensão do que é a ricina, tornando-se, portanto, numa estratégia de explicitação. Uma construção mais semelhante à do original não facilitaria o entendimento, pelo que se decidiu colocar o sintagma nominal, *a ricina*, em primeiro lugar e colocar a restante informação num modificador apositivo, *uma toxina encontrada em plantas*, como forma de explicitação:

(62) Doenças causadas pela libertação deliberada de bactérias, vírus ou fungos perigosos ou de toxinas biológicas como <u>a ricina, uma toxina encontrada em plantas</u>**.** (página 124, Biológicos) – No original:

Illnesses caused by the deliberate release of dangerous bacteria, viruses or fungi, or biological toxins such as the plant toxin ricin.

A perífrase em (63) é diferente dos casos anteriores e teve um objectivo distinto:

(63) Encontra-se regularmente com o pessoal e discute com este as questões de segurança? (Anexo G, página 142) – No original: *Do you regularly meet with staff and discuss security issues?*

Neste caso, introduziu-se o complemento do verbo *discutir*, uma vez que a sua omissão poderia levar a uma interpretação não pretendida, a de que as questões de segurança seriam discutidas com um indivíduo não específico.

Por último, no exemplo (64), a explicitação deveu-se ao facto de o leitor poder inferir, através de uma tradução mais próxima do original, que são os veículos que são hostis, ao invés do atentado propriamente dito.

(64) Há barreiras físicas instaladas para manter todos os veículos excepto os autorizados a uma distância segura e para mitigar um possível atentado hostil com utilização de veículos? (Anexo B, página 135) – No original: *Do you have in place physical barriers to keep all but authorized vehicles at a safe distance and to mitigate against a hostile vehicle attack?*

Neste exemplo, estamos perante a modificação de um nome através de outro nome, *vehicle attack*, e o adjectivo, *hostile*, na posição em que se encontra, pode modificar ambos os nomes ou apenas *vehicle*. Para evitar a ambiguidade, alterou-se a ordem de palavras, colocando-se o adjectivo numa posição em que modifica

exclusivamente o nome *atentado*, e expandindo-se o modificador *vehicle* através de um sintagma preposicional, *com utilização de veículos*.

Considere-se, finalmente, o exemplo (65):

(65) As câmaras de CCTV <u>são alvo de manutenção</u> regularmente? (Anexo C, página 138) – No original: *Do you have your CCTV cameras regularly <u>maintained</u>?*

Em (65), foi necessário modificar a estrutura da frase na tradução. A tradução de *maintain*, segundo o Dicionário de Inglês-Português (2009: 580) é, relativamente a manutenção, *conservar em bom estado*. Em Inglês, podíamos ter como resposta *I (don't) have my CCTV cameras maintained*. Ter em Português a pergunta *tem as câmaras de CCTV conservadas em bom estado?* e a resposta *(não) tenho as câmaras de CCTV conservadas em bom estado* podia ser uma opção de tradução. Porém, mesmo se a escolha de tradução tivesse recaído sobre a tradução apresentada, conservar as câmaras de CCTV em bom estado não é o mesmo que fazer com que estas sejam alvo de manutenção regularmente, pelo que optámos pela perífrase.

1.2.3 Polissemia e falsos amigos

A polissemia, como já referimos na secção sobre léxico especializado, é uma característica da língua comum (Contente, 2008: 33). As palavras polissémicas apresentam "vários significados (mais do que um), sendo possível estabelecer uma relação entre esses vários significados" (Correia, 2001: 1). Não são raros os casos de palavras que são polissémicas; basta-nos consultar um dicionário para nos darmos conta deste factor. Como a mesma palavra pode ter vários significados, o tradutor deve saber escolher o significado correcto e evitar a ambiguidade. Para tal, é importante a consulta de bons dicionários, em papel ou *online*, e, sobretudo, conhecer o contexto linguístico e situacional em que a palavra ocorre.

No texto em questão, a polissemia mais evidente foi a da palavra *concerned* no exemplo (66).

(66) Uma estratégia relativa às comunicações e aos meios de comunicação social inclui lidar com perguntas de familiares e amigos dos envolvidos. (página 92, última marca) – No original: *A communications and media strategy which includes handling enquiries from concerned family and friends.*

Concerned tem várias acepções em língua portuguesa. A tradução mais comum da palavra em Inglês é *preocupado* e foi essa a tradução inicial, uma vez que a frase não se tornaria agramatical se esse termo fosse utilizado. Todavia, não é esse o sentido que se pretende transmitir, visto que considerámos que o adjectivo se referia às vítimas envolvidas nos ataques e não a uma característica dos familiares e amigos dessas vítimas. Por isso, foi decidido traduzir aquela palavra como *envolvidos*, uma vez que a primeira tradução não faria sentido no contexto em questão.

Quanto aos falsos amigos, são palavras "que se correspondem etimologicamente de uma língua à outra, mas que têm sentidos diferentes" (Contente, 2008: 260), ou seja, palavras com uma grafia semelhante nas duas línguas que, porém, têm um significado diferente. Os falsos amigos podem levar a erros de tradução, porque como Fawcett (1997: 43) afirma, estes "are a fact of the language system not of translation competence". Muito embora os falsos amigos não tenham directamente a ver com competências de tradução, o tradutor deve estar ciente de que eles existem e, mais uma vez, deve fazer uso de bons dicionários para não cair neste erro a que pode ser levado pela semelhança entre uma palavra e a outra.

Os exemplos (67) e (68) ilustram os casos de falsos amigos encontrados aquando da tradução do manual de segurança.

(67) A poda da vegetação e das árvores, em especial perto das entradas, vai ajudar na vigilância e prevenir a ocultação de quaisquer embalagens. (página 96, sétimo parágrafo) – No original: *Pruning all vegetation and trees, especially near entrances, will assist in surveillance and prevent concealment of any packages.*

(68) Utilizar as listas de verificação de boas práticas nas páginas seguintes, que o ajudam na tomada de decisões. (página 135, terceira marca) – No original: *Make use of the good practice checklists on the following pages to assist you in your decision making process*.

To assist é, no caso do verbo transitivo, *to help (someone)*, e, no caso do verbo intransitivo, *to help by providing money or information* e *be present as a helper*[9]. No Dicionário de Inglês-Português (2009: 62), a tradução é, no caso do verbo transitivo, *ajudar, auxiliar* e *prestar assistência* e *ajudar* no caso do verbo intransitivo. Note-se que este dicionário também nos indica que a tradução do verbo intransitivo como *ajudar* ou *estar presente* é arcaica. Em (67) e (68), a primeira tradução, influenciada pelo texto de partida, foi *assistir*. Porém, e como estamos perante um verbo transitivo, a tradução como *assistir* não é a correcta e, numa revisão da tradução, modificou-se para *ajudar*.

1.2.4 Sinonímia

A sinonímia é, nas palavras de Mateus e Xavier (1992: 351), a "relação de sentido entre duas ou mais unidades lexicais cujo significado é idêntico ou que podem ser utilizadas individualmente num mesmo contexto sem que com isso se verifique uma alteração no significado da frase". Um sinónimo não é uma palavra que quer dizer o mesmo que outra, apenas que tem aproximadamente o mesmo significado que essa outra palavra.

A sinonímia coloca vários problemas à tradução, porque, para seleccionar o equivalente na língua de chegada, o tradutor precisa de ter em conta o contexto

[9] http://www.oxforddictionaries.com/definition/english/assist?q=assist

linguístico, o grau de formalidade entre os participantes do texto e o registo, mas também o estilo que deve utilizar e as "preferências mais ou menos idiossincráticas, contextuais e textuais" (Vilela, 1994: 29).

A sinonímia pode ser interlinguística, quando se verifica entre duas línguas diferentes, ou intralinguística, se ocorrer dentro da própria língua. Nas palavras de Contente (2008: 233), "o conceito de sinonímia interlinguística proposto por Wuster, Dubuc, Rey, Koucorek designa as diferentes denominações usadas em duas ou mais línguas para exprimir o mesmo conceito". A sinonímia intralinguística, por sua vez, é "a sinonímia no interior de um mesmo sistema linguístico em que a identidade conceptual das denominações concorrentes é fundamental" (Contente, 2008: 185). Isto quer dizer que, numa língua, várias palavras podem ser utilizadas para representar um determinado conceito.

É na sinonímia intralinguística que nos focaremos neste ponto. A frase (69) ilustra um dos casos de sinonímia intralinguística encontrados.

(69) Pessoas que '<u>namorem</u>' bebidas e prestem demasiada atenção às imediações. (página 131) – No original: *People '<u>nursing</u>' drinks.*

Nurse significa cuidar, amamentar ou, inclusive, fomentar. Ora, nenhum destes verbos é adequado à frase (69), porque não é apropriado que alguém está a cuidar de uma bebida. Chegar a uma adaptação que não soasse estranha no contexto português não foi fácil. Foi decidido traduzir por *namorar* visto que é um verbo que diz respeito a uma acção que demora algum tempo (um namoro) e que, por isso, pode ser entendida como uma demora mais prolongada do que o normal para acabar uma bebida.

Veja-se, agora, o exemplo (70):

(70) Proteja os espaços em redor e outras áreas vulneráveis. (página 128, Controle) – No original: *Secure your immediate environment and other vulnerable areas.*

Primeiramente, decidiu-se traduzir a expressão sublinhada em (70) como *ambiente*. Porém, esta tradução não pareceu muito correcta, mesmo que o leitor conseguisse, ao fim de algum tempo, chegar ao que se pretendia designar por aquela expressão. Um *espaço* parece ser mais físico do que um *ambiente*, uma vez que o segundo pode designar algo mais vago, como a ar que respiramos (que, apesar de sabermos que está lá, não é visível) ou aquilo que nos cerca (não apenas os objectos, os cheiros e os sons). *Espaço*, neste contexto, é tido como uma área perto daquela em questão, pelo que considerámos ser a opção mais adequada.

Passemos agora à análise do exemplo (71):

(71) Os espaços protegidos podem oferecer abrigo contra explosões, estilhaços de vidro e outros fragmentos. (página 110, Espaços protegidos) – No original: *Protected spaces may offer the best protection against blast, flying glass and other fragments.*

Relativamente a (71), não há nada na língua portuguesa que impeça que se diga *espaços protegidos oferecem protecção* e, aliás, é mais ou menos isso que nos surge no original. Sobretudo na oralidade, não são raros os casos em que ouvimos (até mesmo nos meios de comunicação social) construções semelhantes e que nos causam estranheza, em virtude do pleonasmo (no caso de (71), *protegidos / protecção*). Foi por esta razão que se decidiu modificar a frase e utilizar *abrigo* em vez de *protecção*, uma vez que o seu emprego não altera o significado da frase nem a sua compreensão.

Nos exemplos (72) e (73), a escolha da tradução de *business* por *negócio*, no primeiro, ou por *empresa*, no segundo, teve em conta o contexto em que a palavra surgia:

(72) Muitas [organizações] dependem dos seus sistemas de informação para realizarem negócios ou levar a cabo funções críticas a nível nacional e para gerir os sistemas de segurança e engenharia. (página 117, primeiro parágrafo) – No original: *Many [organisations] rely on their information systems to carry out business or nationally critical functions and manage safety and engineering systems*.

(73) Como no Passo Um, tenha em consideração se há ou não uma característica da sua empresa ou das suas atividades que os terroristas possam querer utilizar para os ajudar ou para financiar o seu trabalho. (página 89, último parágrafo) – No original: *As with Step One, consider whether there is an aspect of your business or activities that terrorists might want to exploit to aid or finance their work*.

Em (72), a expressão *realizar empresas* seria desadequada, pelo que a escolha recaiu sobre *negócios*. Em (73), por outro lado, uma tradução de *business* por *negócio* podia ser entendida como uma redundância face ao substantivo *actividades*, pelo que pareceu mais apropriada a tradução por *empresa*.

1.3 Denominações e siglas

Uma das tarefas mais morosas e que mais dúvidas suscitou foi a tradução das denominações das leis, dos cargos e dos organismos que o texto incluía.

A maioria dos cargos, das instituições e das leis não tinham tradução já estabelecida em língua portuguesa ou, no caso das leis, a correspondência não era total no que diz respeito a uma lei com um nome aparentemente equivalente. Newmark (1988: 81-83) refere as estratégias que estão à disposição do tradutor, para além da tradução literal e entre as quais se incluem a *transference*, ou seja, a utilização da palavra da língua de partida na tradução (normalmente utilizada no caso de nomes

próprios[10], topónimos, gentílicos, nomes de jornais (New York Times, Le Monde, etc.) e nomes de instituições públicas ou privadas que não tenham uma tradução institucionalizada), a *naturalisation*, a adaptação de uma palavra à pronúncia normal de uma língua, e o *cultural equivalent*, que é a tradução de uma palavra da língua/cultura de partida pelo equivalente da língua/cultura de chegada. A mais utilizada na tradução das denominações e siglas presentes no manual traduzido foi a de *transference*, ou seja, foram mantidas as referidas denominações da língua de partida, uma vez que não existem equivalentes para as mesmas na língua de chegada (em alguns casos, não existe sequer um equivalente próximo, como acontece com o termo *Gold Commander*, cargo que não existe em Portugal). No final do manual traduzido, foi introduzida uma lista que integra todas as denominações em inglês e uma tradução possível em português. Esta opção resultou de uma decisão conjunta com a Dr.ª Cristina Reis**.**

No que diz respeito às instituições, o texto original inclui frequentemente as siglas correspondentes. As siglas "são constituídas por iniciais de certas unidades lexicais ou termos muito longos de modo a serem reproduzidos na sua totalidade; são uma consequência da economia do sistema linguístico e do próprio uso" (Contente, 2008: 263). Foi decidido com a Dr.ª Cristina Reis manter a sigla em Inglês em todas as ocorrências da mesma na tradução, surgindo a respectiva tradução na lista atrás referida (que inclui as denominações de leis, cargos e instituições). A este propósito, considerem-se os exemplos seguintes:

(74) Centre for the Protection of National Infrastructure (CPNI) – Centro para a Protecção das Infra-estruturas Nacionais

(75) National Counter Terrorism Security Office (NaCTSO) – Gabinete Nacional de Segurança Antiterrorismo

(76) Security Industry Authority (SIA) – Autoridade da Indústria de Segurança

[10] Em certos casos, opta-se pela tradução do nome próprio, nomeadamente nos nomes de Papas (Leão XII, João Paulo II, etc.) e nos nomes de alguns monarcas (Rainha Isabel II, **mas** Príncipe Harry).

(77) Gold Commander/Strategic Commander – Comandante Estratégico

(78) Immigration, Asylum and Nationality Act 2006 – Lei relativa à Imigração, Asilo e Nacionalidade de 2006

(79) Operation Lighting – Operação Relâmpago

Algumas traduções foram retiradas do glossário de Cruz (2012) ou, após uma primeira tradução, corrigidas pela Dr.ª Cristina Reis, devido ao conhecimento mais profundo do assunto que a mesma tem. Não existindo uma tradução já instituída em Português, não pareceu oportuno arranjar uma nova sigla para a versão traduzida. Com efeito, a utilização da sigla original pode facilitar a compreensão dos leitores, se já antes se tiverem deparado com a mesma. Quando não foi facultada nenhuma tradução, coube-nos apresentar propostas de tradução, que se encontram nos exemplos abaixo:

(80) Automatic Number Plate Reader (ANPR) system – Sistema de leitura automática de matrículas

(81) Police Search Adviser (POLSA) – Conselheiro da Polícia em matéria de Buscas

(82) Fire (Scotland) Act 2005 – Lei contra Incêndios (Escócia) de 2005

(83) Regulatory Reform (Fire Safety) Order 2005 – Ordem de Reforma Regulamentar (Segurança contra Incêndios) de 2005

(84) Home Office Scientific Development Branch (HOSDB) – Gabinete para o Desenvolvimento Científico do Ministério da Administração Interna

A única excepção a esta opção foi a tradução imediata de *Home Office* por Ministério da Administração Interna e pela respectiva sigla, MAI. A escolha deveu-se ao facto de este ser um organismo com correspondência conhecida e imediata em Português, e que embora faça parte do domínio político, é um termo com que o público em geral está familizarizado.

2. QUESTÕES SINTÁCTICAS

O objectivo da sintaxe é "caracterizar o tipo de conhecimento que suporta a nossa capacidade de compreender e produzir combinações livres de palavras" (Duarte, 2000: 121). O conhecimento sintáctico é intuitivo e permite-nos, mesmo diante de uma construção frásica composta por itens lexicais desconhecidos, saber se essa frase é possível na língua ou não.

Nesta secção, analisaremos alguns aspectos sintácticos que consideramos relevantes para a nossa tradução: alteração à ordem de palavras, propriedades de selecção dos itens lexicais, construções com verbos leves e estruturas de coordenação múltipla. Em todos os casos, procede-se a uma descrição comparada entre as estruturas do Inglês (língua de partida) e as do Português (língua de chegada).

2.1 Alteração à ordem de palavras

A língua portuguesa e a língua inglesa são ambas línguas sujeito-verbo-objecto (SVO). No entanto, há características que distinguem as duas línguas quanto à ordem de palavras, como a posição dos adjectivos, pré- e/ou pós-nominais em Português, mas pré-nominais em Inglês quando não acompanhados de complementos.

Nos exemplos (85) e (86), e como aconteceu várias vezes ao longo da tradução, inverteu-se a posição dos adjectivos, sempre que a língua portuguesa o permite:

(85) Conselhos de segurança antiterrorismo (título) – No original: *Counter Terrorism Protective Security Advice*

(86) Enviar uma mensagem para as equipas de buscas através de um sistema sonoro para comunicações públicas (as mensagens devem ser codificadas para evitar perturbações e alarme desnecessários). (página 107, primeira marca) – No original: *Send a message to the search teams over a public address system (the messages should be coded to avoid unnecessary disruption and alarm).*

Durante a tradução do manual sobre segurança anti-terrorismo em hotéis e restaurantes, foi por vezes necessário inverter a ordem relativa entre sujeito e verbo. Em (87), por exemplo, e apesar de o sujeito estar em posição pré-verbal em Inglês, foi decidido colocá-lo em posição pós-verbal em Português.

(87) Estão à disponibilidade do SECCO variados recursos e opções, que incluem a comunicar com a gerência do hotel ou restaurante, identificar os indivíduos, as agências e os departamentos mais importantes envolvidos no evento, bem como procurar aconselhamento do CTSA relevante. (página 133, Police Security Co-ordinator (SECCO)) – No original: *A number of options and resources are available to the SECCO, which will include liaison with hotel or restaurant management, identifying all the key individuals, agencies and departments involved in the event as well as seeking advice from the relevant CTSA.*

Neste caso particular, a ocorrência da relativa obriga à adjacência entre o pronome relativo e o antecedente (*variados recursos e opções*). Manter a ordem do original levaria a considerar que o antecedente era SECCO, o que não só não corresponde à informação pretendida como também o resultado seria agramatical, uma vez que o

pronome relativo, em posição de sujeito, seria singular, dado que o antecedente seria também no singular, e o verbo se encontra no plural.

2.2 Propriedades de selecção dos itens lexicais

Em certas ocasiões ao longo do texto, houve a necessidade de alterar a construção frásica na tradução devido às propriedades de selecção dos itens lexicais. Esta secção é dedicada a alguns desses casos e às soluções tomadas para os resolver.

Certos itens lexicais condicionam a ocorrência de um certo número de expressões, bem como as propriedades sintácticas e semânticas dessas expressões. Sabemos, por exemplo, que dois verbos com um significado semelhante podem ter propriedades de selecção categorial diferentes, ou seja, seleccionam complementos de categoria diferente (Duarte e Brito, 2003: 186):

(88) a) O João viu [$_{SN}$ o jogo].
b) O João assistiu [$_{SP}$ ao jogo].

Enquanto em (88a) o verbo ver se constrói com dois sintagmas nominais, *o João* e *o jogo*, em (88b), o verbo assistir constrói-se com um sintagma nominal, *o João*, e com um sintagma preposicional, *ao jogo*.

O siginificado de uma palavra e as suas propriedades de selecção semântica são outros factores com implicações no contexto em que essa palavra pode ocorrer (Duarte, 2000: 71). As propriedades de selecção semântica são "a enumeração dos papéis temáticos que [um predicador] atribui aos seus argumentos" (Duarte e Brito, 2003: 187). Mesmo que o número de argumentos seja o exigido por um verbo, a frase pode ser agramatical se esses argumentos não respeitarem as propriedades de selecção semântica desse verbo:

(89) a) O criminoso assassinou três automobilistas.
b) *A tempestade assassinou três automobilistas.

(90) a) A trovoada assustou as crianças.
b) * A trovoada assustou o telhado.

(cf. Duarte e Brito 2003: 187)

Por um lado, em (89), estamos perante o mesmo verbo e dois sintagmas nominais na posição de sujeito, *o criminoso* e *a tempestade*. Porém, o verbo *assassinar* exige um Agente, ou seja, uma expressão que designe uma entidade que possa, intencionalmente, desencadear a acção, o que não é aplicável a *a tempestade*. Por outro lado, os sintagmas nominais *as crianças* e *o telhado* têm, na frase (90), o papel semântico de Experienciador, isto é, designam uma entidade que experimenta um estado psicológico (Duarte e Brito, 2003: 187). Assim, o sintagma nominal *as crianças*, em (90a), é um Experienciador, enquanto *o telhado*, em (90b), não pode sê-lo.

Em alguns casos, procedeu-se à alteração da estrutura sintáctica em virtude das propriedades de selecção dos itens escolhidos na tradução. Veja-se o exemplo (91):

(91) Em grande parte dos hotéis e restaurantes, o gestor de segurança já deve ser responsável pela maioria (senão pela totalidade) das áreas-chave seguintes: (página 91, negrito) – No original: *The security manager at most hotels and restaurants should already have responsibility for most if not all of the following key areas:*

Neste caso, a primeira tradução levou-nos, intuitivamente, a traduzir por *responsável pela maioria, senão por todas, das áreas-chave*. Desta tradução, contudo, decorre a violação das propriedades de selecção categorial dos quantificadores envolvidos: *maioria* combina-se com um sintagma preposicional, ao passo que *todas* selecciona um sintagma nominal. Por isso, a coordenação de ambos os quantificadores

conduz, em português, a uma agramaticalidade. Deste modo, foi necessário optar por substituir o segundo quantificador por *totalidade*, que veicula o mesmo significado do quantificador *todas*, mas que apresenta as mesmas propriedades de selecção que o quantificador *maioria*.

Por outro lado, em (92), foi necessário a ordem de palavras do original, uma vez que os verbos *colocar* (correspondente a *place*) e *atirar* (correspondente a *drop*) têm propriedades de selecção categorial distintas.

(92) O pessoal deve ser informado para prestar atenção a pacotes, malas ou outros objetos em locais estranhos, a objetos colocados cuidadosamente em caixotes do lixo (e não atirados para lá de forma descuidada) e ao interesse pouco usual de estranhos relativamente a locais menos acessíveis. (página 94, primeiro parágrafo) – No original: *Staff should be briefed to look out for packages, bags or other items in odd places, carefully placed (rather than dropped) items in rubbish bins and unusual interest shown by strangers in less accessible places.*

Colocar selecciona um complemento regido pela preposição *em*, ao contrário de *atirar*, cujo complemento é regido pela preposição *para*. Assim, acrescentou-se o complemento *para lá*. Esta opção obrigou-nos a deslocar o constituinte *em caixotes do lixo* (*in rubbish bins*) para a posição antes dos parênteses, uma vez que é necessário que a expressão que fixa a referência do dêictico *lá* se encontre no contexto linguístico anterior a este dêictico.

Também no exemplo (93) se procedeu à alteração da estrutura da frase em função das diferentes propriedades de selecção categorial dos verbos do Português (*possuir*, *operar*, *gerir* e *trabalhar*):

(93) Em particular, aqueles que possuem ou administram hotéis e restaurantes, bem como os que aí operam ou trabalham devem lembrar-se de que quer substancial quer grave indicam um nível elevado de ameaça e de que um atentado pode acontecer sem aviso. (página 134, terceiro parágrafo) – No original: *In particular, those who own, operate, manage or work in hotels or restaurants are reminded that substantial and severe both indicate a high level of threat and that an attack might well come without warning.*

Os verbos *possuir* e *administrar* seleccionam um sintagma nominal com a função de sujeito e um sintagma nominal com a função de objecto directo (neste caso, *hotéis e restaurantes*). Por outro lado, *operar* e *trabalhar* seleccionam, como complemento, um sintagma preposicional (*em hotéis e restaurantes*) ou adverbial, como em (93).

Os exemplos (94), (95) e (96) ilustram uma outra situação: a introdução de argumentos de verbos, a fim de se observarem as propriedades de selecção semânticas destes últimos.

(94) A polícia não irá normalmente revistar hotéis ou restaurantes. (…) Não pode, por isso, revistar a área tão rapidamente nem tão minuciosamente como um membro do seu pessoal ou um membro do pessoal de segurança do local. (página 106, Planos de buscas) – *No original: The police will not normally search hotels or restaurants. (…) They cannot, therefore, search as quickly or as thoroughly as a member of staff or on site security personnel.*

(95) O aconselhamento importante que se segue ajudá-lo-á a planear as medidas necessárias. (página 127, segundo parágrafo) – No original: *The important advice below will help you plan.*

(96) Não reúna <u>as pessoas</u> nos pontos de evacuação. (página 127, Mantenha-se seguro) – No original: *Do not congregate at evacuation points.*

Em todos os casos, foi introduzido o argumento com a função sintáctica de objecto directo: *a área*, OD de *revistar* em (94), *as medidas necessárias*, OD de *planear* em (95), e *as pessoas*, OD de *reunir* em (96). Se não se tivesse tomado a decisão de acrescentar os objectos directos, o resultado em português seria agramatical, por violação das propriedades de selecção dos referidos verbos.

2.3 Verbos leves

Alguns verbos, como *dar*, *ter* e *fazer*, podem ocorrer como verbos principais ou como verbos leves, ou seja, verbos que sofrem um processo de esvaziamento lexical, o que faz com que "o centro semântico da frase se desloque para a expressão nominal" que com eles co-ocorre em posição de complemento (Duarte, 2003b: 312).

Gonçalves *et al*. (2010: 450-451) referem que se pode, normalmente, "parafrasear a sequência <V leve + N> por um verbo pleno, morfologicamente relacionado com o nome, o que mostra que este último contribui para a interpretação semântica da construção", como se verifica em (97):

(97) a) O primeiro-ministro fez um discurso no Parlamento.
b) O primeiro-ministro discursou no Parlamento.

(cf. Gonçalves, 2010: 451)

Os verbos leves, assim como os verbos plenos, seleccionam semanticamente o argumento externo, o que não acontece com os verbos auxiliares, e preservam, geralmente, os argumentos dos verbos plenos correspondentes, como nos exemplos

(98a) e (99a), no caso de uma construção com o verbo pleno, e (98b) e (99b), no caso de uma construção com um verbo leve:

(98) a) O Pedro deu uma gravata ao pai.
b) O Pedro deu uma olhadela ao texto.

(99) a) O Pedro já teve dois peixes vermelhos.
b) O Pedro já teve uma conversa interessante com o professor.

(cf. Gonçalves, 2010: 452)

As construções com verbos leves não são específicas do Português. Em língua inglesa, alguns dos verbos plenos que funcionam como verbos leves são:

(100) *to do*
a) *to do a review*
b) verbo pleno correspondente: *to review*

(101) *to give*
a) *to give a lecture*
b) verbo pleno correspondente: *to lecture*

(102) *to have*
a) *have a conversation*
b) verbo pleno correspondente: *to converse*

(103) *to make*
a) *to make a decision*
b) verbo pleno correspondente: *to decide*

(104) *to take*

a) *to take a look*
b) verbo pleno correspondente: *to look*

O exemplo (105) ilustra a utilização de um verbo leve na tradução:

(105) As viagens de reconhecimento devem ser levadas a cabo como um ensaio para envolver o pessoal e o equipamento que será utilizado no atentado propriamente dito; por exemplo, antes dos atentados de Londres no dia 7 de Julho de 2005, os bombistas fizeram um ensaio nove dias antes do atentado. (Página 132, caixa de texto.) – No original: *Reconnaissance trips may be undertaken as a rehearsal to involve personnel and equipment that will be used in the actual attack e.g. before the London attacks on 7th July 2005, the bombers staged a trial run nine days before the actual attack.*

Num primeiro momento, a tradução foi *ensaiar*, o que era compatível com a definição do dicionário *online* da Oxford University Press para *stage*[11]: "1. present a performance of (a play or other show), i) organize and participate in (a public event), ii) cause (something dramatic or unexpected) to happen; 2. *Medicine* diagnose or classify (a disease or patient) as having reached a particular stage in the expected progression of the disease". No entanto, ao consultarmos um dicionário português, percebemos que *ensaiar* tem como significados "1. fazer o ensaio de; 2. treinar com vista a uma actuação, preparar; 3. experimentar; submeter a experimentação; 4. treinar, adestrar; 5. preparar ou iniciar (uma acção, um gesto) sem completar; 6. tentar (sem segurança)"[12]. É claro que não haveria qualquer problema em traduzir-se directamente *stage* pelo verbo *ensaiar*, uma vez que os significados 1 e 3 do dicionário português se aplicam ao contexto em causa. Contudo, no exemplo (105), decidiu-se pela tradução *fizeram um ensaio*, usando uma construção do tipo <verbo leve + nome deverbal>, em vez de

[11] http://oxforddictionaries.com/definition/english/stage?q=stage, consultado a 07/10/2013
[12] http://www.infopedia.pt/pesquisa-global/ensaiar, consultado a 07/10/2013

simplesmente *ensaiaram*, porque este último verbo remete mais directamente para as artes performativas.

Também se optou pela utilização de um verbo leve (no caso, *dar*) na tradução em (106), em que se decidiu manter a construção utilizada no original, *give advice*, utilizando uma construção como a anterior, <verbo leve + nome deverbal>.

(106) O seu CTSA pode dar aconselhamento relativamente a equipamentos de segurança física e à sua aplicação particular aos métodos utilizados pelos terroristas; o CTSA vai poder comentar a eficácia desse equipamento enquanto elemento dissuasor, de proteção e de ajuda numa investigação posterior ao incidente. (página 91, oitava marca, adaptado) – No original: *Your CTSA can give advice on physical security equipment and its particular application to the methods used by terrorists; the CTSA will be able to comment on its effectiveness as a deterrent, as protection and as an aid to post-incident investigation*.

2.4 Estruturas de coordenação múltipla

A coordenação "é um processo de formação de unidades complexas" (Matos, 2003: 551) que combina constituintes do mesmo nível categorial com as mesmas funções sintácticas ou semânticas. As estruturas de coordenação múltipla são estruturas com "mais de dois termos coordenados associados pelo mesmo nexo coordenativo" (Matos, 2003: 564).

Em (107), estamos perante a ocorrência da mesma conjunção a introduzir membros coordenados sucessivos.

(107) Passo Quatro: Rever as medidas de segurança, ensaiar e rever os planos de segurança e contingência. (página 90) – No original: *Step Four: Review your security measures and rehearse and review security and contingency plans.*

No exemplo (107), a primeira escolha de tradução foi algo presa ao original, tendo-se traduzido como *rever as medidas de segurança e ensaiar e rever os planos de segurança e contingência*.

A conjunção *and* liga membros de níveis hierárquicos diferentes na mesma frase: a primeira ocorrência liga as duas frases [*Review your security measures*] e [*rehearse and review security and contingency plans*]. Na segunda ocorrência, porém, a conjunção liga dois constituintes que ocorrem no interior do segundo membro coordenado: [*rehearse*] e [*review security and contingency plans*]. Apesar de, na ausência da vírgula, o leitor não ser levado a entender que era necessário ensaiar as medidas de segurança, a repetição da conjunção prejudica a leitura da frase. Assim, decidiu-se optar pela coordenação assindética no primeiro caso, mantendo-se apenas a segunda ocorrência da conjunção.

3. A EXPRESSÃO DA MODALIDADE

Oliveira (2003: 245) refere que a modalidade é "a gramaticalização de atitudes e opiniões dos falantes", registando-se diferentes tipos de modalidade, de que se destacam:

- *modalidade alética*
- *modalidade epistémica*
- *modalidade deôntica*
- *modalidade temporal*
- *modalidade bulomaica*
- *modalidade avaliativa*
- *modalidade causal*

Os tipos de modalidade que nos interessam no âmbito deste relatório são a epistémica e a deôntica. A primeira está relacionada com o conhecimento e a crença, ao passo que a segunda "diz respeito às circunstâncias externas (pessoais, regras sociais ou normas) que permitem ou obrigam o participante a envolver-se na situação e está relacionada com valores de permissão e obrigação" (Oliveira, 2003: 248).

Ainda segundo a mesma autora, a modalidade não é apenas expressa através de verbos, mas também de advérbios (*cá, enfim, finalmente, lá*), de adjectivos (*impossível, improvável, possível, provável*), de modos verbais (Indicativo, Conjuntivo, Condicional, Imperativo), de expressões modais (*de facto, efectivamente, na minha opinião*) e de verbos auxiliares de modo (*ter de, dever, haver de, poder*).

Os verbos modais em língua inglesa (*may*, *can*, *shall* e *will*, e as respectivas formas do passado, *might*, *could*, *should* e *would*, bem como o verbo *must*) traduzem-se pelos verbos modais *poder*, *dever*, *haver de* e *ter de* em Português. *Dever* e *poder* exprimem quer a modalidade epistémica quer a modalidade deôntica, mas *ter de* apenas exprime a segunda.

Os verbos modais em Inglês não têm flexão, ou seja, têm a mesma forma para todas as pessoas (I, you, he/she/it, we, you, they) nem podem co-ocorrer uns com os outros, contrariamente ao que acontece em Português. A co-ocorrência de modais em Português está sujeita a restrições: o primeiro verbo modal deve ter uma interpretação epistémica, como *ela deve poder acabar o trabalho amanhã* ou *ela pode ter de acabar o trabalho amanhã* (Oliveira, 2003: 248-249). Uma questão que se põe à tradução é a ambiguidade com que o tradutor pode ser confrontado quando o verbo que tem que traduzir admite quer a modalidade epistémica quer a modalidade deôntica. Sá (2012: 108) refere que, quando confrontado com esta situação, o tradutor pode eliminar a ambiguidade, utilizando o verbo *dever* no caso da modalidade epistémica e o verbo *ter de* no caso a modalidade deôntica.

Considerem-se, de seguida, alguns casos que envolveram verbos modais na nossa tradução.

Em (108) somos confrontados com a utilização do passado do verbo *shall*. Apesar de este verbo também poder ocorrer na formação do condicional, tal tradução não faria

sentido nesta frase. Por isso, optámos pela outra possibilidade de tradução: a utilização de *dever* com um valor deôntico, ou seja, de obrigação.

(108) Todos os hotéis e restaurantes devem ponderar ter uma reserva de cartazes e material (inclusive através de ligações da Internet) para apoiar a prevenção do crime e ter mensagens e iniciativas contra o terrorismo. (página 129, sétimo parágrafo) – No original: *All hotels and restaurants should consider having a supply of posters and material (even via web links) to support crime prevention and counter terrorism messages and initiatives.*

Em (109), porém, o mesmo modal do Inglês foi traduzido de forma diferente para Português:

(109) Concentre o processamento de toda a correspondência e entregas num único local. Idealmente, isto deveria ter lugar fora das instalações ou noutro edifício ou, pelo menos, numa área que possa ser facilmente isolada e onde as entregas possam ser manuseadas sem terem de ser levadas por outras partes do hotel ou restaurante. (página 104, Planeamento dos procedimentos de tratamento de correspondência). No original – *Consider processing all incoming mail and deliveries at one point only. This should ideally be off-site or in a separate building, or at least in an area that can easily be isolated and in which deliveries can be handled without taking them through other parts of the hotel or restaurant*.

No exemplo (109), estamos perante a utilização do verbo *dever* no seu valor epistémico. Maillot (1975: 50-51) refere que o verbo modal *should*, pretérito de *shall*, "não passa de uma forma atenuada de *shall* e, comparado a este, apresenta a diferença

que existe entre uma recomendação e uma prescrição". Em (109) parece tratar-se precisamente de uma recomendação, acentuada pelo advérbio *idealmente*. Assim, optámos por utilizar, na tradução, o modal *dever* no Condicional, de forma a obtermos o valor epistémico.

4. ASPECTOS DE COESÃO REFERENCIAL

Os processos "de sequencialização que asseguram (ou tornam recuperável) uma ligação linguística significativa entre os elementos que ocorrem na superfície textual podem ser encarados como elementos de coesão" (Duarte, 2003: 89). Os mecanismos de coesão textual dividem-se entre coesão lexical e coesão gramatical, sendo que da última fazem parte a coesão frásica, interfrásica, temporal e referencial, assim como o paralelismo estrutural. Esta secção é dedicada aos processos de que nos podemos servir para criar cadeias de referência, que garantem a coesão referencial, que, por sua vez, garante a coesão textual.

Existem dois subtipos de coesão referencial: a exóforica e a endofórica. Duarte (2003, 111) refere que a coesão exofórica, a que a autora também chama referência, acontece sempre que um objecto é dado a conhecer ao destinatário, através de uma instrução linguística que varia em função do que o escritor e o destinatário conhecem desse mesmo objecto. No caso da coesão endofórica, ou co-referência, utilizam-se "fragmentos textuais idênticos, do ponto de vista referencial, a outro fragmento textual presente no texto" (Duarte, 2003: 112) e que se denominam por co-referentes. O conjunto destes fragmentos textuais co-referentes constitui uma cadeia referencial. É da construção de cadeias referenciais que trataremos nesta secção.

Em casos como o exemplificado em (110), introduziu-se um nome para evitar uma leitura ambígua, do ponto de vista referencial, de um constituinte coordenado.

(110) Como já foi mencionado na "Planificação da Segurança", é reconhecido que, para a maioria dos hotéis e restaurantes, a

implementação de qualquer plano de buscas, após uma avaliação de vulnerabilidade e riscos, é da responsabilidade do gestor da segurança ou do gestor das operações. (página 106, segundo parágrafo) – No original: *As previously mentioned under Security Planning, it is recognised that for the majority of hotels and restaurants responsibility for the implementation of any search planning, following a vulnerability and risk assessment, will fall upon the security or operations manager.*

Em (110), foi considerado necessária a reiteração da palavra *gestor* para evitar a ambiguidade. A questão era que, se não se incluísse novamente aquela palavra, podia colocar-se a questão de ser apenas um gestor que fosse responsável quer pela segurança quer pelas operações ou dois gestores, cada um deles responsável por cada uma dessas áreas. Ao introduzir explicitamente o nome no segundo membro da coordenação, torna-se claro que existem dois referentes distintos.

O exemplo (111), por sua vez, ilustra um caso de retoma do antecedente através de um sintagma nominal com determinante demonstrativo.

(111) O pessoal de buscas precisa de ter uma ideia dos passos lógicos a realizar na área que lhes for atribuída e do tempo que tais passos levarão. (página 107, após a caixa de texto) – No original: *The searchers need to get a feel for the logical progression through their designated area and the length of time this will take.*

No exemplo (111), manter o pronome demonstrativo *this* na tradução, *isto*, poderia conduzir a uma frase ambígua, uma vez que o pronome poderia ter como antecedente *ter uma ideia dos passos lógicos a realizar na área que lhes for atribuída* ou apenas *passos lógicos*. Deste modo, a escolha foi introduzir uma expressão nominal com repetição do nome *passos* e com o determinante demonstrativo, para que a compreensão da frase não ficasse comprometida.

O exemplo (112) ilustra a repetição do antecedente, outra estratégia importante para manter a coesão referencial.

(112) Na eventualidade de um atentado que envolva instrumentos de ataque ou armas de fogo, a prioridade de um agente policial é proteger e salvar vidas. (…)

- Inicialmente, os agentes policiais podem não ser capazes de o distinguir dos homens armados.
- Os agentes podem estar armados e apontar-lhe uma arma.
- Podem ter de lidar com o público com firmeza. Siga as instruções dos agentes, mantenha as mãos no ar/à vista.

(página 128, Polícia armada)

No original: *In the event of an attack involving firearms or weapons, a Police Officer's priority is to protect and save lives. (…)*

- *Initially they may not be able to distinguish you from the gunmen.*
- *Officers may be armed and may point guns at you.*
- *They may have to treat the public firmly. Follow their instructions; keep hands in the air / in view.*

Em (112), decidiu-se repetir a expressão *agentes policiais* logo na primeira marca do parágrafo, porque a utilização do pronome pessoal *eles*, ou a sua eliminação, poderia não facilitar a compreensão do enunciado, dado que o seu anrtecedente ocorre no parágrafo anterior, numa posição afastada. Apesa da sua proximidade ao referente anterior, decidiu-se manter a expressão *agentes* na segunda marca de parágrafo, porque poderia ser feita confusão com o SN imediatamente anterior, *homens armados*. Finalmente, foi repetido parcialmente o SN (*agentes* em vez de *agentes policiais*) para tornar clara a interpretação do possessivo.

Em (113) estamos perante uma cadeia referencial constituída pela expressão nominal-clítico.

(113) Conhece o CTSA local e envolve-o em quaisquer desenvolvimentos relativamente ao hotel ou restaurante ou à segurança? (Anexo G) – No original: *Do you know your local CTSA and do you involve him/her in any hotel or restaurant or security developments?*

Repare-se que, em (113) a escolha da forma masculina do pronome pessoal para a retoma do antecedente, *o CTSA local*, prendeu-se com o facto de, em língua portuguesa, ser costume designar uma profissão pelo seu masculino quando o substantivo não tem uma forma para o masculino e outra para o feminino. A escolha do termo anafórico foi baseada neste conhecimento.

5. QUESTÕES CULTURAIS

Se há diferenças gramaticais entre a língua inglesa e a portuguesa, também há várias diferenças ao nível da cultura do Reino Unido e de Portugal, o que pode colocar alguns problemas à tradução.

Newmark (1988: 82-83) faz a distinção entre *cultural equivalent*, que pode ser entendido como "an approximate translation where a SL [source language] cultural word is translated by a TL [target language] cultural word", e *functional equivalent*, um procedimento que requer "the use of a culture-free word, sometimes with a new specific term" (*ibid*.: 83), que neutraliza ou generaliza o termo da língua de partida. Ainda segundo o autor, a procura de um equivalente funcional é o método mais preciso de traduzir, ou seja, de desculturalizar uma palavra pertencente a uma determinada cultura (*ibid*.).

> *"In general, the more serious and expert the readership (...) the greater the requirement for transference – not only of cultural and institutional terms, but of titles, addresses and words used in a special sense. In such cases, you have to bear in mind that the readership may be more or less acquainted with the source language, may only be reading your translation as they have no*

> *access to the original, may wish to contact the writer of the SL text, to consult his other works, to write to the editor or publisher of the original. Within the limits of comprehension, the more that is transferred and the less that is translated, then the closer the sophisticated reader can get to the sense of the original."* (Newmark, 1988: 100-101)

Newmark (1988), na citação acima, defende que quanto maior for o conhecimento do público-alvo da cultura do texto de partida tanto maior será o número de empréstimos que devemos utilizar. É por esta razão que, frequentemente, um tradutor, depois de uma tentativa frustrada de encontrar a tradução equivalente, coloca entre parênteses o termo da língua de partida, mostrando, assim, que não conseguiu propor uma palavra na língua de chegada que tivesse a mesma denotação da palavra da língua de partida. O trabalho de um tradutor "is to translate and then, if he finds his translation inadequate, to help the reader to move a little nearer to the meaning" (Newmark, 1988: 101).

Para além das diferentes formas de tratamento já referidas (cf. secção 1.2.1), outras opções de tradução foram determinadas for factores de natureza cultural. Foi o que aconteceu como o número de telefone de emergência, em (114):

(114) 112 – No original: *999*

O número de emergência no Reino Unido, e em outros países, é o 999. Ora, este número não é reconhecível por um leitor português que não tenha qualquer contacto com o contexto britânico. A adaptação para o número de emergência nacional 112 foi a nossa opção.

Por outro lado, decidiu-se manter os *sites* que apareciam no original:

(115) www.cpni.gov.uk (CPNI)

(116) www.acpo.police.uk (ACPO)

(117) www.acpos.police.uk (ACPO na Escócia)

(118) www.the-sia.org.uk/home/scotland (Autoridade da Indústria de Segurança (SIA - *Security Industry Authority*) na Escócia)

(119) www.itsafe.gov.uk (página de aconselhamento do Governo britânico)

Esta opção está relacionada com a questão da tradução das denominações, referida na subsecção 1.3 da secção sobre questões lexicais. Com efeito, como mantivemos as denominações das instituições e dos organismos do Reino Unido, tivemos de manter igualmente os *sites* originais.

CONCLUSÃO

Este relatório teve como objectivo a apresentação do trabalho de tradução executado ao longo do estágio profissionalizante realizado no Instituto Superior de Ciências Policias e Segurança Interna.

A base o relatório foi a tradução de um manual sobre segurança anti-terrorismo em hotéis e restaurantes, porque, pela sua extensão, era o documento traduzido que mais interesse tinha para uma análise. A tradução deste documento provou ser uma dificuldade, pela terminologia que o mesmo contém. Nem sempre foi fácil encontrar uma tradução, mesmo quando a procura não se restringia a dicionários, bases de dados ou bases terminológicas.

Esta experiência provou que, por vezes, as nossas escolhas de tradução podem não ser as melhores. Isto prende-se com o facto de nos deixarmos levar pela intuição, que nos pode levar a não escolher o melhor significado para um determinado termo ou a cair no erro de traduzir aquela expressão por um 'falso amigo'.

No geral, julgo que este estágio me possibilitou alargar conhecimentos ao nível da Tradução e aumentar a minha experiência no campo da tradução técnica, mais especificamente na parte relacionada com a segurança em hotéis e restaurantes e com a segurança em eventos desportivos realizados pela UEFA.

Concluindo, penso que o Mestrado foi um grande contributo para o meu futuro profissional e o estágio no ISCPSI mostrou-me a realidade da tradução num contexto profissional, para além de me ter permitido aplicar os conhecimentos que adquiri nas disciplinas do primeiro ano do Mestrado.

BIBLIOGRAFIA

Textos

Baakes, K. (1994), *Key issues of syntax in the special languages of science and technology*. Heidelberg: Julius Groos Verlag.

Byrne, J. (2006). *Technical Translation. Usability Strategies for Translating Technical Documentation.* Dordrecht: Springer.

Cabré, M. T. (1998). *Terminology: Theory, methods and applications*. Amsterdam, Philadelphia: John Benjamins Publishing Company.

Cabré, M. T. (2000). *Terminología y lingüística: la teoría de las puertas*. Tradução do francês de Rosanna Folguerà: http://elies.rediris.es/elies16/Cabre.html

Contente, M. M. D. M. (2008). *Terminocriatividade, sinonímia e equivalência interlinguística em Medicina*. Lisboa: Colibri.

Contente, M. M. D. M. (2012). *Denominação terminocriativa e comunicação em Medicina*. Acta Semiótica et Lingvistica, volume 17, nº. 2.

Correia, M. (2001). Homonímia e Polissemia – Contributos para a Delimitação dos Conceitos. In *Palavras*, nº 19. Lisboa: Associação dos Professores de Português, pp. 57-75.

Cruz, L. (2012). *A tradução de sistemas de segurança*. Relatório de estágio de Mestrado. Lisboa: Faculdade de Letras da Universidade de Lisboa.

Crystal, D. (1997). *The Cambridge Encyclopedia of Language*. 2ª edição. Cambridge: Cambridge University Press.

Cunha, C. e Cintra, L. F. L. (2000). *Nova Gramática do Português Contemporâneo*. Lisboa: Sá da Costa.

DeGeorge, J. (1984). *Style and Readibility in Technical Writing*. New York: Random House

Duarte, I. (2000). *Língua Portugues: Instrumentos de Análise*. Lisboa: Universidade Aberta.

Duarte, I. (2003). Aspectos linguísticos da organização textual. In Mateus, M. H. *et al*. *Gramática da Língua Portuguesa*. 5ª edição, revista e aumentada. Lisboa: Caminho, pp. 85-123.

Duarte, I. (2003a). A família das construções inacusativas. In Mateus, M. H. *et al*. *Gramática da Língua Portuguesa*. 5ª edição, revista e aumentada. Lisboa: Caminho, pp. 507-549.

Duarte, I. (2003b). Relações gramaticais, esquemas relacionais e ordem de palavras. In Mateus, M. H. *et al*. *Gramática da Língua Portuguesa*. 5ª edição, revista e aumentada. Lisboa: Caminho, pp. 275-321.

Duarte, I. e Brito, A. M. (2003). Predicação e classes de predicadores verbais. In Mateus, M. H. *et al*. *Gramática da Língua Portuguesa*. 5ª edição, revista e aumentada. Lisboa: Caminho, pp. 179-203.

Fawcett, P. (1997). *Translation and Language: Linguistic Theories Explained.* Manchester, Northampton: St Jerome Publishing.

Fromkin, V. e Rodman, R. (1993). *Introdução à Linguagem*. Coimbra: Almedina.

Gamero Pérez, S. (2001). *La traducción de textos técnicos*. Barcelona: Editorial Ariel.

Gonçalves, A. *et al*. (2010). Propriedades predicativas dos verbos leves: estrutura argumental e eventiva. In Brito, A. M. et al. *Textos Seleccionados do XXV Encontro Nacional da Associação Portuguesa de Linguística*. Porto: APL, pp. 449-464: http://bit.ly/1iZA3XY

Hoffmann, L. (1991), Texts and text types in LSP. In Schröder, H. (ed.), *Subjectoriented Texts*. Berlin: Walter de Gruyter, pp. 158-166.

Hornby, M. S. (2005). *Translation Studies: An Integrated Approach.* Amsterdam: John Benjamins.

Jakobson, R. (1959). On linguistic aspects of translation. In Venuti, Lawrence and Baker, Mona (2000). *The Translation Studies Reader.* London & New York: Routledge, pp. 113-118.

Maillot, J. (1975). *A Tradução Científica e Técnica.* São Paulo: McGraw-Hill do Brasil.

Mateus, M. H. e Xavier, M. F. (1992). *Dicionário de Termos Linguísticos*. Lisboa: Cosmos.

Matos, G. (2003). Estruturas de Coordenação. In Mateus, M. H. *et al*. *Gramática da Língua Portuguesa*. 5ª edição, revista e aumentada. Lisboa: Caminho, pp. 549-589.

Munday, J. (2001). *Introducing Translation Studies: Theories and Applications* London: Routledge.

Newmark, P. (1988). *A Textbook of Translation*. New York: Prentice Hall.

Nord, C. (1991). *Text Analysis in Translation*. Amsterdam: Rodopi.

Oliveira, F. (2003). Modalidade e modo. In Mateus, M. Helena et al., *Gramática da Língua Portuguesa*. 5ª edição, revista e aumentada. Lisboa: Caminho, pp. 243-272.

Reiss, K. (1971). *Möglichkeiten und Grenzen der Übersetzungskritik: Kategorien und Kriteren für eine sachgerechte Beurteilung von Übersetzungen*. Munich: Hueber.

Reiss, K. e Vermeer, H. (1984). *Grundlegung einer allgemeinen Translationstheorie*. Tübingen: Niemeyer.

Robinson, D. (2003). *Becoming a Translator*. 2ª edição. London & New York: Routledge

Rónai, P. (1976). *A tradução vivida*. Rio de Janeiro: Educom.

Sá, P. F. N. (2012). *Relatório de Estágio: Contributo para uma Reflexão Sobre Opções Linguísticas em Tradução*. Dissertação de Mestrado. Lisboa: Faculdade de Letras da Universidade de Lisboa

San Salvador, N. G. (1998). La elección del término correcto en una traducción especializada: casualidad o resultado de una investigación documental y terminológica?. In Correia, Margarita (org.). *VI Simpósio Ibero-Americano de Terminologia*. Lisboa: Colibri: http://www.ufrgs.br/riterm/por/simposios_anteriores_1998.html

Vermeer, H. (1986). *Esboço de uma teoria da tradução*. Porto: Asa.

Vilela. M. (1994). *Estudos de lexicologia do Português*. Coimbra: Almedina.

Yebra, V. G. (1989). *Teoría y Práctica de la Traducción.* Madrid: Gredos.

Yebra, V. G. (2004). Traducción, academias y terminologia. In *V Jornada-Coloquio de la Asociación Española de Terminología (AETER)*. Centro Virtual Cervantes: http://cvc.cervantes.es/lengua/aeter/conferencias/garcia.htm

Zethsen, K. K. (1999), The Dogmas of Technical Translation – Are They Still Valid? In *Journal of Linguistics*, 23, Hermes, http://pure.au.dk/portal/files/9952/H23_05.pdf

Bases de dados

Base de dados Eur-Lex: eur-lex.europa.eu/pt/index.htm (acedida através do Linguee)

Base terminológica europeia IATE: iate.europa.eu

Dicionários

Dicionário de Inglês-Português (2009). Dicionários Editora. Porto: Porto Editora

Dicionário Linguee: linguee.pt

Dicionário online Infopédia (Porto Editora): www.infopedia.pt

Dicionário online Pons: pons.eu

Dicionário online Webster's Online Dictionary with Multilingual Thesaurus Translation: http://www.websters-online-dictionary.org/

Sites consultados

Comissão Nacional de Protecção de Dados: www.cnpd.pt

Diário da República electrónico: www.dre.pt

Instituto Superior de Ciências Policiais e Segurança Interna: www.iscpsi.pt

Portal do Parlamento Europeu: www.europarl.europa.eu (acedido através do Linguee)

Anexo A – Lista de termos

Lista de termos

EN	PT
Acceptable use policy (AUP)	Política de uso aceitável (AUP)
Act	Lei
Additional premium	Prémio adicional
Adressing vulnerability	Prevenção da vulnerabilidade
Anthrax	Antrax
Assembly area	Área de concentração
Attack on life and limb	Ataque à vida e integridade física
Audit trail	Pista de auditoria
Auditing	Fiscalização
Borders and Immigration Agency	Agência da Imigração e Fronteiras
Business continuity planning	Planos de continuidade das actividades
Business premises	Estabelecimentos comerciais
Chemical warfare agent	Substância química de combate
Chemical, biological or radiological (CBR)	Químico, biológico ou radiológico (QBR)
Closed-circuit television (CCTV)	Circuito fechado de televisão (CCTV)
Code of practice	Código de conduta
Compacter	Compactador
Compensation	Indemnização
Contingency arrangements	Disposições de contingência
Contractor	Adjudicatário
Courier	Estafeta
Degaussing	Desmagnetização
Denial of service attack	Ataque de negação de serviço
Disk drive	Unidade de disco
Employment history	Carreira profissional
Flying debris	Projecção de destroços
Flying glass	Estilhaços de vidro
Fortress mentality	Mentalidade de fortaleza
Foyer	Área de recepção
Glazing	Superfícies envidraçadas
Global Positioning System (GPS)	Sistema de Posicionamento Global (GPS)
Goods and service yards	Zonas de bens ou de serviço
Heating, ventilation and air conditioning (HVAC)	Aquecimento, ventilação e ar-condicionado (AVAC)
Home Office	Ministério da Administração Interna
Incident plan	Plano de emergência
Intelligence Community	Serviços de informação
Intruder alarm	Alarme de intrusão
Liaise	Estabelecer contacto

Liaising	Colaboração
Made under it	Feitos ao abrigo de
Magnetic swipe	Cartão magnético
Maintenance hatch	Escotilha de manutenção
Mortar	Morteiro
Mound	Montículo
Operator	Empresário
Optical media	Suportes de dados ópticos
Outsourcing	Externalização
Pan and tilt	Rotação horizontal e rotação vertical
Police adviser	Conselheiro para questões de polícia
Pre-employment	Antecedentes laborais
Proximity card	Cartão de proximidade
Public adress system	Sistema de sonorização
Publicly-funded compensation scheme	Regime de indemnização financiado por fundos públicos
Pulping	Desfibração
Radiological dispersal device (RDD)	Engenho de dispersão radiológica
Raise awareness	Sensibilizar
Reconnaissance	Reconhecimento
Reinforced concrete	Betão armado
Rocket Propelled Grenade (RPG)	Granada-foguete
Royal Mail	CTT
Sarin gas	Gás sarin
Screening	Controlo
Senior management	Quadros superiores
Stakeholder	Parte interessada
Statutory duties	Obrigações estatutárias
Tamper proof seal	Selo de plástico inviolável
Tenant	Locatário
Trade bodies	Organizações empresariais
Traffic-calming	Redução do ruído de trânsito
Trojan	*Trojan*
Underwriter	Segurador
Uninterrupted power supply (UPS)	Unidades de alimentação ininterruptas
Vehicle borne improvised explosive device (VBIED)	Veículo com Dispositivo Explosivo Improvisado (VBIED)
Worm (informática)	*Worm*

Anexo B – Tradução do manual

Conselhos de segurança antiterrorismo para hotéis e restaurantes

Conselhos de segurança antiterrorismo
para hotéis e restaurantes

Prefácio

NaCTSO
Gabinete Nacional de Segurança Antiterrorismo

O *National Counter Terrorism Security Office* (NaCTSO), em nome da *Association of Chief Police Officers, Terrorism and Allied Matters* (ACPO TAM), trabalha em parceria com o Serviço de Segurança para reduzir o impacto do terrorismo no Reino Unido ao:

- Proteger os locais e bens mais vulneráveis e mais valiosos do Reino Unido.
- Melhorar a robustez do Reino Unido contra um atentado terrorista.
- Providenciar aconselhamento sobre segurança relativa ao setor dos locais de grande afluência.

O NaCTSO visa:

- Sensibilizar para a ameaça terrorista e para as medidas que podem ser tomadas de forma a reduzir os riscos e a atenuar os efeitos de um atentado.
- Coordenar a prestação de serviços de segurança nacionais através da rede dos CTSA e controlar a sua eficácia.
- Estabelecer e fomentar parcerias com as comunidades e com os intervenientes policiais e governamentais.
- Contribuir para o desenvolvimento das políticas e do aconselhamento relativos ao Antiterrorismo.

■ Índice

1. INTRODUÇÃO

Este guia oferece aconselhamento de segurança àqueles que possuem ou gerem hotéis e restaurantes, bem como àqueles que aí trabalham. Ajuda a reduzir o risco de um atentado terrorista e a limitar os danos que um atentado possa causar. Destaca o papel vital que o leitor pode desempenhar na estratégia do Reino Unido contra o terrorismo.

Os atentados terroristas no Reino Unido são um perigo real e sério. Os incidentes de Haymarket, Londres, na Sexta-feira, dia 29 de junho de 2007, e do Aeroporto de Glasgow no Sábado, dia 30 de junho de 2007, indicam que os terroristas continuam a ter como alvo locais de grande afluência, uma vez que se trata, normalmente, de espaços com medidas de segurança limitadas e, por isso, proporcionam a ocorrência de um elevado número de vítimas. Para além disto, estes incidentes indicam que os terroristas estão preparados para utilizar veículos como um método de entrega e atacarão locais fora de Londres.

Os hotéis e os restaurantes de todo o mundo foram alvo de atentados terroristas em diversas ocasiões. É possível que o seu hotel ou restaurante possa vir a estar envolvido num incidente terrorista. Isto pode implicar ter de lidar com uma ameaça de bomba ou com objetos suspeitos deixados no interior ou perto das instalações ou enviados por correio.

No pior dos cenários, num atentado terrorista coordenado, múltiplo e sem aviso prévio, o seu pessoal e os seus clientes podem ser mortos ou feridos e as suas instalações destruídas ou danificadas.

Reconhece-se a necessidade de manter uma atmosfera amigável e acolhedora no hotel e no restaurante. Este guia não pretende criar uma ‘mentalidade de fortaleza’; contudo, deve chegar-se a um equilíbrio em que os responsáveis pela segurança sejam informados da existência de medidas de segurança para atenuar a ameaça de terrorismo, como, por exemplo, a proteção contra estilhaços de vidro e o controlo do acesso de viaturas a zonas de grande afluência de pessoas e mercadorias ou áreas de carga, e a parques de estacionamento subterrâneos.

O terrorismo pode surgir sob diferentes formas, não apenas como atentados à vida ou à integridade física. Pode incluir interferências com a informação vital ou com os sistemas de comunicação, o que levará a perturbações e prejuízos económicos. Alguns atentados são mais facilmente levados a cabo se o terrorista tiver o auxílio de um informador infiltrado ou de alguém com conhecimentos ou acesso privilegiados. Também são consideradas formas de terrorismo as ameaças ou os embustes destinados a intimidar e a assustar as pessoas. No passado, várias instalações do Reino Unido foram alvo deste tipo de terrorismo.

Lei, Responsabilidade e Seguro

Existem razões legais e comerciais para que o seu estabelecimento disponha de planos para evitar ou, pelo menos, para reduzir o impacto dos atentados terroristas. Entre essas razões, contam-se:

Os procedimentos jurídicos e fortes penalizações previstos na legislação em matéria de saúde e segurança para empresas e indivíduos que possuam ou giram hotéis e

restaurantes são uma possibilidade real na sequência de um atentado terrorista, principalmente se se vier a descobrir que as normas industriais e as obrigações estatutárias fundamentais não foram cumpridas. As exigências específicas da *Health and Safety at Work Act* de 1974 e dos Regulamentos ao abrigo da mesma são particularmente relevantes para a segurança em hotéis e restaurantes, no sentido de:

- Levar a cabo **avaliações dos riscos** apropriadas e introduzir medidas adequadas à gestão dos riscos identificados, mesmo quando não são da sua autoria e estão fora do seu controlo direto; esteja atento à necessidade de proceder a revisões urgentes e regulares dessas avaliações e medidas à luz de novas ameaças e novos desenvolvimentos.
- **Manter e coordenar** acordos relativos à segurança entre proprietários, gerentes, pessoal de segurança, inquilinos e outras pessoas envolvidas, incluindo a partilha de planos de emergência e o trabalho conjunto no que diz respeita a simulações, auditoria e melhoramentos dos planos e da resposta. **As tensões comerciais que naturalmente se criam entre os proprietários e os inquilinos, bem como entre organizações vizinhas que podem estar em concorrência direta umas com as outras devem, ser totalmente deixadas de lado aquando do planeamento da segurança.**
- **Garantir** que todo o pessoal e, em especial, os indivíduos envolvidos diretamente na segurança e na proteção recebem **a formação, a informação e o equipamento adequados.**
- Implementar procedimentos apropriados e recrutar pessoal competente para lidar com um **perigo grave e iminente**, assim como com a evacuação.

Geralmente, encontra-se disponível um **seguro** contra danos provocados por atos terroristas no seu estabelecimento comercial, mas, normalmente, implica um prémio adicional. Uma cobertura adequada à perda de receitas e à interrupção da atividade durante a reconstrução ou a descontaminação é dispendiosa, mesmo quando disponível no grupo limitado de seguradoras especializadas. Pode conseguir uma proteger-se totalmente contra os pedidos de indemnização por morte ou danos provocados pelo terrorismo no pessoal e em membros do público, embora isto tenha um custo adicional.

Com as indemnizações individuais no caso de morte e lesões graves a excederem o limite máximo do regime de compensação por danos criminais financiado por fundos públicos, as vítimas têm todos os incentivos para procurar compensar qualquer falha através de via judicial direta contra proprietários, empresários, gerentes e inquilinos, ao abrigo das leis de responsabilidade dos ocupantes. O facto de ter de pagar do seu bolso pedidos de indemnização avultados e em grande número sem ter seguro pode atrasar o seu negócio durante vários anos.

Os planos de **continuidade operacional** são essenciais para garantir que os seus estabelecimentos podem fazer frente a um incidente ou atentado e regressar à **normalidade** assim que possível. Um atentado a um adjudicatário ou fornecedor fundamental pode também ter impacto na continuidade operacional. Este facto é particularmente importante para atividades mais pequenas que possam não ter os recursos para resistir, mesmo que sejam apenas alguns dias de perda financeira.

A reputação e a boa vontade são valiosas, mas propensas a danos graves e permanentes se se descobrir que não foi dada uma prioridade forte, responsável e profissional à melhor proteção dos indivíduos em caso de atentado. Ter a segurança em

mente e estar bem preparado garante aos seus clientes e ao seu pessoal que está a levar a sério as questões relacionadas com a segurança.

Sabe quem são os seus vizinhos e qual a natureza do seu negócio? Será que um incidente nos estabelecimentos deles podia afetar a sua atividade? A vantagem da segurança isolada do seu estabelecimento comercial é limitada. Tenha em conta os planos dos seus vizinhos e dos serviços de emergência.

Algumas organizações adotaram boas práticas para melhorar as medidas de segurança nos seus estabelecimentos e nas redondezas dos mesmos. Este documento identifica e complementa essas medidas de boas práticas.

Este guia reconhece que os hotéis e os restaurantes diferem uns dos outros em vários aspetos, incluindo dimensão, localização, estrutura e atividade, e que uma parte dos conselhos incluídos neste documento pode já ter sido introduzida em alguns locais.

Para conselhos específicos relacionados com a sua atividade, contacte a rede nacional de conselheiros especialistas em questões de polícia conhecidos como *Counter Terrorism Security Advisers* (CTSAs), através da sua polícia local. Os CTSAs são coordenados pelo NaCTSO.

É essencial que todo o trabalho que leve a cabo em matéria de segurança seja conduzido em parceria com a polícia, com outras autoridades relevantes e com os seus vizinhos se estiver em causa a segurança do seu estabelecimento.

Vale a pena lembrar que as medidas que pode implementar para combater o terrorismo também funcionarão contra outras ameaças, como furtos e assaltos. Quaisquer medidas adicionais que forem consideradas devem integrar-se, sempre que possível, nas medidas de segurança já existentes.

2. GESTÃO DOS RISCOS

Gerir o risco do terrorismo é apenas uma parte da responsabilidade do gerente de um hotel ou de um restaurante aquando da preparação de planos de contingência para dar resposta a qualquer incidente no seu estabelecimento ou nas redondezas deste que possa prejudicar a segurança pública ou perturbar as atividades normais.

A gerência já tem responsabilidade ao abrigo da *Regulatory Reform (Fire Safety) Order* de 2005 ou, na Escócia, da *Fire (Scotland) Act* de 2005 e dos *Fire Safety (Scotland) Regulations* de 2006.

No que diz respeito à segurança, a melhor forma de gerir os riscos para o seu estabelecimento é começar por entender e identificar as ameaças, bem como as suas vulnerabilidades a essas ameaças.

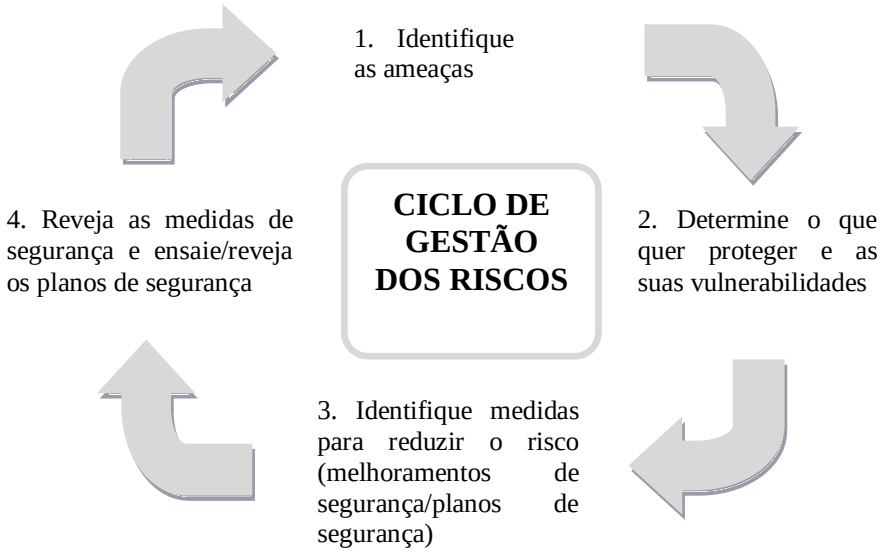
Isto irá ajudá-lo a decidir sobre:

- Os melhoramentos de segurança que deve fazer.
- O tipo de planos de segurança e contingência que é necessário desenvolver.

Para alguns hotéis e restaurantes, as meras boas práticas – aliadas a uma vigilância e a planos de contingência bem conseguidos – podem ser suficientes.

Contudo, se considerar que está vulnerável a um atentado, deve aplicar medidas de segurança apropriadas para reduzir o risco ao mínimo possível.

O diagrama seguinte ilustra um ciclo típico de gestão dos riscos:



Passo Um: Identificar as ameaças

Perceber as intenções e as capacidades dos terroristas – o que poderão fazer e como poderão fazê-lo – é crucial para avaliar a ameaça. Coloque a si próprio as seguintes questões:

- O que podemos aprender com o governo e com a comunicação social sobre o clima de segurança atual ou as atividades terroristas? (Visite www.cpni.gov.uk ou consulte a secção de Contactos Úteis no final deste folheto).

- Existe algo na localização do seu estabelecimento, nos clientes, proprietários e pessoal do mesmo ou na própria atividade que seja particularmente atrativo para um atentado terrorista?
- Existe alguma associação a indivíduos ou a organizações de grande notoriedade que possam ser alvos terroristas?
- Tem procedimentos vigentes e disponíveis para implementação nas ocasiões em que estão presentes *VIPs* no seu estabelecimento?
- Podem ocorrer danos colaterais devido a um atentado ou a outro incidente que afete um vizinho de elevado risco?
- O que é que o serviço de polícia local lhe pode dizer sobre delitos e outros problemas na sua área?
- Há alguma particularidade da sua empresa ou da sua atividade que os terroristas possam querer usar para os ajudar no seu trabalho, como, por exemplo, planos, conhecimentos técnicos ou acesso não autorizado?
- Transmite informação sobre a ameaça e os níveis de resposta?

Passo Dois: Determinar o que necessita para proteger e identificar as vulnerabilidades.

As suas prioridades para proteção devem integrar-se nas seguintes categorias:

- Pessoas (pessoal, visitantes, concessionários, adjudicatários)
- Bens físicos (edifícios, conteúdo, equipamento, planos e materiais sensíveis).
- Informação (dados eletrónicos e em papel)
- Processos (cadeias de abastecimento, procedimentos críticos) – o processo operacional propriamente dito e os serviços essenciais necessários para o apoiar.

Sabe o que é importante para si e para a sua empresa. É provável que já tenha planos em funcionamento para lidar com incêndios e crimes, procedimentos para avaliar a integridade daqueles que contrata, proteção contra vírus e piratas informáticos, bem como medidas para proteger setores dos seus estabelecimentos.

Reveja os seus planos regularmente e, se achar que há um forte risco de atentado – talvez dada a natureza da sua empresa ou a localização do seu estabelecimento – , então, pense como é que os outros podem descobrir as suas vulnerabilidades, entre os quais se inclui:

- Informação sobre si que esteja publicamente disponível, por exemplo, na Internet ou em documentos públicos.
- Tudo o que nas suas instalações ou serviços seja considerado vital para a continuação da sua atividade.
- Quaisquer alvos com prestígio que possam ser atrativos para os terroristas, independentemente de a sua perda poder resultar, ou não, na falência da empresa.

Deve ter em funcionamento medidas para limitar o acesso ao serviço ou aos corredores das traseiras e para controlar o acesso de veículos a zonas de bens ou de serviços.

Como no Passo Um, tenha em consideração se há ou não uma característica da sua empresa ou das suas atividades que os terroristas possam querer utilizar para os ajudar ou para financiar o seu trabalho. Se há, quão rigorosos são os controlos que faz àqueles

que recruta ou ao pessoal contratado? O seu pessoal tem preocupações com a segurança?

É importante que o seu pessoal seja capaz de identificar e reportar uma atividade suspeita; veja "Reconhecimento Hostil" na página 48.

Passo Três: Identificar medidas para reduzir o risco

É essencial uma abordagem integrada à segurança, o que envolve pensar em segurança física, segurança da informação e segurança do pessoal (isto é, boas práticas de recrutamento e emprego).

Faz pouco sentido investir em medidas de segurança dispendiosas se estas puderem ser facilmente comprometidas por um membro descontente do pessoal ou por um processo de recrutamento pouco cuidadoso.

Lembre-se, **O TERRORISMO É UM CRIME**. Muitas das precauções de segurança normalmente utilizadas para dissuadir criminosos também são eficazes contra terroristas. Por isso, antes de investir em medidas de segurança adicionais, reveja o que já tem em funcionamento. Pode já ter um bom regime de segurança a partir do qual possa trabalhar.

Se precisar de medidas de segurança adicionais, torne-as, sempre que possível, rentáveis através de um planeamento diligente. Introduza novos equipamentos e procedimentos quando fizer obras. Tente chegar a acordo relativamente a planos de segurança comuns. Mesmo que os seus vizinhos não estejam preocupados com atentados terroristas, estarão preocupados com a criminalidade em geral – e as suas medidas de segurança irão ajudar a proteger contra criminalidade e terrorismo.

O pessoal pode não ter conhecimento das medidas de segurança existentes ou pode ter desenvolvido hábitos para as contornar, como, por exemplo, atalhos através das saídas de emergência. Restabelecer as boas práticas básicas de segurança e revê-las regularmente trarão benefícios a um custo insignificante.

Passo Quatro: Rever as medidas de segurança, ensaiar e rever os planos de segurança e contingência.

Deve rever e ensaiar os seus planos para assegurar que continuam rigorosos, viáveis e atualizados. Deve estar ciente da necessidade de os modificar na sequência de quaisquer alterações no seu hotel ou restaurante (por exemplo, obras, mudanças no pessoal, sistemas de informação e comunicação, e revisão de questões relacionadas com saúde e segurança).

Os ensaios e exercícios devem, sempre que possível, ser conduzidos em articulação com todos os parceiros, serviços de emergência e autoridades locais.

Tenha a certeza de que o seu pessoal entende e aceita a necessidade de medidas de segurança e que esta é vista como parte da responsabilidade de todos, não apenas algo para especialistas ou profissionais. Faça com que seja mais fácil para as pessoas expor problemas ou relatar observações.

LEMBRE-SE DE QUE A MAIOR VULNERABILIDADE DE QUALQUER ORGANIZAÇÃO É A COMPLACÊNCIA.

3. PLANIFICAÇÃO DA SEGURANÇA

Reconhece-se que, para muitos hotéis e restaurantes, a responsabilidade na implementação de medidas de segurança após a avaliação de vulnerabilidades e riscos irá recair num gestor de segurança designado ou em outra pessoa responsável dentro da equipa de organização, que deverá ter autoridade suficiente para conduzir o processo de resposta a uma ameaça à segurança.

Essa pessoa deve estar envolvida no planeamento da segurança exterior dos estabelecimentos, no controlo de acessos, nos planos de contingência, entre outros aspetos, para que a dimensão terrorista seja tida em conta. O gestor de segurança deve também ser consultado em caso de construção de novos edifícios ou remodelações, para que as medidas contra o terrorismo, por exemplo, relativamente a superfícies envidraçadas e barreiras físicas, possam ser tidas em conta, considerando os regulamentos de planeamento e segurança, bem como a *Fire Safety Order* de 2005 ou, na Escócia, a *Fire (Scotland) Act* de 2005 e os *Fire Safety (Scotland) Regulations* de 2006.

Em grande parte dos hotéis e restaurantes, o gestor de segurança já deve ser responsável pela maioria (senão pela totalidade) das áreas-chave seguintes:

- Elaboração do plano de segurança com base na avaliação dos riscos.
- Formulação e manutenção de um plano de busca.
- Formulação e manutenção de outros planos de contingência que digam respeito a ameaças de bomba, embalagens suspeitas e evacuação.
- Colaboração com a polícia, outros serviços de emergência e autoridades locais.
- Organização de formação do pessoal, incluindo os seus diretores e condução de reuniões de informação e de balanço.
- Realização de revisões regulares dos planos.

Muitos hotéis têm planos específicos para a gestão de crises em determinados lugares. Estes documentos contêm as políticas e os procedimentos a serem implementados em resposta a vários incidentes, incluindo incêndio, evacuação, ameaça de bomba, desmoronamento, crimes e incidentes graves.

Para conselhos e orientação antiterrorismo independentes e imparciais em locais específicos, o gestor de segurança deve estabelecer contacto com o CTSA da polícia local. A maioria das forças policiais do Reino Unido tem, pelo menos, dois CTSAs.

O seu CTSA pode:

- Ajudá-lo a avaliar a ameaça, de modo geral e específico.
- Dar aconselhamento relativamente a equipamentos de segurança física e à sua aplicação particular aos métodos utilizados pelos terroristas; o CTSA vai poder comentar a eficácia desse equipamento enquanto elemento dissuasor, de proteção e de ajuda numa investigação posterior ao incidente.
- Facilitar o contacto com serviços de emergência e com as autoridades locais responsáveis pelo planeamento para o desenvolvimento de planos de resposta e contingência apropriados.
- Identificar organizações empresariais adequadas ao fornecimento e à instalação de equipamento de segurança.
- Oferecer aconselhamento no que diz respeito a planos de buscas.

Criação do seu Plano de Segurança

O gestor de segurança deve ter como objetivo a elaboração de um plano que tenha sido inteiramente testado e que seja regularmente revisto para garantir que ainda se encontra atual e viável.

Antes de investir em medidas de segurança adicionais, reveja as que já tem, incluindo as fragilidades conhecidas como os ângulos mortos do seu circuito fechado de televisão.

Aquando da criação do seu plano de segurança, tenha em conta os aspetos seguintes:

- Detalhes de todas as medidas de segurança a serem implementadas, abrangendo segurança física, informações e pessoal.
- Instruções sobre a forma como responder a diferentes tipos de ameaça (por exemplo, ameaça de bomba feita por telefone).
- Instruções sobre a forma como responder à descoberta de um objeto ou de um evento suspeitos.
- Existência de um plano de busca.
- Planos de evacuação e detalhes sobre o modo como a segurança do hotel ou do restaurante deve ser feita em caso de evacuação total.
- O seu plano de continuidade da atividade.
- Uma estratégia relativa às comunicações e aos meios de comunicação social inclui lidar com perguntas de familiares e amigos dos envolvidos.

Os gestores de segurança também devem estar familiarizados com os conselhos incluídos no documento de orientação para os hotéis – *Fire Safety Risk Assessment*

O seu planeamento deve incluir as sete instruções-chave aplicáveis à maioria dos incidentes:

1. **Não tocar em objetos suspeitos.**
2. **Levar todas as pessoas para um local a uma distância segura.**
3. **Evitar que outros se aproximem.**
4. **Comunicar em segurança com o pessoal, com os visitantes em negócios e com o público.**
5. **Utilizar rádios portáteis ou telemóveis longe das imediações de um objeto suspeito, mantendo-se fora da linha de visão e atrás de uma zona protegida.**
6. **Avisar a polícia.**
7. **Assegurar que quem encontrou o objeto ou presenciou o incidente permanece no local para prestar declarações à polícia.**

Os planos de segurança eficazes são simples, claros e flexíveis, mas devem ser compatíveis com os planos existentes, como, por exemplo, os planos de evacuação e as estratégias de segurança em caso de incêndio. Todos devem ter a certeza do que devem fazer em caso de um incidente particular. Uma vez elaborados, os seus planos devem ser seguidos.

4. SEGURANÇA FÍSICA

A segurança física é importante na proteção contra uma variedade de ameaças e na redução de vulnerabilidades.

Coloque em prática medidas de segurança para eliminar ou reduzir as suas vulnerabilidades a um nível tão baixo quanto possível, tendo em conta que deve sempre considerar a segurança como sendo uma prioridade. Estas medidas não devem comprometer a estabilidade.

A sua avaliação dos riscos vai determinar que medidas deve adotar, que variam desde uma boa gestão interna básica (mantendo as áreas comuns limpas e arrumadas) a circuitos fechados de televisão, alarmes de intrusão, segurança de computadores e iluminação, passando por soluções especializadas como equipamento de verificação de correio eletrónico.

As soluções especializadas, em particular, devem basear-se numa avaliação minuciosa – de outra forma, pode investir em equipamento ineficaz, desnecessário e dispendioso.

Medidas de segurança bem-sucedidas requerem:

- O apoio de quadros superiores.
- Sensibilizar o pessoal para essas medidas e para a responsabilidade que tem no seu cumprimento.
- Um superior devidamente identificado dentro da organização que seja responsável pela segurança.

Ações que deve considerar

No início do processo, contacte o seu CTSA através da polícia da sua área. Pode aconselhá-lo no que diz respeito à segurança física, bem como encaminhá-lo para organismos profissionais que regulam e supervisionam os fornecedores de equipamento acreditados.

Lembre-se: vai precisar de garantir que todas os regulamentos exigidos são cumpridos, tais como a autorização de planeamento das autoridades locais, licenças de construção, requisitos de segurança e de saúde, bem como de prevenção de incêndios.

Planeie cuidadosamente, uma vez que isso pode ajudá-lo a reduzir os custos. Embora seja importante não atrasar a introdução do equipamento e dos procedimentos necessários, os custos podem ser reduzidos se as novas mudanças coincidirem com a construção de novos edifícios ou com renovações.

Sensibilização para as questões de segurança

A vigilância por parte dos seus funcionários (incluindo segurança, frente e traseiras do estabelecimento, limpeza, manutenção e pessoal contratado) é essencial para as suas medidas de proteção, uma vez que eles conhecem muito bem as suas próprias áreas de trabalho e os escritórios, devendo, por conseguinte, ser encorajados a estarem atentos a um comportamento fora do comum ou a objetos fora do lugar.

O pessoal deve ter confiança para reportar quaisquer suspeitas, sabendo que os seus relatórios – incluindo os falsos alarmes – serão levados a sério e considerados um contributo para o bom funcionamento do hotel ou restaurante.

Consequentemente, a formação é particularmente importante. O pessoal deve ser informado para prestar atenção a pacotes, malas ou outros objetos em locais estranhos, a objetos colocados cuidadosamente em caixotes do lixo (e não atirados para lá de forma descuidada) e ao interesse pouco usual de estranhos relativamente a locais menos acessíveis. Veja “Reconhecimento Hostil” na pág. 48.

Controlo de acessos

Os locais de acesso devem ser reduzidos ao mínimo. Certifique-se de que a fronteira entre as áreas pública e privada da sua atividade está assegurada e devidamente assinalada. Invista em sistemas de controlo de acessos de boa qualidade operados através de cartão magnético ou cartões de proximidade com o apoio de mecanismos de verificação do número de identificação pessoal. Veja “Controlo de Acessos” na página 16.

Cartões de segurança

Se tiver instalado um sistema de cartões para o pessoal, insista para que este ande sempre com os mesmos e que a sua emissão seja rigorosamente controlada e revista regularmente. Os visitantes das áreas privadas devem ser acompanhados e devem utilizar passes visivelmente identificados como ‘visitante’, que devem ser devolvidos à saída. Qualquer pessoa que não exiba cartões de segurança em áreas privadas deve ser interpelada ou imediatamente conduzida à segurança ou à gerência. Considere a hipótese de introduzir um sistema de cartões se ainda não o tiver.

Controlo e Patrulha

O controlo de malas é um dissuasor significativo que pode ser uma medida de segurança adequada ao seu hotel ou restaurante em certas alturas ou em eventos específicos.

As buscas e o patrulhamento de rotina às instalações representam outro nível de vigilância, cobrindo quer as áreas interiores quer as exteriores. Mantenha patrulhamentos regulares, embora não demasiado previsíveis (isto é, de hora a hora). Veja “Planos de Buscas” na página 28.

Controlo de trânsito e de estacionamento

Se acredita que pode estar em risco pela presença de um veículo armadilhado, o princípio básico é manter todos os veículos a uma distância de segurança. Aqueles cujo acesso é indispensável devem ser previamente identificados antes de lhes ser autorizada a entrada. Se possível, deve garantir que controla adequadamente os acessos e que dispõe de uma envolvente paisagística cuidada, medidas de controlo da velocidade e barreiras ou pinos retrácteis robustos e bem iluminados. O ideal será manter os veículos não essenciais a pelo menos 30 metros do seu edifício.

Para conselhos e orientação específicos do lugar em que se encontram as suas instalações, deve contactar o CTSA da sua polícia local. Veja também “Veículos com Dispositivos Explosivos Improvisados (VBIED)” na página 40.

Portas e janelas

Portas e janelas de boa qualidade são essenciais para garantir a segurança do edifício. As portas exteriores devem ser fortes, bem iluminadas e equipadas com fechaduras de boa qualidade. As portas que não são utilizadas com frequência devem ser protegidas interiormente em conformidade com as normas de segurança em caso de incêndio relevantes e a sua segurança deve ser monitorizada através de um sistema de alarme. **Isto é particularmente importante para os hotéis ou restaurantes que têm operações de busca ou de controlo externa de modo a evitar a entrada não autorizada ou desvios a qualquer sistema de investigação.**

- No mínimo, as janelas de fácil acesso devem estar protegidas com fechaduras de boa qualidade, com chave. A polícia pode dar-lhe mais conselhos sobre como melhorar a segurança de portas envidraçadas e janelas de acesso fácil.
- Muitas baixas nos atentados terroristas urbanos devem-se a estilhaços de vidro, em particular em edifícios modernos, e a proteção das superfícies envidraçadas é uma medida importante para a redução de vítimas.
- Têm sido levadas a cabo investigações exaustivas sobre os efeitos de uma explosão no vidro. Há tecnologias que minimizam os estilhaços e as baixas, bem como os custos de reocupação do edifício.
- A película anti-estilhaço, que retém os pedaços de vidro, constitui uma melhoria relativamente económica e rápida no que diz respeito às superfícies envidraçadas existentes. Se instalar janelas novas, tenha em consideração o vidro laminado, mas, antes de empreender quaisquer melhoramentos, procure o conselho de especialistas através do CTSA da sua polícia ou visite www.cpni.gov.uk para mais detalhes.

Sistemas de segurança integrados

Alarmes de intrusão, CCTV e iluminação são comummente utilizados para evitar crimes, detetar infratores e atrasar as suas ações. Todos estes sistemas devem estar integrados de forma a trabalharem em conjunto de um modo eficaz e coordenado.

A tecnologia de deteção de intrusos pode desempenhar um papel importante num sistema de segurança integrado, sendo, simultaneamente, um meio de dissuasão e de proteção. Se for requerida a resposta da polícia a qualquer alarme, o seu sistema deve ser compatível como a política de sistemas de segurança da *Association of Chief Police Officers* (ACPO) (www.acpo.police.uk ou, na Escócia, em www.acpos.police.uk). Para mais informações, contacte o Serviço de Alarmes na esquadra da sua polícia local.

Utilizar o CCTV pode ajudar a esclarecer se um alerta de segurança é real e é muitas vezes crucial em investigações posterior ao incidente quando as imagens têm qualidade suficiente para identificar o que aconteceu e podem ser utilizadas em tribunal.

A iluminação exterior constitui um meio de dissuasão e de deteção eficaz, mas tenha em conta o impacto de iluminação adicional nos seus vizinhos. Se for cuidadosamente concebida e utilizada, a iluminação exterior ajudará o pessoal de segurança e melhorará as capacidades dos sistemas de CCTV.

Lembre-se de que o CCTV só é eficiente se for devidamente monitorizado e preservado.

Veja “Orientações sobre Circuitos Fechados de Televisão (CCTV)” na página 18.

5. BOA GESTÃO INTERNA

A boa gestão interna melhora o ambiente do seu hotel ou restaurante, reduz a oportunidade de colocação de objetos ou sacos suspeitos e ajuda a lidar com alarmes falsos e embustes.

Pode reduzir o número de locais onde os dispositivos podem ser deixados se considerar os pontos seguintes:

- Se possível, evite a utilização de caixotes do lixo nas proximidades do restaurante (mas, se o fizer, certifique-se de que há uma limpeza adicional e rápida).
- Em alternativa, reveja a gestão dos caixotes do lixo e tenha em consideração o tamanho das suas aberturas, as suas capacidades de atenuar uma explosão e a localização, isto é, não coloque caixotes do lixo ao lado ou perto de superfícies envidraçadas ou de estruturas de suporte do edifício.
- A utilização de sacos transparentes para a colocação de resíduos é uma alternativa, uma vez que facilita a análise inicial dos objetos suspeitos.
- Reveja a utilização e a segurança de compactadores, caixotes com rodas e caixotes de metal utilizados para guardar lixo nas áreas de serviço, nas entradas de mercadoria e perto de áreas onde se verifica uma grande afluência de pessoas.
- Mantenhas as áreas públicas e comuns – saídas, entradas, áreas de receção, escadas, salões e instalações sanitárias – limpas e arrumadas, bem como os corredores e os pátios de serviço.
- Mantenha o mínimo de mobiliário nessas áreas, assegurando que há poucas oportunidades para esconder dispositivos, incluindo as áreas sob cadeiras e sofás.
- Tranque os escritórios, as salas e os armários de arrumação que não estão a ser usados.
- Assegure que tudo tem um lugar e que os objetos regressam a esse lugar.
- Coloque selos de plástico invioláveis nas escotilhas da manutenção.
- Mantenha as áreas exteriores tão limpas e arrumadas quanto possível.
- Todos os hotéis e restaurantes devem elaborar acordos para a gestão dos adjudicatários, dos veículos destes e dos serviços de lixo. A matrícula de cada veículo e os seus ocupantes devem ser fornecidos à segurança ou à administração com antecedência.
- A poda da vegetação e das árvores, em especial perto das entradas, vai ajudar na vigilância e prevenir a ocultação de quaisquer embalagens.

Além disto, tenha em conta os seguintes pontos:

Assegure-se de que todo o pessoal tem formação no que diz respeito a procedimentos para lidar com ameaças de bomba ou, pelo menos, tem acesso fácil a instruções e sabe onde elas estão (veja a "Lista de Verificação de Ameaças de Bomba").

Reveja o seu sistema de CCTV para assegurar que tem cobertura interna e externa suficientes.

A gestão deve assegurar que os extintores estão identificados como propriedade do restaurante ou hotel e verificar que não houve qualquer alteração ou substituição dos mesmos.

A administração do hotel deve identificar um local seguro secundário que funcione com sala de controlo (se tiver uma) como parte dos seus planos de contingência normais.

Todos os hotéis e restaurantes devem ter fontes de alimentação ininterrupta, disponíveis e testadas regularmente.

Veja a "Lista de Verificação de Boas Práticas – Gestão Interna" no Apêndice A.

6. CONTROLO DE ACESSOS

Qualquer falha de vigilância nas imediações das entradas pedonais ou de veículos do seu hotel ou restaurante, bem como das filas que se formem fora da sua área de segurança, permite que um potencial terrorista opere sob anonimato.

O pessoal de segurança designado para o exterior deve adotar uma abordagem de 'ver e ser visto' e, quando possível, policiar qualquer fila fora do estabelecimento. A fila deve ser ordenada, monitorizada por operadores de CCTV, caso existam, e deve ser estabelecida a comunicação entre clientes e funcionários.

Deve haver uma demarcação clara entre as áreas públicas e as privadas, com medidas apropriadas de controlo de acessos à entrada e à saída destas últimas. Isto diz respeito a áreas privadas dentro do hotel e restaurante, não a entradas públicas.

Avaliação dos riscos

Consulte a secção de "Gestão dos Riscos" na página 6 e determine qual o nível de segurança de que necessita antes de planear o seu sistema de controlo de acessos. Tenha em conta quaisquer características especiais de que possa precisar.

Aparência

O sistema de controlo de acessos às áreas privativas, corredores das traseiras e áreas de serviço é, normalmente, a primeira impressão de segurança que têm os clientes do seu hotel ou restaurante.

Facilidade de acesso

Examine a disposição do seu sistema. Assegure que os seus procedimentos de entrada e saída permitem que os utilizadores legítimos passem sem esforço ou demora desnecessários.

Formação

Assegure-se de que o seu pessoal está completamente ciente do papel e da operacionalidade do seu sistema de controlo de acessos. O responsável pela instalação do sistema deve fornecer formação adequada relativamente ao serviço.

Manutenção do sistema

O responsável pela instalação do sistema deve disponibilizar toda a documentação relevante, como, por exemplo, livros de registo e horários do serviço. Está ciente do que deve fazer em caso de avaria do sistema? Tem um contrato de manutenção do sistema que considere satisfatório?

Interação

O seu sistema de controlo de acessos deve funcionar como apoio a outras medidas de segurança. Tenha em consideração a compatibilidade entre sistemas.

Cumprimento de normas

O seu sistema de controlo acessos deve estar em conformidade com:

- A *Disability Discrimination Act* de 1995
- A *Data Protection Act* de 1998
- A *Human Rights Act* de 1998
- A *Fire Safety Order* de 2005
- Legislação sobre Saúde e Segurança (*Health and Safety Acts*)
- A *Fire (Scotland) Act* de 2005

O controlo de acessos é apenas um dos elementos importantes do seu sistema de segurança global.

LEMBRE-SE:
Quer esteja a guiar um camião ou a carregar explosivos, um terrorista necessita de acesso físico de modo a aceder ao alvo pretendido.

Veja a "Lista de Verificação de Boas Práticas – Controlo de Acessos" no Apêndice B.

7. ORIENTAÇÕES SOBRE CIRCUITOS FECHADOS DE TELEVISÃO (CCTV)

O CCTV pode ajudar a esclarecer se um alerta de segurança é real e é, normalmente, vital em qualquer investigação posterior ao incidente.

Deve monitorizar constantemente as imagens captadas pelo sistema de CCTV ou verificar regularmente as gravações à procura de atividade suspeita, assegurando sempre total conformidade com a *Data Protection Act* de 1998, que deve estar especificada na sua Política de Proteção de Dados relativos a CCTV.

Se contratar operadores de CCTV, estes devem estar certificados pela *Security Industry Authority* (SIA) quer o equipamento de CCTV seja instalado em posições fixas quer tenha possibilidades de rotação horizontal, rotação vertical e *zoom* e em que os operadores:

- Monitorizam proactivamente as atividades dos membros do público quer estejam em áreas públicas ou em propriedade privada.
- Utilizam as câmaras para focar as atividades de pessoas específicas quer pelo controlo ou pelo direcionamento das câmaras para as atividades de um indivíduo.
- Utilizam as câmaras para procurar indivíduos específicos.
- Utilizam as imagens de CCTV gravadas para identificar indivíduos ou investigar as suas atividades.

Desde 20 de março de 2006, os operadores de CCTV contratados devem ter uma licença de CCTV SIA (*Public Space Surveillance*), sem a qual é ilegal trabalhar. O seu adjudicatário deve estar ciente disto e deve assegurar-se de que trabalha apenas com pessoal credenciado.

O licenciamento da SIA aplica-se na Escócia desde 1 de novembro de 2007. Pode encontrar mais orientações em www.the-sia.org.uk/home/scotland.

As câmaras de CCTV devem, se possível, cobrir todas as entradas e saídas dos seus estabelecimentos e outras áreas críticas, para uma gestão segura e para segurança da sua atividade.

Existindo cada vez mais organizações a optar por sistemas de CCTV digitais, deve estabelecer contacto com a polícia local para se certificar de que o *software* do seu sistema é compatível com o deles de forma a possibilitar-lhes a recuperação e utilização das suas imagens para efeitos de prova.

Coloque a si próprio as seguintes questões:

- O seu sistema de CCTV está atualmente a fazer o que é preciso? Precisa dele para confirmar alarmes, detetar intrusos através de portas ou corredores e produzir imagens com qualidade suficiente para ser usadas como prova?
- As câmaras de CCTV em funcionamento para a segurança do seu hotel ou restaurante estão integradas com as que são utilizadas para monitorizar o movimento de clientes?
- A introdução de um sistema de *Automatic Number Plate Reader* (ANPR) (Leitura Automática de Matrículas) poderá complementar a sua operação de segurança?

O *Home Office Scientific Development Branch* (HOSDB) publicou muitos documentos úteis relacionados com o CCTV, incluindo o *CCTV Operational Requirements Manual* (Ref: 55/06), o *UK Police Requirements for Digital CCTV Systems* (Ref: 09/05) e o *Performance Testing of CCTV Systems* (Ref: 14/95).

Tenha também em conta os pontos seguintes:

- Assegure-se de que os registos de data e hora do sistema são rigorosos e se encontram sincronizados.
- Verifique regularmente a qualidade das gravações.
- As imagens de CCTV digitais devem ser guardadas de acordo com as necessidades de provas por parte da Polícia. Veja a publicação 09/05 do HOSDB.
- Assegure-se de que o seu sistema é complementado por iluminação apropriada de dia e de noite.
- No caso dos sistemas analógicos, mude as cassetes diariamente – não utilize a mesma mais do que 12 vezes.
- Mantenha as cassetes durante 31 dias, pelo menos.
- Utilize cassetes de vídeo de boa qualidade e verifique-as regularmente passando-as numa máquina diferente.
- Assegure-se de que as imagens gravadas são nítidas – que as pessoas e os veículos estão claramente identificados.
- Verifique que as imagens captadas são da área certa.
- Implemente procedimentos operacionais, códigos de conduta e pistas de auditoria normalizados.
- Tenha em conta o número de imagens de câmara que um único operador de CCTV pode monitorizar eficazmente em simultâneo.
- Tem pessoal qualificado suficiente para continuar a monitorizar o seu sistema de CCTV durante um incidente, uma evacuação ou uma busca?

Veja a "Lista de Verificação de Boas Práticas – CCTV" no Apêndice C.

Manutenção de CCTV

A manutenção de CCTV deve ser planeada e organizada previamente e não levada a cabo numa base *ad hoc*. Se a manutenção regular não for efetuada, o sistema pode eventualmente não conseguir cumprir os requisitos operacionais.

O que poderá ocorrer se um sistema não for alvo de manutenções?

- O sistema adquire **SUJIDADE**, o que enfraquece a sua utilização.
- Os **CONSUMÍVEIS** gastam-se, o que causa um desempenho deficitário.
- Podem ocorrer **FALHAS** dos componentes principais.
- Os danos provocados por **CONDIÇÕES METEOROLÓGICAS** podem provocar uma cobertura incorreta.
- Os danos **DELIBERADOS**/mudanças ambientais e as infrações das medidas de segurança podem passar despercebidos.

8. TRATAMENTO DE CORRESPONDÊNCIA

Os hotéis e restaurantes podem receber grandes quantidades de correspondência e outras de entregas, o que oferece aos terroristas uma via atrativa para o acesso às instalações.

Objetos Entregues

Os objetos entregues, incluindo cartas, pacotes, embalagens e tudo o que seja entregue por correio ou por um estafeta, têm sido uma estratégia vulgarmente utilizada pelos terroristas. Uma avaliação dos riscos devidamente conduzida deve dar-lhe uma ideia da ameaça provável para a sua organização e indicar quais as precauções a tomar.

Os objetos entregues podem ser explosivos ou incendiários (os dois tipos mais comuns), químicos, biológicos ou radiológicos. É improvável que quem quer que receba uma entrega suspeita saiba qual o seu tipo, por isso os procedimentos devem ser adequados a qualquer eventualidade.

Um objeto entregue recebeu, provavelmente, um tratamento bastante descuidado nos correios e, por isso, é improvável que detone devido ao movimento, mas qualquer tentativa para o abrir, ainda que mínima, pode fazê-lo explodir. A menos que seja entregue por estafeta, é improvável que contenha um dispositivo com temporizador. Os objetos entregues apresentam uma grande variedade de formas e tamanhos; um dispositivo bem feito parecerá inócuo, mas poderá evidenciar sinais denunciadores.

Indicadores de Correspondência Suspeita

- É inesperada, de origem suspeita ou remetente desconhecido.
- Não há endereço de devolução ou este não pode ser verificado.
- Está incorreta ou erradamente endereçada, por exemplo, tem um título incorreto ou mal escrito, tem título mas não nome, ou é endereçada a um indivíduo que já não está na empresa.
- O endereço foi impresso irregularmente ou de forma não habitual.
- A escrita está num estilo pouco familiar ou pouco habitual.
- Há carimbos postais ou marcas de porte pago pouco habituais.
- Foi utilizado um envelope almofadado ou semelhante.
- Parece ter um peso não adequado ao seu tamanho. A maioria das cartas pesa até 28g, enquanto as cartas-bomba mais eficazes pesam 50-100g e têm uma espessura de 5mm ou mais.
- Tem mais do que o valor de selos apropriado para o seu tamanho e peso.
- Está identificado como ‘pessoal’ ou ‘confidencial’.
- Tem uma forma estranha ou desequilibrada.
- A aba do envelope está completamente colada (normalmente, uma carta inofensiva tem, nos cantos, uma fenda descolada de 3-5mm).
- Há um buraco do tamanho de um alfinete no envelope ou no embrulho.
- Existe um odor, em especial a amêndoas ou a maçapão.
- Contém um envelope interior adicional e está colado ou atado firmemente (contudo, algumas organizações enviam, normalmente, o material sensível ou ‘restrito’ em envelopes duplos).

Materiais químicos, biológicos ou radiológicos enviados por correio

Os terroristas podem tentar enviar materiais químicos, biológicos ou radiológicos (QBR) por correio. É difícil providenciar uma lista completa dos possíveis indicadores de QBR devido à natureza diversa dos materiais. Contudo, alguns dos mais óbvios e comuns são:

- Material granulado, cristalino ou em pó fino inesperado (de qualquer cor e, normalmente, com a consistência do café, do açúcar ou do fermento em pó), à solta ou num recipiente.
- Substâncias viscosas, *sprays* ou vapores inesperados.
- Peças de metal ou de plástico inesperadas, como discos, varetas, folhas pequenas ou esferas.
- Odores estranhos, por exemplo, a alho, peixe, fruta, naftalina ou pimenta. Se detetar um odor, tente não o inalar. Contudo, certos materiais QBR são inodoros e insípidos.
- Manchas ou humidade na embalagem.
- Início repentino de doença ou irritação na pele, nos olhos ou no nariz.

Os dispositivos de QBR que contêm um pó finamente moído ou um líquido podem ser perigosos mesmo sem serem abertos.

O que pode fazer:

- A natureza precisa do incidente (química, biológica ou radiológica) pode não ser imediatamente percetível. Mantenha ativos os seus planos de resposta e espere pela ajuda especializada dos serviços de emergência.
- Reveja os planos para proteger os funcionários e os clientes no caso de uma ameaça ou de um atentado terrorista. Lembre-se de que a evacuação pode não ser a melhor solução. Nesse momento, precisará da orientação dos serviços de emergência.
- Planeie a desativação de sistemas que possam contribuir para a circulação aérea de materiais perigosos (por exemplo, equipamentos informáticos que contenham ventoinhas ou unidades de ar-condicionado).
- Assegure-se de que as portas podem ser fechadas rapidamente se for necessário.
- Se as suas janelas exteriores não estão permanentemente seladas, desenvolva planos para as fechar em resposta a um aviso ou incidente.
- Examine a viabilidade da desativação de emergência dos sistemas de circulação de ar e assegure-se de que qualquer plano está bem ensaiado.
- Quando um perigo puder ser isolado através da evacuação imediata da área, faça-o o mais rápido possível, fechando as janelas e as portas à medida que vai saindo.
- Desloque todos aqueles que possam ser diretamente afetados por um incidente para um sítio seguro, o mais próximo possível do local do incidente, para minimizar a propagação da contaminação.
- Separe aqueles que foram diretamente afetados por um incidente daqueles que não foram envolvidos, de modo a minimizar o risco acidental de contaminação cruzada.
- Peça às pessoas para se manterem no mesmo local – embora não as possa reter contra a sua vontade.

Não precisa de tomar medidas especiais para além da prestação de primeiros socorros. Os serviços de emergência responsabilizar-se-ão pelo tratamento das vítimas.

Planeamento dos procedimentos de tratamento de correspondência

Embora qualquer objeto suspeito deva ser levado a sério, lembre-se de que a maioria constitui falsos alarmes e alguns podem ser embustes. Tente garantir que os seus procedimentos, ainda que eficazes, não são desnecessariamente perturbadores. Tenha em conta o seguinte ao elaborar o seu planeamento:

- Procure o aconselhamento do CTSA da polícia local acerca da ameaça e de medidas defensivas.
- Concentre o processamento de toda a correspondência e entregas num único local. Idealmente, isto deveria ter lugar fora das instalações ou noutro edifício ou, pelo menos, numa área que possa ser facilmente isolada e onde as entregas possam ser manuseadas sem terem de ser levadas por outras partes do hotel ou restaurante.
- Assegure-se de que todo o pessoal que manuseia a correspondência está informado e treinado. Inclua o pessoal da receção e encoraje os correspondentes habituais a colocar o endereço do remetente em cada objeto.

- Assegure-se de que todas as fontes de entrega de correspondência (por exemplo, correios, estafetas e entrega em mão) estão incluídas no seu processo de triagem.
- Idealmente, as salas de correio devem ter ar-condicionado e sistemas de alarme independentes, bem como *scanners* e máquinas de raios-X. Contudo, embora os *scanners* possam detetar dispositivos, por estes libertarem materiais QBR (por exemplo, engenhos explosivos), eles não irão detetar os materiais propriamente ditos.
- Atualmente, não existem detetores de QBR capazes de identificar com fiabilidade todos os riscos.
- As salas de correio também devem ter as suas próprias instalações sanitárias, com sabão e detergente.
- Os funcionários devem ser conhecedores do padrão habitual das entregas e informados de ocorrências não habituais. Treine-os para abrir o correio com abre-cartas (e com o mínimo de movimentos), para manter as mãos afastadas do nariz e da boca e para lavar sempre as mãos após o manuseamento da correspondência. Não devem soprar para os envelopes nem agitá-los. Idealmente, as embalagens suspeitas de conterem material biológico, químico ou radiológico devem ser colocadas num saco duplamente selado.
- Verifique se o pessoal que trata do correio precisa de equipamento de proteção, como luvas de látex e máscaras faciais (procure aconselhamento de um especialista em saúde e segurança qualificado). Tenha disponíveis fatos-macaco e calçado para o caso de o pessoal precisar de retirar a roupa contaminada.
- Tenha a certeza de que as áreas de abertura de correspondência podem ser evacuadas com prontidão. Ensaie procedimentos e vias de evacuação, que devem incluir as instalações para lavagem do corpo onde o pessoal contaminado possa ser isolado e tratado.
- O pessoal responsável pelo tratamento de correspondência deve estar ciente da importância do isolamento para a redução da contaminação.
- Prepare sinalética para mostrar ao pessoal em caso de uma suspeita de atentado ou de um atentado real.

9. PLANOS DE BUSCAS

As buscas em hotéis e restaurantes devem fazer parte de uma rotina diária de boa gestão interna. Devem, também, ser conduzidas em resposta a uma ameaça específica e quando se verifica um nível de resposta elevado.

Como já foi mencionado na "Planificação da Segurança", é reconhecido que, para a maioria dos hotéis e restaurantes, a implementação de qualquer plano de buscas, após uma avaliação de vulnerabilidade e riscos, é da responsabilidade do gestor da segurança ou do gestor das operações.

Os conselhos que se seguem são genéricos para a maioria dos hotéis, mas reconhecem que estes são construídos e geridos de forma diferente. Se for necessário, deve procurar aconselhamento e orientação sobre planos de buscas junto do seu CTSA ou do *Police Search Adviser* (POLSA).

Planos de buscas

- Os planos de buscas devem ser preparados com antecedência e o pessoal deve estar devidamente treinado.
- A condução de buscas dependerá das circunstâncias do local e do conhecimento do mesmo, mas o objetivo principal é assegurar que os estabelecimentos e os terrenos sejam revistados de forma sistemática e minuciosa para que nenhuma parte seja deixada por verificar.
- Se decidir evacuar o seu hotel ou restaurante em resposta a um incidente ou a uma ameaça, também precisará de o revistar de modo a garantir que a sua reocupação é segura.
- A polícia não irá normalmente revistar hotéis ou restaurantes (Veja "Eventos de Grande Visibilidade" na página 52). Não conhece as instalações e não estará ciente do que ali devia estar e do que está fora do lugar. Não pode, por isso, revistar a área tão rapidamente nem tão minuciosamente como um membro do seu pessoal ou um membro do pessoal de segurança do local.
- Os membros do pessoal nomeados para levar a cabo as buscas não precisam de ter conhecimento acerca de explosivos ou outro tipo de dispositivos, mas devem estar familiarizados com o local que estão a revistar. Estão à procura de objetos que não devam estar ali, que não tenham explicação, e objetos que estejam fora do sítio.
- Idealmente, o pessoal de busca deve operar em equipas de dois elementos, para assegurar que as buscas são sistemáticas e minuciosas.

Medidas que deve tomar

Considere dividir o seu hotel ou restaurante em setores. Se o local estiver organizado por departamentos e secções, estes devem ser identificados como setores de busca separados. Cada setor deve ter um tamanho controlável.

O plano de buscas de cada setor deve ter uma lista de verificação – assinada quando estiver finalizada – para informação do gestor de segurança do hotel ou restaurante.

Lembre-se de incluir escadas, saídas de emergência, corredores, casas-de-banho e elevadores no plano de buscas, bem como estacionamentos, áreas de serviço e outras áreas no exterior do edifício. Se for considerada ou implementada a

evacuação, antes de esta ter lugar, devem também ser realizadas buscas às áreas de concentração, às respetivas vias de acesso e à área circundante.

Considere qual o método mais eficaz de iniciar as buscas. Pode:

- Enviar uma mensagem para as equipas de buscas através de um sistema sonoro para comunicações públicas (as mensagens devem ser codificadas para evitar perturbações e alarme desnecessários).
- Utilizar rádios pessoais ou *pagers*.

O seu planeamento deve incorporar as sete instruções-chave aplicáveis à maioria dos incidentes:

1. **Não tocar em objetos suspeitos.**
2. **Mover todas as pessoas para um local a uma distância segura.**
3. **Evitar que outros se aproximem.**
4. **Comunicar em segurança com o pessoal, com os visitantes e com o público.**
5. **Utilizar rádios portáteis ou telemóveis longe das imediações de um objeto suspeito, mantendo-se fora da linha de visão e atrás de uma zona protegida.**
6. **Avisar a polícia.**
7. **Assegurar que quem encontrou o objeto ou presenciou o incidente permanece no local para prestar declarações à polícia.**

Ponha regularmente em prática o seu plano de buscas. O pessoal de buscas precisa de ter uma ideia dos passos lógicos a realizar na área que lhes for atribuída e do tempo que tais passos levarão. Deve também ter a capacidade de fazer buscas sem alarmar excessivamente os clientes.

Pode haver ocasiões em que revistar clientes, visitantes e os seus pertences seja considerado um nível apropriado de segurança. Isto pode dever-se a um aumento da ameaça ou do nível de resposta ou a um evento importante. Os hotéis e restaurantes devem considerar a implementação de um regime de buscas que seja flexível e possa ser adaptado a eventuais alterações.

Discuta o seu plano de buscas com o CTSA da polícia local ou com o POLSA.

Veja a "Lista de Verificação de Boas Práticas – Buscas" no Apêndice D.

10. PLANOS DE EVACUAÇÃO

Tal como o planeamento de buscas, a evacuação deve ser parte do seu plano de segurança. Pode ter de evacuar o seu estabelecimento devido a:

- **Uma ameaça recebida diretamente no seu estabelecimento.**
- **Uma ameaça recebida noutro local** e da qual lhe foi dado conhecimento pela polícia.
- **Uma descoberta de um objeto suspeito no hotel ou restaurante** (talvez uma embalagem postal, um saco de viagem ou uma mochila não reclamados).
- **Uma descoberta de um objeto suspeito ou de um veículo no exterior do edifício.**
- **Um incidente** para o qual a polícia o alertou.

Quaisquer que sejam as circunstâncias, deve dizer à polícia, tão rapidamente quanto possível, o que vai fazer.

O maior dilema com que alguém responsável por um plano de evacuação se confronta é saber qual poderá ser o local mais seguro. Por exemplo, se a rota de evacuação fizer com que as pessoas passem por algo suspeito no exterior do edifício ou através de uma área que se acredita estar contaminada, a evacuação para o exterior pode não ser a melhor medida a tomar.

Algo a ter em conta quando planear rotas de evacuação em resposta a atentados terroristas quase simultâneos é assegurar-se de que as pessoas são levadas para longe de outras áreas possivelmente vulneráveis ou de áreas onde um instrumento secundário de maiores dimensões possa explodir.

A decisão de evacuar a área será normalmente sua, mas a polícia dar-lhe-á conselhos. Em casos excecionais, a polícia pode insistir na realização da evacuação, embora deva fazê-lo sempre em conjunto com o seu gestor de segurança. Do mesmo modo, a polícia pode ter necessidade de aconselhar a não evacuação do estabelecimento, por exemplo, quando tem informação específica de que há um dispositivo explosivo no exterior do edifício, podendo a evacuação colocar as pessoas em maior risco.

Uma regra geral é descobrir se o dispositivo está no exterior ou no interior do estabelecimento. Se estiver no interior, deve tomar em consideração a evacuação; porém, se o dispositivo estiver no exterior do edifício, pode ser mais seguro ficar no interior.

Planear e iniciar a evacuação deve ser da responsabilidade do gestor de segurança.

Dependendo do tamanho do hotel ou restaurante e da sua localização, o plano pode incluir:

- Evacuação total do exterior do edifício.
- Evacuação de parte do edifício, se o dispositivo for pequeno e se pensar que está limitado a um local (por exemplo, uma carta armadilhada na sala do correio).
- Evacuação total ou parcial para uma área segura no interior, como, por exemplo, um espaço protegido, se estiver disponível.
- Evacuação de todo o pessoal à exceção do pessoal de busca nomeado.

Evacuação

As instruções de evacuação devem ser comunicadas com clareza ao pessoal e as rotas e saídas devem estar bem definidas. Designe pessoas que atuem como agentes policiais e como contactos quando se chegar à área de concentração. As áreas de concentração devem distar, no mínimo, 500 metros do incidente. No caso da maioria dos veículos armadilhados, por exemplo, esta distância colocá-las-ia para além dos cordões da polícia – embora fosse recomendável ter uma alternativa a uma distância de cerca de um quilómetro.

É importante assegurar que o pessoal está ciente das localizações das áreas de concentração no caso de uma evacuação devido a um incidente, bem como das áreas de evacuação no caso de uma evacuação devido a um incêndio. É igualmente importante garantir que os responsáveis pelo encaminhamento do público não confundam essas áreas de concentração.

Os parques de estacionamento não devem ser utilizados como áreas de concentração. Além disso, as áreas de concentração devem ser sempre examinadas antes de serem utilizadas.

O pessoal com deficiência deve ser informado individualmente acerca dos procedimentos de evacuação respetivos.

Em caso de suspeita de:

Cartas ou encomendas armadilhadas

Evacue de imediato a sala e o piso em questão e as salas adjacentes, bem como os dois pisos imediatamente acima e abaixo.

Incidentes Químicos, Biológicos e Radiológicos

As respostas a incidentes QBR irão variar mais do que aquelas que envolvam dispositivos convencionais ou incendiários, mas devem ser tidos em conta os seguintes pontos gerais:

- A natureza exata de um incidente pode não ser imediatamente evidente. Por exemplo, um engenho explosivo improvisado também pode envolver a libertação de material QBR.
- Em caso de suspeita de um incidente QBR dentro do edifício, desligue todos os sistemas de climatização, ventilação e outros, ou objetos que impliquem circulação de ar (por exemplo, ventoinhas e computadores pessoais). Não permita que ninguém, tenha ou não estado exposto, saia das áreas de evacuação antes de os serviços de emergência terem providenciado aconselhamento, avaliações ou tratamento médico.
- No caso de um incidente no exterior do edifício, feche todas as portas e janelas e desligue todos os sistemas de ventilação de ar do edifício.

Com antecedência, combine com os serviços de polícia e de emergência, com as autoridades locais e com os seus vizinhos o plano de evacuação. Assegure-se de que o pessoal com responsabilidades específicas tem formação adequada e de que todo o pessoal está treinado. Lembre-se, igualmente, de dizer à polícia o que vai fazer perante qualquer incidente.

Os gestores de segurança devem certificar-se de que têm conhecimentos práticos dos sistemas de aquecimento, ventilação e ar-condicionado (AVAC) e de como estes podem contribuir para a propagação de materiais QBR no interior do edifício.

Espaços Protegidos

Os espaços protegidos podem oferecer abrigo contra explosões, estilhaços de vidro e outros fragmentos. Também podem oferecer a melhor proteção quando a localização da bomba é desconhecida, podendo estar perto da via de evacuação para o exterior, ou em caso de um atentado QBR no exterior.

Uma vez que o vidro e outros fragmentos podem matar ou ferir a uma distância considerável do centro de uma grande explosão, deslocar o pessoal para espaços protegidos é, habitualmente, mais seguro do que proceder à sua evacuação para a rua. Os espaços protegidos devem estar localizados:

- Em áreas com paredes de alvenaria como, por exemplo, corredores internos, instalações sanitárias ou salas de conferências com portas a abrir para o interior.
- Longe de janelas, portas e paredes exteriores.
- Longe da área localizada entre o perímetro do edifício e a primeira linha de pilares de suporte (conhecida como 'vão estrutural do perímetro').
- Longe de escadarias ou de áreas com acesso a poços de elevador se estes abrirem ao nível do solo para a rua, uma vez que a explosão pode subir através deles. Contudo, se os núcleos da escada e do elevador forem completamente fechados, são bons espaços protegidos.
- Se possível, não ao nível do solo ou do primeiro andar.
- Numa área com espaço suficiente para acolher os ocupantes.

Quando estiver a escolher um espaço protegido, aconselhe-se com um engenheiro mecânico com conhecimentos sobre efeitos explosivos e não negligencie a disponibilização de instalações sanitárias, assentos, água potável e comunicações.

Considere a hipótese de duplicar os sistemas ou recursos críticos noutros edifícios a uma distância suficiente para que não sejam afetados numa emergência que não lhe permita aceder ao seu próprio edifício. Se tal for impossível, tente que os sistemas vitais estejam localizados numa parte do edifício que ofereça proteção semelhante à que é providenciada por um espaço protegido.

Comunicações

Assegure-se de que o pessoal designado conhece o seu papel na segurança e de que eles próprios ou os seus representantes estão sempre contactáveis. Todo o pessoal, incluindo o pessoal noturno ou temporário, deve estar familiarizado com as instalações de gravação telefónica, remarcação ou visualização e saber como contactar a polícia e o pessoal de segurança dentro ou fora do horário de trabalho.

É essencial ter comunicações adequadas dentro de e entre espaços protegidos. A determinada altura, vai querer dar luz verde ou dizer ao pessoal que permaneça onde está, que vá para outro espaço protegido ou que evacue o edifício. As comunicações podem ser realizadas através de um sistema público (para o qual precisará de alimentação suplementar), rádios portáteis ou outros sistemas autónomos. Quaisquer que sejam os sistemas que escolher, estes devem ser testados regularmente e estar disponíveis no interior do espaço protegido.

Conversão para *open space*

Se está a transformar o seu edifício num espaço *open space*, lembre-se de que a remoção de paredes interiores reduz a proteção contra explosões e fragmentos.

Muitas vezes, as salas interiores com paredes de betão armado ou de alvenaria são espaços protegidos adequados, uma vez que têm tendência para permanecer intactas caso haja uma explosão no exterior do edifício. Se já não houver corredores, pode igualmente perder as suas vias de evacuação, as áreas de concentração e os espaços protegidos; a nova planta irá, provavelmente, afetar os seus procedimentos de contingência no caso de uma ameaça de bomba.

Quando realizar tais alterações, tente assegurar-se de que não existe uma redução significativa na proteção do pessoal, introduzindo, por exemplo, melhorias na proteção das superfícies envidraçadas. Se os seus estabelecimentos já forem em *open space* e não existirem espaços protegidos adequados, a evacuação pode ser a sua única opção.

11. SEGURANÇA DO PESSOAL

Algumas ameaças externas, feitas por criminosos, por terroristas ou por concorrentes à procura de benefícios para as suas empresas, podem contar com a colaboração de um 'infiltrado'. Este pode ser um empregado ou qualquer trabalhador contratado ou temporário (por exemplo, empregado de limpeza ou de segurança, assim como um fornecedor) que tenha acesso autorizado ao seu estabelecimento. Se for um empregado, pode já estar a trabalhar para si há algum tempo ou ser alguém que tenha sido contratado recentemente e que se tenha infiltrado na sua organização para obter informações ou explorar as instalações.

O que é a segurança do pessoal?

A segurança do pessoal é um sistema de políticas e procedimentos que procuram gerir os riscos de o pessoal ou de adjudicatários tirarem partido do acesso legítimo a mercadorias ou a estabelecimentos para fins não-autorizados. Estes fins podem abranger diversas formas de atividade criminosa, desde pequenos furtos ao terrorismo.

A segurança do pessoal tem como objetivo a minimização dos riscos, o qual é concretizado quando as organizações empregam indivíduos com credibilidade, reduzindo as possibilidades de o pessoal se tornar indigno de confiança depois de contratado. Quando os comportamentos suspeitos são detetados e as preocupações com a segurança estão resolvidas, os riscos são igualmente minimizados.

Este capítulo refere-se, principalmente, ao controlo dos antecedentes laborais, mas as organizações devem estar cientes de que o controlo do pessoal deve continuar ao longo do ciclo de vida do empregado. Pode encontrar mais informação acerca do controlo contínuo do pessoal em www.cpni.gov.uk.

Compreender e avaliar os riscos de segurança do pessoal

É frequente as organizações lidarem com muitos tipos de risco diferentes. Um deles consiste na possibilidade de os funcionários ou os adjudicatários abusarem da sua posição na organização para fins ilegítimos. Estes riscos podem ser reduzidos, mas nunca podem ser totalmente evitados. Em vez disso, como acontece com muitos outros riscos, a organização deve utilizar um processo contínuo para garantir que os riscos sejam geridos de forma proporcionada e rentável.

Lei de Proteção de Dados

A *Data Protection Act* de 1998 aplica-se ao processamento de informação pessoal dos indivíduos. As medidas de segurança do pessoal devem ser levadas a cabo de acordo com os princípios de proteção de dados estabelecidos na lei.

Controlo dos antecedentes laborais

A segurança do pessoal envolve um número de procedimentos de controlo, os quais fazem parte do processo de recrutamento, mas também são aplicados de forma regular no que diz respeito ao pessoal existente. A forma como o controlo é levado a cabo varia muito de organização para organização: alguns métodos são mais simples e outros são mais sofisticados. Em todos os casos, o objetivo do controlo é recolher informação

acerca do pessoal potencial ou existente e, depois, utilizar essa informação para identificar quaisquer indivíduos que coloquem problemas à segurança.

O controlo dos antecedentes laborais procura verificar as credenciais dos candidatos a um trabalho e averiguar se os candidatos satisfazem os requisitos de emprego (por exemplo, se o candidato tem permissão legal para aceitar uma oferta de emprego). No decorrer destes controlos, determinar-se-á se o candidato ocultou informação importante ou, ainda, se prestou falsas declarações. Nesta medida, o controlo de antecedentes laborais pode ser considerado um teste de personalidade.

Verificação da pré-contratação

A segurança do pessoal começa com a candidatura ao emprego, durante o qual os candidatos devem ser sensibilizados para o facto de o fornecimento de informação falsa ou a falha na divulgação de informação relevante poderem ser motivos para o despedimento e constituir uma infração penal. Os candidatos também devem saber que qualquer oferta de emprego está sujeita à conclusão satisfatória da verificação dos antecedentes laborais. Se uma organização pensa que há uma candidatura fraudulenta que envolve atividade ilegal, a polícia deve ser informada.

A verificação dos antecedentes laborais pode ser realizada diretamente por uma organização ou subcontratada a terceiros. Em qualquer dos casos, a empresa necessita de compreender claramente quais os motivos para negar emprego a alguém. Por exemplo, sob que circunstâncias seria um candidato rejeitado com base no seu registo criminal e porquê?

Política de controlo dos antecedentes laborais

Os processos de controlo dos antecedentes laborais serão mais eficientes se forem parte integrante das suas políticas, práticas e procedimentos para o recrutamento, a contratação e, quando necessário, a formação dos empregados. Se levou a cabo uma avaliação dos riscos da segurança do pessoal, isto ajudá-lo-á a decidir quais os níveis de controlo apropriados para os diferentes postos.

Identidade

De todos os controlos dos antecedentes laborais, a verificação da identidade é o mais importante. Podem ser utilizadas duas abordagens:

- Uma abordagem em suporte de papel que envolva a verificação de documentos-chave de identificação e a correspondência entre esses documentos e o portador.
- Uma abordagem eletrónica que envolva pesquisas em bases de dados (por exemplo, bases de dados de contratos de crédito ou de recenseamento) para se estabelecer o percurso eletrónico do indivíduo. Depois solicita-se ao candidato que responda a perguntas acerca desse percurso, às quais apenas o verdadeiro dono da identidade poderia responder corretamente.

Os controlos dos antecedentes laborais podem ser utilizados para confirmar a identidade, a nacionalidade e o estatuto de imigrante de um candidato, assim como para verificar a sua experiência e as qualificações que declarou.

A *Immigration, Asylum and Nationality Act* de 2006 entrou em vigor em fevereiro de 2008, o que indica que há mudanças na lei e os **empregadores enfrentam novas exigências para evitar o trabalho ilegal no Reino Unido**. Estas mudanças incluem a responsabilidade contínua de levar a cabo controlos sobre os empregados com estatuto provisório de imigrante. A falha no cumprimento das novas regras pode resultar em multa ou em condenação penal. A orientação do *Centre for the Protection of National Infrastructure* (CPNI) relativamente ao controlo dos antecedentes laborais foi atualizada de forma a incorporar esta nova lei. Pode encontrar informação mais detalhada no sítio da *Borders and Immigration Agency* (www.bia.homeoffice.gov.uk).

Qualificações e carreira profissional

A verificação das qualificações e da carreira profissional podem ajudar a identificar os candidatos que tentarem ocultar informações negativas, como, por exemplo, penas de prisão ou despedimentos. As lacunas inexplicadas devem ser analisadas.

Qualificações

Descobriu-se que um contabilista estava a defraudar uma organização da Infraestrutura Nacional. Quando o caso foi investigado, soube-se que o indivíduo não tinha todas as qualificações e tinha mentido acerca das suas habilitações académicas numa entrevista.

Quando estiver a confirmar os detalhes das qualificações de um indivíduo, é sempre importante:

- Considerar se o argo necessita de um controlo das qualificações.
- Solicitar os certificados originais e tirar fotocópias.
- Comparar as informações constantes no certificado com as fornecidas pelo candidato.
- Confirmar por si a existência do estabelecimento de ensino e entrar em contacto com este para confirmar os detalhes fornecidos pelo indivíduo.

Controlos laborais

Por razões legais, é cada vez mais difícil obter referências, mas deve ser solicitado aos empregadores que confirmem as datas de trabalho. Nos locais onde foram levados a cabo controlos laborais, é importante:

- Conferir um mínimo de três, mas idealmente cinco, anos de trabalho anterior.
- Confirmar por si próprio a existência do empregador e os respetivos contactos (incluindo os do superior hierárquico).
- Confirmar datas, posição e salário com os Recursos Humanos.
- Se possível, pedir ao superior hierárquico referências do empregador.

Condenações penais

Uma condenação penal – cumprida ou não – não é necessariamente um obstáculo para o emprego (veja a *Rehabilitation of Offenders Act*). Contudo, há certas posições onde certas formas de registo criminal serão inaceitáveis. Para obter informação acerca do registo criminal, e empresa deve pedir ao candidato que:

1. Complete um formulário de como uma declaração do próprio sobre o seu registo criminal ou
2. Solicite o *Basic Disclosure certificate* da Disclosure Scotland.

Controlos financeiros

Para alguns cargos, pode justificar-se levar a cabo controlos financeiros quando, por exemplo, a função do empregado exige lidar com dinheiro. Não é simples interpretar as implicações de segurança do historial financeiro; isto exigirá que cada organização determine os seus limites (por exemplo, em termos de nível aceitável de dívida).

Há variadas formas de se levar a cabo controlos financeiros. Os formulários de candidatura gerais podem incluir um elemento de auto-declaração (por exemplo em relação às *County Court Judgments* (CCJs)) ou pode-se contratar os serviços de terceiros para levar a cabo controlos de crédito.

Recrutamento de adjudicatários

As organizações empregam uma vasta variedade de pessoal contratado, como pessoal informático, pessoal de limpeza e consultores de gestão. É importante assegurar que os adjudicatários têm o mesmo nível de controlo de antecedentes laborais que os funcionários permanentes com níveis de acesso equivalentes aos bens da empresa, sejam eles instalações, sistemas, informações ou pessoal.

Os contratos devem delinear o tipo de controlos necessários para cada cargo e os requisitos devem ser transmitidos em cascata a todos os sub-adjudicatários. Seja um adjudicatário seja uma agência de controlo a levar a cabo os controlos, também eles devem ser auditados (veja o capítulo ‘Contrato Seguro’ para orientação adicional no que diz respeito a lidar com adjudicatários através do sítio do CPNI.

Controlos estrangeiros

Com o crescimento do nível de terciarização e o aumento do número de cidadãos estrangeiros a trabalhar nas Infraestruturas nacionais, é cada vez mais necessário controlar os candidatos que tenham vivido ou trabalhado no estrangeiro. As organizações devem procurar, tanto quanto possível, recolher para os candidatos estrangeiros a mesma informação que recolheriam para residentes de longa data no Reino Unido (por exemplo, prova de residência, referências profissionais, registo criminal). É importante ter em conta que os outros países terão requisitos legais e regulamentares diferentes no que diz respeito à recolha de informação necessária para gerir a segurança do pessoal e, por isso mesmo, este passo pode ser difícil.

Encontram-se disponíveis várias opções para organizações que desejem levar a cabo controlos estrangeiros:

1. Solicitar documentação ao candidato.
2. Contratar um profissional para um serviço de controlo externo.
3. Conduzir os seus próprios controlos estrangeiros.

Em determinadas circunstâncias, pode não ser capaz de completar os controlos estrangeiros satisfatoriamente (por exemplo, devido à falta de informação por parte de outro país). Neste caso, pode decidir negar o emprego ou implementar outros controlos de gestão dos riscos (por exemplo, supervisão adicional) para compensar a falta de garantia.

Veja a "Lista de Verificação de Boas Práticas – Segurança do Pessoal" no Apêndice E.

12. SEGURANÇA DA INFORMAÇÃO

A perda de confidencialidade, integridade e, mais importante, da disponibilidade de informação em papel ou em formato eletrónico pode ser um problema crítico para as organizações. Muitas dependem dos seus sistemas de informação para realizarem negócios ou levar a cabo funções críticas a nível nacional e para gerir os sistemas de segurança e engenharia.

A sua informação confidencial pode ser do interesse de empresas concorrentes, criminosos, serviços de informação estrangeiros ou terroristas. Podem tentar aceder à sua informação entrando no seu sistema informático, obtendo os dados que descartou ou infiltrando-se na sua organização. Um atentado destes pode perturbar a sua empresa e prejudicar a sua reputação.

Antes de tomar medidas de segurança específicas, deve:

- **Avaliar a ameaça e as suas vulnerabilidades** (Veja "Gestão dos Riscos" na página 6).
- Ter em consideração até que ponto a sua informação está em risco, quem pode querê-la, como pode consegui-la, em que é que a perda ou o roubo da mesma o prejudicarão.
- Ter em consideração boas práticas de segurança da informação para combater atentados eletrónicos e para proteger documentos.

Para aconselhamento geral relativamente à proteção contra atentados eletrónicos visite www.cpni.gov.uk/advice/infosec.

Atentado eletrónico

Os atentados a sistemas eletrónicos podem:

- Permitir que o atacante roube ou modifique informações sensíveis.
- Permitir que o atacante ganhe acesso ao seu sistema informático e faça tudo aquilo que o proprietário da rede pode fazer. Isto pode incluir a modificação de dados, talvez de forma subtil para não ser imediatamente evidente, a instalação de programas informáticos maliciosos (vírus ou *worm*) que podem danificar o seu sistema ou a instalação de dispositivos de *hardware* ou *software* para retransmitir a informação ao atacante. Estes atentados contra sistemas ligados à Internet são extremamente comuns.
- Tornar impossível a utilização dos seus sistemas através de atentados de negação de serviço. Estes são cada vez mais comuns, relativamente simples de lançar e dificilmente evitáveis.

Os atentados eletrónicos são muito mais fáceis de executar quando os sistemas informáticos estão ligados direta ou indiretamente a redes públicas como a Internet.

Os métodos típicos de atentado eletrónico são:

Software Malicioso

As técnicas e os efeitos do *software* malicioso (por exemplo, vírus, *worms*, *Trojans*) são tão variáveis quanto conhecidos. As principais formas de propagação de um vírus são:

- Fazer correr ou executar um ficheiro anexo recebido numa mensagem de correio eletrónico.
- Carregar numa hiperligação para um sítio na Internet recebida num sítio da Internet.
- Navegar na Internet de forma inapropriada, o que muitas vezes leva à distribuição de *software* malicioso por parte de um sítio da Internet.
- Permitir que o pessoal ligue dispositivos de memória removíveis (*pens*, discos, CDs, DVDs) às máquinas da empresa.
- Permitir que o pessoal ligue leitores de música e telemóveis aos computadores da empresa.

Negação de serviço (DoS)

Estes atentados têm como objetivo arrasar o sistema ao inundá-lo com dados indesejados. Alguns destes atentados são distribuídos através de um grande número de máquinas desprotegidas e 'inocentes' (conhecidas como 'zombies') que são recrutadas para preparar os referidos atentados.

Pirataria informática

Esta é uma tentativa de acesso não-autorizado, quase sempre com intenção maliciosa ou criminal. Tem havido atentados sofisticados e ocultos levados a cabo por serviços de informação estrangeiros que procuram informações que têm como alvo os sistemas governamentais, mas outras organizações também podem ser vítimas.

Modificação maliciosa do *hardware*

O *hardware* do computador pode ser modificado para preparar ou permitir um atentado eletrónico. Isto é normalmente realizado antes da instalação, durante o processo de fabrico ou de fornecimento, apesar de também poder ser efetuado durante visitas de manutenção ou por um infiltrado. O objetivo de tais modificações consiste em permitir que possa ser levado a cabo um ataque subsequente, possivelmente através de ativação à distância.

O que fazer

- Adquira os seus sistemas informáticos através de fabricantes e fornecedores reputados.
- Assegure-se de que o seu *software* é atualizado de forma regular. Os fornecedores estão continuamente a corrigir as vulnerabilidades de segurança do *software*. Estas reparações e correções estão disponíveis no sítio da Internet desses fornecedores. Pondere procurar diariamente correções e atualizações.
- Assegure-se de que todos os computadores ligados à Internet estão equipados com *software* anti-vírus e protegidos por uma *firewall*.
- Efetue uma cópia de segurança da informação, de preferência mantendo uma cópia segura noutro local.
- Avalie a fiabilidade daqueles que fazem a manutenção, trabalham com os seus sistemas e os protegem (consulte a secção de "Segurança do Pessoal", na página 30).
- Considere a utilização de pacotes de encriptação para o material que quiser proteger, em particular se este for levado para o exterior – mas, primeiro, procure aconselhamento especializado.
- Tome precauções básicas de segurança para evitar que o *software* ou outra informação delicada caia nas mãos erradas. Incentive o pessoal a estar consciente da segurança, treinando-os para que não deixem material delicado ao acaso e para que levem a cabo uma política de 'secretária limpa' (isto é, as mesas de trabalho devem ficar arrumadas de todo o material no fim de cada sessão de trabalho).
- Assegure-se de que o seu pessoal tem consciência de que os utilizadores podem ser enganados, de forma a revelarem informações que possam ser utilizadas para obter acesso ao sistema, como nomes de utilizador e palavras-passe.
- Invista em armários seguros e em portas com fechadura e assegure-se de que o material delicado é destruído adequadamente.
- Sempre que possível, bloqueie ou desative unidades de disco, portas USB e ligações sem fios.
- Assegure-se de que o acesso aos computadores é protegido ou por palavras-passe individuais controladas e seguras ou por biometria e palavras-passe.
- Implemente uma política de uso aceitável para o pessoal no que diz respeito a navegação na Internet, correio eletrónico, salas de *chat*, redes sociais, sítios de comércio e de *download* de jogos e música.

As organizações podem procurar aconselhamento no sítio do Governo: www.itsafe.gov.uk.

Exemplos de atentados eletrónicos

- Um antigo administrador de sistemas conseguiu intercetar correio eletrónico entre os diretores da empresa, porque o fornecedor de serviços de segurança externo não tornou o sistema seguro.

- Um antigo empregado foi capaz de se ligar remotamente a um sistema e fazer alterações a uma revista especializada em eletrónica, o que levou à perda de confiança por parte dos clientes e acionistas.

Eliminação de informação delicada

As empresas e os indivíduos, por vezes, precisam de se desfazer de informação delicada. Parte do material que é deitado fora pelas empresas de forma rotineira pode ser útil para uma grande variedade de grupos, incluindo empresas concorrentes, ladrões de identidade, criminosos e terroristas.

Os tipos de informação podem variar desde os nomes do pessoal e respetivos endereços e números de telefone a informações sobre o produto, passando por detalhes acerca dos clientes, informação à qual se aplique a Lei de Proteção de Dados, especificações técnicas e dados químicos e biológicos. Sabe-se que os grupos terroristas têm mostrado interesse nas últimas duas áreas.

As principais formas de destruir desperdícios delicados são:

Trituração

Deve ser utilizada uma trituradora de corte transversal para que dois carateres adjacentes não sejam legíveis. Isto produzirá um corte de 15mm x 4mm para um texto com um tamanho de letra 12.

Incineração

A incineração é, provavelmente, a forma mais eficaz de destruir desperdícios delicados, incluindo discos e outras formas de suportes de dados magnéticos e óticos, desde que seja utilizada uma incineradora adequada (consulte a autoridade local). As fogueiras não são seguras, uma vez que o material nem sempre é destruído e os papéis ainda legíveis podem ser espalhados através de correntes ascendentes de ar.

Desfibração

Este processo reduz os desperdícios a um estado fibroso e é eficaz apenas para desperdícios de papel e cartão. Contudo, algumas máquinas de desfibração apenas rasgam o papel em grandes fragmentos e transformam-no num produto de papel maché do qual ainda é possível retirar informação. Este risco é maior atualmente, porque as tintas utilizadas pelas impressoras e fotocopiadoras a *laser* modernas não desbotam quando molhadas.

Há métodos alternativos para a eliminação de suportes de dados eletrónicos, como a reescrita e a desmagnetização. Para mais informações, visite www.cpni.gov.uk.

Antes de investir em equipamento de destruição de desperdícios, deve:

- Se utilizar adjudicatários, assegurar-se de que o equipamento e os procedimentos estão de acordo com as normas. Descubra quem supervisiona o processo, que tipo de equipamento utiliza e se os veículos de recolha dispõem de dois condutores, para que um deles possa ficar no veículo enquanto o outro faz a recolha. Também são desejáveis as comunicações entre o veículo e a base.
- Assegurar-se de que o equipamento pode realizar o trabalho, o que depende do material que deseja destruir, da quantidade implicada e do nível de confidencialidade.
- Assegurar-se de que os procedimentos são seguros, o mesmo acontecendo com o pessoal. Não vale a pena investir em equipamento dispendioso se as pessoas contratadas para o utilizar são elas próprias riscos para a segurança.
- Atribuir a responsabilidade pela destruição de desperdícios delicados ao departamento de segurança e não ao gestor das instalações.

Veja a "Lista de Verificação de Boas Práticas – Segurança da Informação", no Apêndice F.

13. VEÍCULOS COM DISPOSITIVOS EXPLOSIVOS IMPROVISADOS (VBIED)

Os veículos com dispositivos explosivos improvisados (VBIED) são uma das armas mais eficazes no arsenal de um terrorista, uma vez que são capazes de fazer chegar uma grande quantidade de explosivos a um alvo e podem causar grandes danos.

Uma vez montada, a bomba pode ser entregue à hora que o terrorista escolher e com uma precisão razoável, **dependendo das defesas existentes**. Pode ser detonada a uma distância segura através da utilização de um cronómetro ou de um controlo remoto, podendo ainda ser detonada no local por um bombista suicida.

A construção de um VBIED exige investimento de tempo, recursos e conhecimento significativos. Assim, os terroristas procurarão obter o máximo impacto do seu investimento.

Normalmente, os terroristas escolhem alvos em que podem causar mais danos, provocar um elevado número de vítimas ou atrair publicidade generalizada.

Efeitos dos VBIED

Os VBIED podem ser muito destrutivos. Não são apenas os efeitos da explosão imediata de uma bomba que podem ser letais, uma vez que a projeção de destroços, como é o caso de vidros, pode representar um perigo num ponto a muitos metros de distância do local da explosão.

O que pode fazer

Se pensa que o seu hotel ou restaurante pode correr o risco de ser alvo de um atentado por parte de qualquer forma de VBIED, deve:

- Assegurar-se de que tem um controlo eficaz de acessos de veículos, particularmente em áreas onde pode existir um elevado número de vítimas, nas zonas de entrada de mercadorias e nas áreas de serviço. Não permita que veículos não autorizados estacionem em zonas de serviço subterrâneas, diretamente por baixo ou perto de áreas públicas onde possa haver muitas pessoas e onde haja o risco de colapso da estrutura.
- Insistir em que os detalhes dos veículos contratados e a identificação do condutor e de quaisquer passageiros que se aproximem das zonas de mercadorias/serviço sejam autorizados com antecedência.
- Ter em consideração um sistema de buscas em veículos nas zonas de mercadorias/serviço que seja flexível e possa ser alterado em função da ameaça ou do nível de resposta. Pode ser necessário levar a cabo uma avaliação dos riscos para benefício do pessoal de segurança que também possa estar envolvido no controlo de acessos de veículos.
- Fazer o possível para tornar o estabelecimento resistente a explosões, prestando especial atenção às janelas. Quando procurar aconselhamento relativamente a espaços protegidos, assegure-se de que as estruturas são vistoriadas por um engenheiro de segurança/estrutura qualificado.
- Estabelecer e ensaiar simulações de ameaças de bomba e evacuação. Tenha em mente que, dependendo de onde está estacionada a VBIED e do projeto do edifício, os corredores sem janelas ou as caves podem ser mais seguros do que o exterior.
- **Considerar a utilização de barreiras físicas robustas para manter todos os veículos a uma distância segura, excluindo os que estão autorizados. Aconselhe-se junto do CTSA da polícia local sobre o que devem ser estas barreiras e sobre outras medidas que pode tomar, como a vigilância eletrónica, incluindo o ANPR e a proteção contra estilhaços de vidro.**
- As áreas de concentração devem ter em conta a proximidade de uma potencial ameaça. Deve ter em conta que uma viatura armadilhada que entre no edifício – por exemplo, através de zonas de serviço, parques subterrâneos ou através da fachada do estabelecimento – pode ter um efeito muito mais destrutivo na estrutura do que um engenho detonado no exterior.
- **Treinar e ensaiar o pessoal para identificar veículos suspeitos, receber informações e atuar em caso de ameaças de bomba. As informações essenciais e os números de telefone de emergência devem estar bem à vista e prontos a ser utilizados.**
- Deve salientar-se que a instalação de barreiras físicas deve obedecer a requisitos de segurança e não deve ser levada a cabo sem uma análise completa dos regulamentos de planeamento e de avaliação dos riscos de segurança em caso de incêndio.

Veja a "Lista de Verificação de Boas Práticas – Controlo de Acessos", no Apêndice B.

14. ATENTADOS COM SUBSTÂNCIAS QUÍMICAS, BIOLÓGICAS E RADIOLÓGICAS (QBR)

Desde o início dos anos 90 que a preocupação com o facto de os terroristas poderem utilizar materiais QBR como armas tem vindo constantemente a aumentar. Os perigos são:

Químicos

Envenenamento ou ferimentos causados por substâncias químicas, incluindo agentes químicos usados em combate militares e químicos domésticos ou industriais legais mas nocivos.

Biológicos

Doenças causadas pela libertação deliberada de bactérias, vírus ou fungos perigosos ou de toxinas biológicas como a ricina, encontrada em plantas.

Radiológicos

Doenças causadas pela exposição a materiais radioativos nocivos que contaminam o ambiente.

Um engenho de dispersão radiológica, muitas vezes referido como 'bomba suja', é normalmente um engenho em que materiais radioativos são combinados com explosivos convencionais. Quando se dá a detonação, não é produzida uma explosão nuclear, mas, dependendo do tipo de fonte radioativa, as zonas circundantes podem ficar contaminadas.

Para além de provocar feridos na explosão inicial, pode muito bem existir uma ameaça a longo prazo para a saúde. Alguns grupos terroristas mostraram interesse numa 'bomba suja' ou tentaram utilizá-la como método de ataque.

Até à data, grande parte da atividade relacionada com QBR tem sido criminosa ou tem envolvido embustes e falsos alarmes. Poucos exemplos há de terroristas que tenham utilizado materiais QBR. Os mais importantes foram o atentado com gás sarin no metropolitano de Tóquio, em 1995, que matou doze pessoas, e as cartas com antrax nos Estados Unidos, em 2001, que mataram cinco pessoas.

As armas QBR têm sido pouco utilizadas até agora, em grande parte devido à dificuldade na obtenção dos materiais e à complexidade de os utilizar com eficácia. Quando os terroristas tentam levar a cabo atentados QBR, utilizam, em geral, materiais relativamente simples. Contudo, a Al Qaeda e os grupos com ela relacionados manifestaram um sério interesse na utilização de materiais QBR. O impacto de qualquer atentado terrorista QBR dependerá, em grande parte, do sucesso do método de disseminação escolhido e das condições atmosféricas na altura do atentado.

A probabilidade de um atentado QBR continua a ser baixa. Como com outros atentados terroristas, o seu hotel ou restaurante pode não receber um aviso prévio relativamente a um incidente QBR. Além disso, a natureza exata de um incidente pode não ser imediatamente óbvia. Os primeiros indicadores podem ser o aparecimento súbito de pós, líquidos ou odores estranhos no interior do edifício, com ou sem efeito imediato nas pessoas.

As boas medidas gerais de segurança física e do pessoal contribuirão para a resiliência contra os incidentes QBR. Lembre-se de aplicar as normas de segurança do pessoal apropriadas aos adjudicatários, em especial àqueles que têm acesso frequente ao local.

O que pode fazer

- Reveja a segurança física dos sistemas de sistemas de tratamento de ar, como os acessos às entradas e saídas.
- Melhore os filtros de ar ou atualize os sistemas de tratamento de ar conforme seja necessário.
- Restrinja o acesso aos tanques de água e a outros serviços-chave.
- Reveja a segurança das cadeias de fornecimento de alimentação e bebidas.
- Pense se precisa ou não de tomar providências especiais para correspondência e encomendas, por exemplo, salas de correio independentes, possivelmente com circulação de ar exclusiva ou até Infraestruturas especializadas fora do local. (Veja "Tratamento de Correspondência", na página 20).
- **O Ministério da Administração Interna (*Home Office*) recomenda que as organizações não utilizem as tecnologias de deteção de QBR como parte das suas medidas de contingência no presente, isto porque a tecnologia ainda não está comprovada no contexto civil e, em caso de um incidente QBR, os serviços de emergência entrariam em cena com detetores apropriados e aconselhariam em conformidade.** Uma consciência básica das ameaças e dos perigos de QBR, combinada com medidas de segurança gerais (por exemplo, controlo de visitantes, monitorização por CCTV do perímetro e das áreas de entrada, estado de alerta relativamente a correspondência e pacotes suspeitos), deve oferecer um bom nível de resiliência. Em primeiro lugar, procure o aconselhamento do CTSA da força policial local.
- Se tiver um local protegido designado, este também pode ser adequado como abrigo QBR, mas procure o aconselhamento especializado do CTSA da força policial local antes de fazer planos para o utilizar como tal.
- Pondere sobre a forma de fazer chegar ao pessoal o aconselhamento de segurança e de oferecer garantias. Nisto têm que estar incluídas instruções para aqueles que queiram entrar no edifício, bem como aqueles que de lá queiram sair ou que pretendam regressar ao mesmo.

15. ATENTADOS SUICIDAS

A utilização de bombistas suicidas é um método muito eficaz para a entrega de um engenho explosivo num local específico. Os bombistas suicidas podem utilizar um camião, um avião ou outro tipo de veículo como bomba, podendo também transportar ou esconder explosivos no seu próprio corpo. Ambos os tipos de atentado são, normalmente, perpetrados sem aviso. Os alvos mais prováveis são os locais de grande afluência de pessoas, lugares que sejam considerados simbólicos e instalações importantes onde pode ocorrer um elevado número de vítimas.

Quando considerar medidas de proteção contra bombistas suicidas, pense em:

- Utilizar barreiras físicas para evitar que um veículo hostil entre no hotel ou restaurante através das entradas principais, das entradas de mercadorias/serviços, das entradas para peões ou dos espaços abertos.
- Negar acesso a qualquer veículo que chegue às entradas de mercadorias/serviços sem aviso prévio e reter veículos nos pontos de controlo de acessos ao hotel ou restaurante até ter a certeza de que são verdadeiros.
- Sempre que possível, estabelecer o ponto de controlo de acessos de veículos distante do local protegido, implementando patrulhas regulares e instruindo o pessoal para que vigie alguém com um comportamento suspeito. Muitos ataques bombistas são precedidos por reconhecimento ou ensaios. Assegure-se de que tais incidentes são denunciados à polícia.
- Assegurar-se de que ninguém visita a área protegida sem que a identidade seja verificada ou sem que seja concedida a devida autorização de entrada. Procure mais aconselhamento junto do CTSA da força policial local.
- Utilizar sistemas de CCTV eficazes que possam impedir um atentado terrorista ou até mesmo identificar atividades ainda em planeamento. Imagens com boa qualidade podem ser uma prova crucial em tribunal.

Não há um perfil físico definido para um bombista suicida; por isso, mantenha-se atento e denuncie qualquer suspeito à polícia.

Veja “Reconhecimento Hostil” – página 48.

16. ATENTADOS COM INSTRUMENTOS DE ATAQUE E ARMAS DE FOGO

Os atentados com instrumentos de ataque e armas de fogo ainda são pouco frequentes, mas é importante estar preparado para lidar com um incidente destes.

O aconselhamento importante que se segue ajudá-lo-á a planear as medidas necessárias.

No caso de um atentado, tome estas quatro medidas:

Mantenha-se seguro

- Sob FOGO ARMADO imediato – Abrigue-se inicialmente, mas abandone a área assim que possível se tal for seguro
- Na iminência de FOGO ARMADO – Abandone imediatamente a área, se tal for possível e seguro.
- Deixe ficar os seus pertences.
- Não reúna as pessoas nos pontos de evacuação.

ABRIGAR-SE DO FOGO ARMADO	ABRIGAR-SE DA VISTA
Paredes de alvenaria ou betão	Paredes divisórias internas
Blocos de motor	Portas de automóveis
Base do tronco de árvores vivas de grande porte	Vedações de madeira
Encostas/colinas/montículos	Cortinas

LEMBRE-SE – longe da vista não quer, necessariamente, dizer fora de perigo, em especial se não se 'abrigar do fogo armado'.

SE NÃO PUDER FUGIR – pondere trancar-se juntamente com as restantes pessoas num quarto ou num armário. Barrique a porta e, depois, mantenha-se afastado dela.

Se for possível, escolha um quarto de onde seja possível fugir ou que permita outras movimentações. Silencie todas as formas de ruído, como telemóveis, que possam revelar a sua presença.

Veja

Quanto mais informação passar à polícia melhor, mas NUNCA ponha em risco a sua própria segurança ou a de outros para conseguir manter-se seguro. Quando possível, pondere a utilização de CCTV e de outros métodos de controlo remotos para reduzir os riscos. Se for seguro, tenha em consideração o seguinte:

- Trata-se de um incidente com armas de fogo/outras armas? • Localização exata do incidente.
- O que mais transportam os terroristas? • Número e descrição dos homens armados.
- Movem-se numa direção específica? • Tipo de arma de fogo – de cano longo ou pistola.
- Comunicam com outros? • Número de feridos/pessoas na área.

Contacte

- Contacte a **POLÍCIA** imediatamente, ligando o 112 ou através da sala de controlo, dando-lhe a informação presente em 'Veja'.
- Utilize todos os **canais de comunicação** à disposição para informar do perigo o pessoal, os visitantes, os estabelecimentos vizinhos e outros.

Controle

- Proteja os espaços em redor e outras áreas vulneráveis.
- Mantenha as pessoas longe das áreas públicas, como corredores e áreas de receção.
- Afaste-se da porta e mantenha-se silencioso até lhe ser dito o contrário pelas autoridades competentes ou se precisar de se mover por razões de segurança, como um incêndio no edifício.

Polícia armada

Na eventualidade de um atentado que envolva instrumentos de ataque ou armas de fogo, a prioridade de um agente policial é proteger e salvar vidas. Por favor, lembre-se:

- Inicialmente, os agentes policiais podem não ser capazes de o distinguir dos homens armados.
- Os agentes podem estar armados e apontar-lhe uma arma.
- Podem ter de lidar com o público com firmeza. Siga as instruções dos agentes, mantenha as mãos no ar/à vista.
- Não realize movimentos bruscos em direção aos agentes e evite apontar, gritar ou berrar.

Planeie

Considere os pontos seguintes quando fizer o planeamento relativamente a um incidente com instrumentos de ataque /armas de fogo:

1. Como comunicaria com o pessoal, visitantes, estabelecimentos vizinhos, etc.
2. Que informações importantes lhes passaria de modo a mantê-los seguros.
3. Tente proteger partes-chave do edifício para impedir as movimentações livres dos homens armados.
4. Pense em incluir isto no planeamento e nas instruções de emergência.
5. Teste o plano pelo menos uma vez por ano.

Se necessitar de mais informações, por favor contacte o CTSA.

17. COMUNICAÇÕES

Deve implementar uma estratégia de comunicação para sensibilizar o pessoal e outros que precisem de conhecer o seu plano de segurança e a respetiva execução. Isto incluirá os serviços de emergência, as autoridades locais e, possivelmente, os estabelecimentos vizinhos.

Deverá haver igualmente acordos para lidar com pessoas que possam ser afetadas pela operação de segurança, mas que não sejam empregados da organização (por exemplo, compradores, clientes, adjudicatários, visitantes).

Recorde-se de que, imediatamente após um atentado terrorista, a comunicação por telemóvel poderá estar indisponível devido a uma sobrecarga das redes.

As questões com a segurança devem ser discutidas e determinadas ao nível da administração e fazer parte da cultura da organização.

Os gestores de segurança devem encontrar-se regularmente com o pessoal para discutir problemas com a segurança e encorajar o pessoal a apresentar as suas preocupações relativamente à mesma.

Deve considerar-se a utilização do sítio Web do hotel ou restaurante e/ou publicações para comunicar iniciativas sobre prevenção da criminalidade e sobre antiterrorismo.

Todos os hotéis e restaurantes devem ponderar ter uma reserva de cartazes e material (inclusive através de ligações da Internet) para apoiar a prevenção do crime, mensagens e iniciativas contra o terrorismo.

Todos os gestores de segurança devem envolver o CTSA da polícia local quando pensarem na realização de melhorias no hotel ou restaurante.

Veja a “Lista de Verificação de Boas Práticas – Comunicações”, no Apêndice G.

18. RECONHECIMENTO HOSTIL

A *Operation Lighting* é uma operação nacional de recolha de informações para registar, pesquisar, investigar e analisar:

- Observações suspeitas.
- Atividade suspeita.

em ou perto de:

- Locais de grande afluência

ou em locais proeminentes ou vulneráveis:

- Edifícios,
- Estruturas,
- Infraestruturas de transportes

A capacidade para reconhecer os envolvidos no reconhecimento hostil pode evitar um atentado e dar origem a importantes orientações para recolha de informações.

Papel Principal do Reconhecimento:

- Obter um perfil da localização do alvo.
- Determinar o melhor método de ataque.
- Determinar o tempo ideal para realizar o ataque.

O reconhecimento hostil é utilizado para providenciar aos responsáveis operacionais informações sobre alvos potenciais durante a fase preparatória e a fase operacional das operações terroristas.

Os agentes de reconhecimento podem visitar os alvos potenciais várias vezes antes do atentado. Quando há medidas de segurança proactivas, é dada particular atenção a qualquer variação nos padrões de segurança e no fluxo de pessoas a entrar e a sair.

O que procurar

As observações ou atividades seguintes podem ser particularmente relevantes para hotéis e restaurantes.

- Interesse significativo pelo exterior do hotel ou restaurante, incluindo zonas de estacionamento, portões de entrega de mercadorias, portas e entradas e estacionamentos subterrâneos.
- Grupos ou indivíduos que mostrem especial interesse na localização das câmaras de CCTV e nas áreas controladas.
- Pessoas a tirar fotografias, a filmar, a tirar notas ou a fazer esboços das medidas de segurança nas imediações do hotel ou restaurante. Os turistas não devem necessariamente ser considerados terroristas e devem ser tratados com sensibilidade, ainda que com precaução.
- Fotografia evidente/dissimulada, câmaras de vídeo, posse de fotografias, mapas, plantas, etc., de Infraestruturas críticas, transformadores de eletricidade, condutas de gás, cabos telefónicos, etc.
- Posse de mapas, de sistemas de posicionamento global (GPS) e de equipamento fotográfico (máquinas fotográficas, lentes de *zoom*, câmaras de

vídeo). O GPS ajudará no posicionamento e na orientação correta de armas como morteiros e granadas-foguete. Deve ser considerada esta possibilidade até um quilómetro de distância de qualquer alvo.

- Veículos estacionados no exterior de edifícios de outras instalações, com um ou mais indivíduos que permaneçam na viatura por mais tempo do que aquele que seria considerado normal.
- Estacionar, permanecer de pé ou vaguear na mesma área diversas vezes sem explicação razoável aparente.
- Vigilância estática prolongada, realizada por responsáveis disfarçados de manifestantes, varredores de rua, etc., ou que parem ou pareçam estar com problemas no automóvel para testar o tempo de resposta dos serviços de emergência, das companhias de reboque de viaturas ou do pessoal local.
- Observação simples, como olhar fixamente ou desviar o olhar rapidamente.
- Atividade inconsistente com a natureza do edifício.
- Questões não habituais – número de funcionários e rotina dos mesmos/*VIP*s que residem no local.
- Indivíduos que pareçam deslocados por qualquer razão.
- Indivíduos que pareçam vaguear pelas áreas públicas.
- Indivíduos que coloquem questões sobre a identidade ou as características de hóspedes específicos, grupos de hóspedes, atividades ou nacionalidades de hóspedes que frequentam o hotel.
- Pessoas que façam perguntas sobre as medidas de segurança e evacuação.
- Pessoas que façam perguntas sobre os pontos de encontro do pessoal.
- Pessoas que façam perguntas sobre os visitantes *VIP*.
- Veículos de entregas em frente ao hotel ou restaurante.
- Veículos, embalagens e bagagem abandonados.
- Veículos que pareçam ter excesso de peso.
- Pessoas que pareçam estar a contar os peões/veículos.
- Estranhos que circulem em redor do perímetro do hotel ou restaurante.
- Pessoas que ‘namorem’ bebidas e prestem demasiada atenção às imediações.
- Pessoas a vaguear pela área durante muito tempo.
- Pessoas que tentem aceder à maquinaria da piscina ou a equipamento nas áreas dos produtos químicos da piscina.
- Veículos de entregas ou outros camiões que tentem aceder à entrada principal do hotel ou restaurante.
- Veículos de entregas que cheguem ao hotel ou restaurante a horas fora do habitual.
- Veículos que emitam odores suspeitos, por exemplo, a combustível ou a gás.
- Veículos de entregas que entrem à hora errada.
- Veículos que pareçam deslocados do contexto.
- Condução irregular.
- Perguntas relativamente à estrutura do hotel ou restaurante.
- Padrão conhecido ou série de falsos alarmes que indiciam um possível teste aos sistemas de segurança e observação do comportamento e dos procedimentos de resposta (ameaças de bomba, através do abandono de dispositivos ou embalagens dissimuladas).
- O regresso a um local (locais) do mesmo veículo e indivíduos diferentes ou dos mesmos indivíduos num veículo diferente
- Atividade não habitual por parte dos veículos dos adjudicatários.

- Danos recentes ao perímetro de segurança, brechas em vedações ou paredes, utilização de locais para esconder placas de base de morteiros ou de equipamento que possa ser usado em atos terroristas, como, por exemplo, cordas, escadas, comida, etc. O patrulhamento regular ao perímetro deve ser iniciado com meses de antecedência relativamente a um evento importante para assegurar que estas situações não acontecem.
- Tentativas de disfarce da identidade – capacetes de motociclos, capuzes, etc., ou vários conjuntos de roupa para mudar de aparência.
- Utilização constante de caminhos e/ou de rotas de acesso diferentes para chegar a um local. 'Aprender a rota' ou vigilância a pé que envolva um número de pessoas que pareçam não ter qualquer ligação, mas que estão a trabalhar em conjunto.
- Múltiplos documentos de identificação – documentos suspeitos, contrafeitos, alterados, etc.
- Ausência de cooperação com a polícia ou com o pessoal de segurança.
- Quem estiver empenhado no reconhecimento tentará várias vezes entrar no estabelecimento para aceder à disposição interna e, ao fazê-lo, modificará a sua aparência e fornecerá histórias inventadas.
- No passado, alguns operacionais de reconhecimento chamaram a atenção sobre si próprios ao colocarem questões peculiares e aprofundadas acerca dos empregados e de outros indivíduos mais familiarizados com o local.
- A observação de atividades suspeitas deve ser comunicada de imediato ao gestor de segurança, para controlo da situação através de CCTV e gravação do evento para efeitos de prova.

Os operacionais de reconhecimento também podem procurar informação adicional através de:

- Pesquisa da largura das ruas adjacentes – explorando a variedade de opções táticas disponíveis para a entrega do dispositivo.
- Níveis de segurança interna e externa – são levadas a cabo buscas a veículos/pessoas/malas?

O PAPEL DA EQUIPA DE RECONHECIMENTO TEM VINDO A TORNAR-SE CADA VEZ MAIS IMPORTANTE NAS OPERAÇÕES TERRORISTAS.

As viagens de reconhecimento devem ser levadas a cabo como um ensaio para envolver o pessoal e o equipamento que será utilizado no atentado propriamente dito; por exemplo, antes dos atentados de Londres no dia 7 de julho de 2005, os bombistas tinham feito um ensaio nove dias antes do atentado.

Para reportar à polícia atividade suspeita que não requeira uma resposta imediata, contacte a *ANTI-TERRORIST HOTLINE* (LINHA DIRETA ANTITERRORISTA) – 0800 789 321.

QUALQUER INCIDENTE QUE EXIJA UMA RESPOSTA IMEDIATA – MARQUE 112.

19. EVENTOS DE GRANDE VISIBILIDADE

Pode haver eventos que, por variadas razões, são considerados de maior visibilidade do que as operações do dia-a-dia. Isto pode envolver pré-eventos publicitários da presença de um *VIP* ou de uma celebridade, o que resulta em mais público no dia do evento, na necessidade de uma resposta de segurança apropriada e no aumento da vigilância.

Em certos casos, a polícia local pode nomear um *Gold Commander* (*Strategic Commander* na Escócia) responsável pelo evento, o qual pode, por sua vez, nomear um *Police Security Co-ordinator* (SECCO) e/ou um POLSA.

Police Security Co-ordinator (SECCO)

O SECCO tem um papel único no planeamento e coordenação de medidas de segurança em eventos de grande visibilidade.

Trabalha de acordo com a estratégia estabelecida pelo *Police Gold/Strategic Commander* e age como conselheiro e coordenador das questões de segurança.

Estão à disponibilidade do SECCO variados recursos e opções, que incluem a comunicar com a gerência do hotel ou restaurante, identificar os indivíduos, as agências e os departamentos mais importantes envolvidos no evento, bem como procurar aconselhamento do CTSA relevante.

O SECCO fornecerá ao *Gold/Strategic Commander* uma série de observações e recomendações para assegurar que a resposta em termos de segurança é realista e adequada.

Police Search Adviser (POLSA)

O SECCO pode considerar necessário nomear um POLSA para um evento de grande visibilidade.

O POLSA procederá à avaliação do local e da natureza do evento, tomando em consideração uma avaliação atualizada da ameaça e outras questões de segurança.

O SECCO submeterá ao *Gold/Strategic Commander* um relatório em que se incluem a avaliação, recomendações e subsequente plano de buscas subsequente.

20. NÍVEIS DE AMEAÇA

Desde 1 de agosto de 2006 que está disponível informação acerca do nível de ameaça nacional nos sítios da Internet dos Serviços de Segurança, Ministério da Administração Interna e dos *Intelligence Community Websites* do Reino Unido.

Os níveis de ameaça do terrorismo fornecer indicações gerais sobre a probabilidade de um atentado terrorista. Baseiam-se na avaliação de um conjunto de fatores, incluindo informação atual, eventos recentes e o que se sabe acerca das intenções e das capacidades dos terroristas. Esta informação pode estar incompleta e as decisões sobre a resposta de segurança apropriada devem ser tomadas tendo este facto presente.

Em particular, aqueles que possuem ou administram hotéis e restaurantes, bem como os que aí operam ou trabalham devem lembrar-se de que quer SUBSTANCIAL quer GRAVE indicam um nível elevado de ameaça e de que um atentado pode acontecer sem aviso.

Definições dos Níveis de Ameaça

CRÍTICO	**UM ATENTADO ESTÁ IMINENTE**
GRAVE	**É ALTAMENTE PROVÁVEL QUE ACONTEÇA UM ATENTADO**
SUBSTANCIAL	**EXISTE A FORTE POSSIBILIDADE DE UM ATENTADO**
MODERADO	**É POSSÍVEL, MAS NÃO PROVÁVEL, QUE EXISTA UM ATENTADO**
BAIXO	**É IMPROVÁVEL QUE EXISTA UM ATENTADO**

Níveis de Resposta

Os níveis de resposta dão uma indicação vasta sobre as medidas de segurança que devem ser aplicadas num momento específico. São atualizados a partir do nível de ameaça, mas também têm em conta avaliações específicas das vulnerabilidades e dos riscos.

Os níveis de resposta tendem a estar relacionados com locais, enquanto os níveis de ameaça costumam estar relacionados com as amplas áreas de atividade.

Há uma variedade de medidas de segurança específicas para locais que podem ser aplicadas no que diz respeito aos níveis de resposta, embora as mesmas medidas possam não se aplicam a todos os locais.

As medidas de segurança implementadas em níveis de resposta diferentes não devem ser tornadas públicos, para evitar informar os terroristas acerca do que sabemos e do que estamos a fazer relativamente a isso.

Há três níveis de resposta que, em traços gerais, igualam os níveis de ameaça, como se mostra de seguida:

CRÍTICO	**EXCECIONAL**
GRAVE	**ELEVADO**
SUBSTANCIAL	
MODERADO	**NORMAL**
BAIXO	

Definições dos Níveis de Resposta

NÍVEL DE RESPOSTA	DESCRIÇÃO
NORMAL	Medidas de segurança rotineiras, adequadas à sua empresa e à sua localização.
ELEVADO	Medidas de segurança adicionais e sustentáveis que reflitam a amplitude da ameaça combinada com a especificidade da atividade e vulnerabilidades geográficas, e avaliação do risco aceitável.
EXCECIONAL	Medidas de segurança máxima que vão ao encontro de ameaças específicas e pretendem minimizar a vulnerabilidade e o risco.

O que posso fazer agora?

- **Levar a cabo uma avaliação do risco e da vulnerabilidade que seja específica para o seu hotel ou restaurante.**
- **Identificar um conjunto de medidas de segurança práticas apropriadas para cada um dos níveis de resposta. O seu CTSA pode ajudá-lo nisto.**
- **Utilizar as listas de verificação de boas práticas nas páginas seguintes, que o ajudam na tomada de decisões.**

As contra-medidas a ser implementadas em cada nível de resposta são da competência dos estabelecimentos individuais e das organizações, diferindo de acordo com uma variedade de circunstâncias.

Todas as medidas de segurança devem ser identificadas antes de qualquer mudança nos níveis de ameaça e resposta e devem ser comunicadas com clareza ao pessoal responsável pelo seu cumprimento.

LISTAS DE VERIFICAÇÃO DE BOAS PRÁTICAS

As listas de verificação que se seguem pretendem ser um guia para aqueles que possuem, operam ou gerem hotéis e restaurantes, bem como aqueles que aí trabalham, de forma a ajudá-los na identificação de perigos e riscos associados ao planeamento antiterrorismo.

Contudo, não são exaustivas e parte das orientações pode não ser relevante para todos os hotéis e restaurantes.

As listas de verificação devem ser consideradas tendo em conta os seguintes fatores:

- Alguma vez consultou o CTSA da polícia, as autoridades locais e os bombeiros e/ou a Proteção Civil locais?
- Quem mais deverá estar incluído na consulta aos serviços?
- Que medidas podem ser facilmente implementadas?
- Que medidas necessitarão de mais planeamento e investimento?

APÊNDICE A

Boas Práticas de Gestão Interna

	Sim	Não	Não sabe
Reviu a utilização e localização de todos os contentores de desperdícios no interior e à volta do hotel ou restaurante, tendo em consideração o seu tamanho e a sua proximidade de superfícies envidraçadas e de estruturas de suporte do edifício?			
Mantém limpas e arrumadas as áreas exteriores, as entradas, as saídas, as escadas, as áreas de receção e as casas-de-banho?			
Mantém o mobiliário reduzido ao mínimo para reduzir as oportunidades de ocultação de dispositivos, incluindo debaixo de cadeiras e sofás?			
Os escritórios, as salas de reuniões e as salas de trabalho estão fechados à chave?			
Utiliza selos/fechaduras para proteger escotilhas de manutenção, compactadores e caixotes do lixo industriais quando a sua utilização imediata não é necessária?			
Verifica todo o correio e pode isolar a área de tratamento da correspondência?			
O pessoal da receção e os vigilantes estão treinados e têm competência para lidar com ameaças telefónicas de bomba?			
Ponderou marcar o equipamento de primeiros-socorros e de combate a incêndios como propriedade do hotel e certificou-se de que não foi substituído?			

APÊNDICE B

Controlo de Acessos a Hotéis e Restaurantes

	Sim	Não	Não sabe
Evita a entrada de todos os veículos nas zonas de mercadorias e de serviço imediatamente abaixo, acima ou perto de zonas pedestres onde haja muitas pessoas até que esses veículos estejam autorizados pela segurança?			
Há barreiras físicas instaladas para manter todos os veículos exceto os autorizados a uma distância segura e para mitigar um possível atentado hostil com utilização de veículos			
Há uma demarcação bem visível entre as áreas públicas e as áreas restritas do hotel ou restaurante?			
O pessoal, incluindo adjudicatários, pessoal de limpeza e outros empregados, utiliza cartões de identificação sempre que está no estabelecimento?			
Adota uma 'cultura de interpelação' para qualquer pessoa que não utilize um passe nas áreas restritas?			
Insiste em que os dados dos veículos contratados e a identidade do condutor e de outros passageiros que requeiram permissão para estacionar ou trabalhar no hotel ou restaurante sejam autorizados com antecedência?			
Exige dados dos condutores e dos veículos de recolha de resíduos com antecedência?			

APÊNDICE C

CCTV

	Sim	Não	Não sabe
Monitoriza constantemente as imagens de CCTV ou reproduz as gravações noturnas à procura de provas de atividade suspeita?			
As câmaras de CCTV são alvo de manutenção regularmente?			
As câmaras de CCTV cobrem as entradas e saídas do hotel ou restaurante?			
Considerou a introdução de um sistema de leitura automática de matrículas como complemento da operação de segurança?			
Tem câmaras de CCTV a abranger áreas críticas da empresa, como salas de servidores, geradores de apoio, caixas registadoras e corredores das traseiras?			
Guarda as imagens de CCTV de acordo com as necessidades de prova da polícia?			
Conseguiria identificar com certeza um indivíduo através das imagens gravadas no seu sistema de CCTV?			
Os registos de data e hora do sistema estão corretos e sincronizados?			
O sistema de iluminação complementa o sistema de CCTV durante o dia e durante a noite?			
Verifica regularmente a qualidade das gravações?			
Os operadores de CCTV contratados são creditados pela SIA?			
Implementou procedimentos operacionais, códigos de conduta e pistas de auditoria?			
Cada câmara de CCTV está a desempenhar as funções para as quais foi instalada?			

APÊNDICE D

Buscas

	Sim	Não	Não sabe
Realiza buscas sectorizadas, sistemáticas e minuciosas ao seu hotel ou restaurante como parte da gestão interna rotineira e como resposta a um incidente específico?			
O seu plano de buscas tem uma lista de verificação escrita, assinada pelo responsável das buscas e considerada completa, para informação do gestor de segurança?			
O plano de buscas inclui fachada, casas-de-banho, elevadores, corredores das traseiras, parques de estacionamento e zonas de serviço?			
Ponderou um regime de buscas a veículos nas entradas de mercadorias/serviço que seja flexível e possa ser adaptado caso se verifique uma alteração no nível de ameaça ou de resposta?			
Leva a cabo buscas explícitas aleatórias a veículos como fator de dissuasão visual?			
Tem um plano de contingência para um sistema de buscas a hóspedes que seja flexível e possa ser adaptado a e implementado num evento de grande visibilidade ou caso exista uma alteração no nível de ameaça ou de resposta?			
Utiliza o seu sítio da Internet ou publicações para informar os adjudicatários e visitantes sobre as suas políticas de buscas, assim como para transmitir as mensagens de prevenção do crime e do terrorismo?			
Tem uma política de recusa de entrada a qualquer veículo cujo condutor se negue a permitir uma busca?			
O pessoal de buscas está treinado e devidamente informado acerca dos seus poderes e daquilo que devem procurar?			
O pessoal está treinado para lidar eficazmente com embalagens não identificadas encontradas no estabelecimento?			
Tem pessoal suficiente para buscas eficazes?			
Faz buscas às rotas de evacuação e às áreas de concentração antes de estas serem utilizadas?			

APÊNDICE E

Segurança do Pessoal

	Sim	Não	Não sabe
Durante a seleção do pessoal **deverá exigir** os seguintes dados:			
Nome completo			
Morada atual e todas as moradas anteriores dos últimos cinco anos			
Data de nascimento			
Número de Segurança Social			
Detalhes completos das referências (nomes, moradas e detalhes de contacto)			
Detalhes completos de antigos empregadores, incluindo datas de emprego			
Comprovativo das habilitações académicas e profissionais relevantes			
Comprovativo de autorização de trabalho no Reino Unido para cidadãos que não sejam britânicos ou que não pertençam ao Espaço Económico Europeu (EEE)			
Pede aos cidadãos britânicos os seguintes documentos?			
Passaporte completo (atualizado) válido por um mínimo de 10 anos			
Carta de condução britânica (idealmente com fotografia)			
P45[13]			
Certidão de Nascimento – emitida no prazo de seis semanas após o nascimento			
Cartão de crédito – com três extratos e prova de assinatura			
Livro de cheques e cartão bancário – com três extratos e prova de assinatura			
Comprovativo de residência – fatura do IMI, do gás, da eletricidade, da água ou do telefone			
Cidadãos do EEE:			
Passaporte completo do EEE			
Bilhete de Identidade Nacional			
Outros Cidadãos:			
Passaporte completo e um documento do MAI que confirme o estatuto de imigrante do indivíduo e a autorização para trabalhar no Reino Unido			

[13] Código de referência de um formulário com quatro partes intitulado *Details of employee leaving work*, relativamente a cessação de contrato e que deve ser entregue pela entidade empregadora. (https://www.gov.uk/paye-forms-p45-p46-p60-p11d - consultado a 8/4/2013)

APÊNDICE F

Segurança da Informação

	Sim	Não	Não sabe
Guarda em segurança todos os documentos comerciais no final do dia?			
Tem uma política de "secretária limpa" fora das horas de trabalho?			
Desliga todos os computadores no final do dia?			
Todos os computadores estão protegidos por palavra-passe?			
Tem *firewall* e *software* anti-vírus nos sistemas informáticos?			
Atualiza regularmente esta proteção?			
Pensou num pacote de encriptação para informações confidenciais que deseje proteger?			
Destrói devidamente os dados confidenciais quando já não são necessários?			
Cria regularmente cópias de segurança das informações fundamentais da sua empresa?			
Possui cópias de segurança protegidas num local diferente daquele onde gere a sua empresa? (Procedimento de segurança)			
Investiu em armários seguros para o seu equipamento informático?			

APÊNDICE G

Comunicações

	Sim	Não	Não sabe
As questões de segurança são discutidas ao nível da administração e fazem parte da cultura da organização?			
Tem uma política de segurança ou outra documentação que mostre como é que os procedimentos de segurança devem funcionar na sua empresa?			
Esta documentação é revista regularmente e, se necessário, atualizada?			
Possui um plano de gestão de crise que seja atualizado regularmente e o pessoal envolvido está ciente das suas funções e das suas responsabilidades?			
Encontra-se regularmente com o pessoal e discute as questões de segurança?			
Encoraja o pessoal a expor as suas preocupações relativamente à segurança?			
Conhece o CTSA local e envolve-o em todos os desenvolvimentos relativamente ao seu estabelecimento ou à segurança?			
Fala com as empresas vizinhas acerca de questões de segurança e de crime que vos possam afetar?			
Lembra o pessoal que deve estar atento quando viajar entre a casa e o emprego e de informar as autoridades relevantes ou a polícia acerca de algo suspeito?			
Utiliza o sítio da Internet para comunicar iniciativas relativamente ao crime e ao antiterrorismo, incluindo o aviso prévio de buscas?			

Resultados da Listas de Verificação

Depois de completar as várias listas de verificação de 'Boas Práticas', tem de prestar mais atenção às perguntas às quais respondeu 'Não' ou 'Não sabe'.

Se respondeu 'Não sabe' a uma pergunta, procure saber mais sobre essa questão em particular para se certificar de que essa vulnerabilidade está a ser tratada ou precisa de ser tratada.

Se respondeu 'Não' a alguma pergunta, deve procurar tratar dessa questão específica o mais rapidamente possível.

Se respondeu 'Sim' a uma pergunta, lembre-se de rever regularmente as necessidades de segurança para assegurar que as medidas de segurança estão ajustadas a essa finalidade.

LISTA DE VERIFICAÇÃO DE AMEAÇAS DE BOMBA

Esta lista de verificação foi elaborada para ajudar o pessoal a lidar com uma ameaça telefónica de bomba e a registar a informação necessária.

Visite www.cpni.gov.uk para descarregar um PDF e imprimi-lo.

Medidas tomadas após a receção de uma ameaça de bomba:

Ligar o gravador de voz/*voicemail* (se conectado)
Dizer ao autor da chamada de que cidade/zona está a responder
Registar o texto exato da ameaça: _____

Faça as seguintes perguntas:

Onde está a bomba agora? _____
Quando é que vai explodir? _____
Qual é a aparência da bomba? _____
Que tipo de bomba é? _____
O que a fará explodir? _____
Foi você quem colocou a bomba? _____
Porquê? _____
Como se chama? _____
Qual é a sua morada? _____
Qual é o seu número de telefone? _____
(Registe a hora a que a chamada terminou:)
Onde exista equipamento que mostre automaticamente o número, registe o número mostrado: _____
Informe o gerente do estabelecimento do nome e do número de telefone da pessoa informada: _____
Contacte a polícia através do 112. Hora da informação: _____

A parte seguinte deve ser preenchida assim que o autor da chamada tenha desligado e o gerente do estabelecimento tenha sido informado.

Hora e data da chamada: _____
Duração da chamada: _____
Número em que a chamada foi recebida (i.e. número da sua extensão): _____

ACERCA DO AUTOR DA CHAMADA
Sexo: _____
Nacionalidade: _____
Idade: _____

TIPO DE LINGUAGEM DA AMEAÇA (assinalar)
☐ Bem-falante?
☐ Irracional?
☐ Mensagem gravada?
☐ Ofensiva?
☐ Incoerente?
☐ Mensagem lida pelo perpetrador?

VOZ DO AUTOR DA CHAMADA (assinalar)
☐ Calma?
☐ A chorar?
☐ A pigarrear?
☐ Irritada?
☐ Nasalada?
☐ Pouco clara?
☐ Excitada?
☐ A gaguejar?
☐ Disfarçada?
☐ Lenta?
☐ Com ceceio?
☐ Com sotaque? Se sim, de que tipo? _____
☐ Rápida?
☐ Profunda?
☐ Rouca?
☐ Risonha?
☐ Familiar? Se sim, com que voz se parecia? _____

SONS DE FUNDO (assinalar)
☐ Ruídos de rua?
☐ Ruídos de casa?
☐ Ruídos de animais?
☐ Loiça?
☐ Motor?
☐ Límpido?
☐ Vozes?
☐ Estático?
☐ Sistema de comunicação pública?
☐ Cabine telefónica?
☐ Música?
☐ Equipamento fabril?
☐ Equipamento de escritório?
☐ Outro? (especificar) _____

OUTRAS OBSERVAÇÕES _____

Assinatura _____
Data _____
Nome _____

PUBLICAÇÕES E CONTACTOS ÚTEIS

Publicações

Protecting Against Terrorism (3ª Edição)

Esta brochura de 52 páginas fornece conselhos gerais relativamente à segurança do CPNI. É dirigida a empresas e outras organizações que procurem reduzir o risco de um atentado terrorista ou limitar os danos que o terrorismo pode causar.

A brochura está disponível em formato PDF e pode ser descarregada em www.cpni.gov.uk ou pode ainda pedir uma cópia enviando uma mensagem para enquiries@cpni.gsi.gov.uk.

Personnel Security: Threats, Challenges and Measures

Esta brochura foi desenvolvida pelo CPNI. Resume as várias atividades que constituem um sistema de segurança do pessoal. Como tal, fornece uma referência introdutória para gestores de segurança e gestores de recursos humanos que estejam a desenvolver ou a rever a sua abordagem à segurança do pessoal.

A brochura está disponível em formato PDF e pode ser descarregada em www.cpni.gov.uk.

Risk Assessment for Personnel Security

A avaliação da segurança do pessoal foca-se nos funcionários, no acesso destes aos bens da organização, nos riscos que podem representar para a organização e na suficiência de contramedidas. Constitui a base do processo de gestão da segurança do pessoal. É, também, crucial para ajudar os gestores de segurança e recursos humanos a comunicar aos quadros superiores o risco a que a organização está exposta.

Muitas vezes, não existe uma lógica evidente na utilização de medidas específicas de segurança do pessoal e os recursos não estão proporcionalmente direcionados. As orientações do CPNI para a avaliação dos riscos da segurança do pessoal, ilustradas a partir de um estudo de caso ficcional, têm como objetivo ajudar os gestores de segurança e recursos humanos a:

- Conduzir avaliações dos riscos de segurança do pessoal de forma a equilibrar pragmatismo e rigor.
- Dar prioridade aos riscos internos de uma organização.
- Identificar as contramedidas apropriadas para contrariar esses riscos.
- Distribuir recursos de segurança do pessoal de forma rentável e proporcional ao nível de risco.

Good Practice Guide on Pre-employment Screening

O *Preemployment Screening* do CPNI é o último numa série de produtos de aconselhamento relativos à segurança do pessoal. Fornece orientação detalhada relativamente às medidas de controlo dos antecedentes laborais, incluindo:

- Verificação da identidade.
- Confirmação do direito de trabalhar no Reino Unido.
- Verificação do historial de dados pessoais de um candidato (incluindo verificações do registo criminal).

O manual está disponível em formato PDF e pode ser descarregado em www.cpni.gov.uk.

Expecting the Unexpected

Este guia resulta de uma parceria entre a comunidade empresarial, a polícia e os especialistas na continuidade operacional. Providencia aconselhamento relativamente à continuidade operacional na eventualidade de uma emergência e nos momentos subsequentes e contém ideias úteis no que diz respeito aos processos de gestão da continuidade operacional, bem como uma lista de verificação.

Secure in the Knowledge

Este manual destina-se principalmente a pequenas e médias empresas. Providencia orientação e informação para ajudar a melhorar a segurança básica. Idealmente, deve ser lido em conjunto com *Expecting the Unexpected*, acima mencionado. Ao seguir as orientações de ambas as brochuras, as empresas encontram-se na melhor posição para evitar e gerir uma variedade de ameaças aos seus negócios e recuperar dessas ameaças. Ambas as brochuras estão disponíveis para descarregar em www.cpni.gov.uk.

Lista de organismos e cargos

- ***Association of Chief Police Officers (ACPO)*** – Associação de Chefes de Polícia
- ***Association of Chief Police Officers, Terrorism and Allied Matters (ACPO TAM)*** – Associação de Chefes de Polícia, Terrorismo e Questões Aliadas
- ***Automatic Number Plate Reader (ANPR)*** – Leitura Automática de Matrículas
- ***Basic Disclosure certificate*** – Certificado de Divulgação Básica
- ***Borders and Immigration Agency*** – Agência de Imigração e Fronteiras
- ***CCTV Operational Requirements Manual (Ref: 55/06)*** – Manual de requisitos operacionais de CCTV
- ***Centre for the Protection of National Infrastructure (CPNI)*** – Centro para a Proteção das Infraestruturas Nacionais
- ***Counter Terrorism Security Adviser (CTSA)*** – Conselheiro de Segurança sobre Antiterrorismo
- ***County Court Judgments (CCJs)*** – Sentenças do Tribunal da Comarca
- ***Data Protection Act 1998*** – Lei de Proteção de Dados de 1998
- ***Disability Discrimination Act 1995*** – Lei para a não-discriminação da Deficiência de 1995
- ***Fire (Scotland) Act 2005*** – Lei contra Incêndios (Escócia) de 2005
- ***Fire Safety (Scotland) Regulations 2006*** – Regulamentos de Segurança contra Incêndios (Escócia) de 2006
- ***Fire Safety Order 2005*** – Ordem de Segurança contra Incêndios de 2005
- ***Fire Safety Risk Assessment*** – Avaliação do Risco de Segurança em caso de incêndio
- ***Gold Commander*/*Strategic Commander*** **(Escócia)** – Comandante Estratégico
- ***Health and Safety Acts*** – Legislação sobre Saúde e Segurança
- ***Health and Safety at Work Act 1974*** - Lei da Saúde e Segurança no Trabalho de 1974
- ***Home Office Scientific Development Branch (HOSDB)*** – Gabinete para o Desenvolvimento Científico do Ministério da Administração Interna
- ***Human Rights Act 1998*** – Lei dos Direitos Humanos de 1998
- ***Immigration, Asylum and Nationality Act 2006*** – Lei relativa à Imigração, Asilo e Nacionalidade de 2006
- ***Intelligence Community Websites*** – Serviços de Informação
- ***National Counter Terrorism Security Office (NaCTSO)*** – Gabinete Nacional de Segurança Antiterrorismo
- ***Operation Lighting*** – Operação Relâmpago
- ***Performance Testing of CCTV Systems (Ref: 14/95) –*** Testes de *performance* dos sistemas de CCTV
- ***Police Search Adviser (POLSA)*** – Conselheiro da Polícia em matéria de Buscas
- ***Police Security Co-ordinator (SECCO)*** – Coordenador de Segurança Policial
- ***Preemployment Screening*** – Controlo dos Antecedentes Laborais
- ***Public Space Surveillance*** – Vigilância do espaço público

- ***Regulatory Reform (Fire Safety) Order 2005*** – Disposição da Reforma Regulamentar (Segurança contra Incêndios) de 2005
- ***Rehabilitation of Offenders Act*** – Lei de Reabilitação de Delinquentes
- ***Security Industry Authority (SIA)*** – Autoridade da Indústria de Segurança
- ***UK Police Requirements for Digital CCTV Systems (Ref: 09/05)*** – Requisitos da polícia do Reino Unido para os sistemas de CCTV digitais