CONVENÇÃO DE QUIOTO

ANEXO GERAL
DIRECTIVAS

Capítulo 7

APLICAÇÃO DA TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO

(Versão Dez/2007 - Março/2017)

ORGANIZAÇÃO MUNDIAL DAS ALFÂNDEGAS

"Direitos de Autor © 2006 Organização Mundial das Alfândegas. Todos os direitos reservados. Os pedidos e as questões concernentes à tradução, reprodução e direitos de adaptação devem ser enviados a copyright@wcoomd.org".

ÍNDICE

1. Resumo 7

1.1. Objectivo das Directivas 7
1.2. O papel estratégico das TIC.. 7
1.3. Tendência futura 11
1.4. Âmbito 15
1.5. Tabela de concordância com a Convenção de Quioto 16

2. Benefícios da tecnologia de informação e comunicação (TIC) 17

2.1. Introdução 17
2.2. Controles aduaneiros mais eficazes 17
2.3. Desalfandegamento mais eficaz 18
2.4. Aplicação uniforme da legislação aduaneira 19
2.5. Arrecadação mais eficiente das receitas 19
2.6. Análise mais efectiva de dados 19
2.7. Apresentação eficiente de estatísticas do comércio externo 19
2.8. Melhor qualidade dos dados 20

3. Decisão de informatizar 21

3.1. Gestão de mudança 21
3.1.1. As dez etapas na implementação de mudança 22
3.1.2 Porque é que a mudança falha 24
3.1.3. Como assegurar que a mudança tenha êxito 25
3.2. Quem deve desenvolver o sistema? 26
3.2.1 Escolha de uma empresa de consultoria 27
3.3. O Comité Directivo 28
3.4. Tipos de planificação 28
3.4.1. Planificação estratégica 28
3.4.2. Planificação de projectos 29
3.4.3. Planificação de continuidade das actividades 30
3.5. Elaboração de uma arquitectura empresarial… 32

4. A importância das consultas 34

4.1. A comunidade empresarial 34
4.2. Pessoal Aduaneiro 34

5. O processo de desenvolvimento do sistema 36

5.1. Investigação detalhada e análise do sistema existente 36
5.2. Configuração detalhada do sistema 37
5.3. Programação 38
5.4. Aquisição e instalação de hardware 38
5.4.1. Aquisição 38
5.4.2. Pedido de Proposta (PP) 39
5.4.3. Avaliação das respostas aos PP 40
5.4.4. Instalação 41
5.5. Implementação do sistema 42
5.5.1. Teste do sistema 42
5.5.2. Conversão de ficheiros 43
5.5.3. Formação do utilizador 43
5.5.4. Estratégia de transição 44
5.6. Avaliação pós implementação 45
5.7. Manutenção do sistema 46
5.7.1. Motivos para a manutenção 46
5.7.2. Tipos de manutenção 47
5.7.3. Responsabilidade pela manutenção 47

5.8. Estabelecimento de um Serviço de Apoio 48
5.8.1 Compromissos de serviço com os clientes das Alfândegas 48
5.8.2. As Alfândegas precisam de um Serviço de Apoio? 49
5.8.3. Várias dimensões de Serviço de Apoio 49
5.8.3.1. Conceito de Serviço de Apoio: 49
5.8.3.2. Objectivos dos serviços e "momentos da verdade": 50
5.8.3.3. Recuperação de serviço 50
5.8.4. O Serviço de Apoio como um meio de prestação de valor 50
5.8.5. Como criar um Serviço de Apoio 51
5.8.6. Como avaliar o desempenho do Serviço de Apoio? 53
5.8.7. Impacto do Serviço de Apoio nas operações das Alfândegas. 53

6. Resumo das principais áreas de aplicação 54

6.1. Introdução 54
6.2 Validação de dados 55
6.3. Controle de inventário da carga 57
6.4. Processamento de declarações de mercadorias (importação e exportação) 58
6.4.1. Processamento antes da chegada/partida das mercadorias 59
6.4.2. Gestão de licenças, alvarás, certificados e outro tipo de autorizações 59
6.5. Reconciliação de dados 60
6.6. Notificação da autorização de saída 60
6.7. Luta contra a fraude aduaneira 60
6.8. Selecção 61
6.8.1. Gestão de Riscos 62
6.9. Controle antecipado de passageiros 62
6.10. Contabilização das receitas 62
6.11. Estatísticas do comércio externo 64
6.12. Sistema de Gestão da Informação (SGI) 64
6.13. Realização de relatórios 64
6.14. Armazenagem de dados 64
6.14.1 Recuperação de dados 65
6.14.2. Exploração de dados 65
6.15. Sistema de registo dos operadores comerciais 65
6.16. Trânsito aduaneiro 66
6.17. Outras aplicações 66
6.18. Informatização de escritórios 66
6.19. Intranet e Extranet das Alfândegas 67

7. Terceirização das alfândegas 69

7.1. Visão 69
7.1.1. Terceirização, deslocalização e internalização 69
7.1.2. Crescimento da terceirização 69
7.2. A terceirização no seio das Alfândegas e áreas que podem ser terceirizadas: actividades essenciais e actividades não essenciais 70
7.3. Vantagens da terceirização 71
7.3.1. Regresso às actividades essenciais 71
7.3.2. Responsabilidade 71
7.3.3. Qualidade 71
7.4. Desafios da terceirização 71
7.4.1. Questões ligadas à qualidade dos serviços 71
7.4.2. Questões ligadas aos recursos humanos 72
7.4.3. Questões ligadas à segurança 72
7.5. Conclusão: como estabelecer o equilíbrio apropriado 72

8. Interfaces entre as aplicações de TI 74

8.1. Arquitectura orientada para os serviços 75

9. Troca de informação 77

9.1 Troca de informação com os operadores comerciais 77
9.2. Troca de informação com outras instituições governamentais 78
9.3. Troca de informação com outras administrações aduaneiras 78

10. Comunicações 80

10.1. Soluções em matéria de transferência de dados 80
10.2. Telecomunicações 81
10.3. Troca de Mensagens 81
Anexo A à Secção 10.3. Mensagem 83
10.4. Códigos 84

11. Segurança das TIC 85

11.1. Segurança das TIC – Definição e objectivo 86
11.2. Política em matéria de segurança das TIC 86
11.3. Segurança da TIC - Considerações 86
11.3.1. Aquisição, desenvolvimento e manutenção dos sistemas 90
11.4. Autenticação 91
11.4.1. Porque é que a autenticação é necessária? 91
11.4.2. As alternativas electrónicas 92
11.4.3. Que método utilizar? 97
11.4.4. Risco Aceitável 97
11.4.5 Comparação de métodos de autenticação 98
11.5. Não-Rejeição 99
11.5.1. Definição de não-rejeição 99
11.5.2. A não-rejeição não é uma questão autónoma 99
11.5.3. Consequências legais da rejeição 100
11.5.4. Garantia 101
11.5.5. Razões da rejeição 101
11.6. Garantia de Identidade 102
11.6.1. Prova de identidade 102
11.6.2. Prova de autorização 102
11.6.3. O quadro 103
11.7. Garantia da Conteúdo 103
11.7.1. Garantia da Integridade 103
11.7.2. Combinar as diferentes partes. 103
11.7.3. Armazenamento e Reprodução 103
11.8 Integridade dos Processos 104
11.8.1. Sistema de Gestão 104
11.8.2. Arquitectura e Regulamentos do Sistema 104
11.9. Infra-estrutura de Chave Pública (PKI) 104
11.9.1. Antecedentes 105
11.9.2. Definição de uma PKI 105
11.9.3. Comparação de assinaturas digitais e convencionais 105
11.9.4. O ciclo de vida operacional de um certificado digital 106
11.9.5. Considerações importantes na implementação de soluções baseadas na PKI 106
11.9.6. Uso de assinaturas digitais no EDI e nas mensagens de Linguagem de Marcas Extensível (XML) 108
11.9.7. Autoridade de Certificação e Quadro Legal 108
11.9.8. PKI e Alfandegas: Principais questões a analisar 109
Apêndice A da Parte 11. Segurança das TIC. 110
11.10. Gestão da Identidade 111

12. Questões legais 114

12.1. Introdução 114
12.2. Adaptabilidade da legislação existente 114
12.3. Tipos de questões legais 114
12.4. Assinatura 115
12.5. Admissibilidade 115

12.6. Protecção dos dados e protecção da privacidade 116

13. Auditoria de controles internos aos sistemas informáticos 117

13.1. Generalidades 117
13.2. Auditorias de concepção 117
13.3. Planificação 118
13.4. Inquérito ou recolha de informações 119
13.4.1. Entrevistas 119
13.4.2. Exame da documentação 119
13.5. Consignação dos resultados de uma auditoria 120
13.6. Avaliação 120
13.7. Confirmação das conclusões de uma auditoria 120
13.8. Relatório 121
13.9. Verificação após auditoria 121
13.10. Conclusão 121

14. Problemas Correntes 122

14.1. Introdução 122
14.2. Resistência cultural 122
14.3. Informatização dos dados de base 122
14.4. Ausência de infra-estrutura adequada 122
14.5. Legislação aduaneira 123
14.6. Limitação dos recursos e das competências 123

Apêndice 1 – Estruturas de Telecomunicações e de Informação para o Comércio Electrónico 124
Apêndice 2 – Processo de Selecção Local 132
Apêndice 3 – Sistema de Filtro do Perfil de Selectividade 133
Apêndice 4 – Modelo de Procedimentos Aduaneiros e de Acesso aos Arquivos 134
Apêndice 5 – Fluxograma do Programa 135
Apêndice 6 – Diagrama de Processamento por Computador 136
Apêndice 7 – Glossário dos Termos e Abreviaturas 137
Apêndice 8 – Diagrama lógico de função de tecnologia de informação 145
Apêndice 9 – Recomendação da OMA sobre Tecnologia de Informação 147
Apêndice 10 – Recomendação da OMA sobre o uso de websites pelas Administrações Aduaneiras 149
Anexo à Recomendação sobre os Websites das Alfândegas 150
Apêndice 11 – Recomendação da OMA sobre o Guia de Transferência de Dados da OMA 154
Apêndice 12 – Recomendação da OMA sobre as necessidades de dados para Informação Antecipada sobre Viajantes (IAV) 155
Apêndice 13 – Recomendação da OMA sobre o uso da UNTDED 156
Apêndice 14 – Recomendação da OMA sobre o uso das regras de EDIFACT 158
Definição de ONU/EDIFACT 160
Apêndice 15 – Recomendação da OMA sobre o uso de códigos para elementos de Dados +ANEXO I a ANEXO IX 161
Apêndice 16 – Recomendação da OMA sobre a informação aduaneira processada por computador 172
Apêndice 17 – Recomendação da OMA sobre o uso dos padrões do CCC/IATA 174
Apêndice 18 – Recomendação do Conselho de Cooperação Aduaneira relativa à utilização do Modelo de Dados da OMA 175
Apêndice 19 – Recomendação do Conselho de Cooperação Aduaneira relativa À utilização das Informações Antecipadas sobre os Viajantes (IAV) e do Registo de Nomes dos Viajantes (RNV) para assegurar a eficiência dos controles aduaneiros 177
Apêndice 20 – Recomendação do Conselho de Cooperação Aduaneira relativa à desmaterialização dos documentos suporte 179

1. Resumo

1.1 Objectivo das Directivas

As presentes Directivas visam chamar a atenção das Administrações aduaneiras para a incidência das Tecnologias da Informação e da Comunicação ("TIC" mas por vezes igualmente designadas "TI") sobre as actividades aduaneiras. Descrevem como é que as Alfândegas podem utilizar esta técnica para melhorar os seus programas e planificar as melhorias a fazer nos serviços prestados aos seus clientes e parceiros comerciais. Elas não se destinam a fornecer um catálogo das últimas tecnologias disponíveis ou sugerir soluções na área do material/*hardwares* e/ou dos *softwares*. O foco destas Directivas continua a ser os princípios-chave que regem o uso das TIC nas Administrações Aduaneiras

1.2 O papel estratégico das TIC

Espera-se hoje das autoridades públicas do mundo inteiro, que prestem serviços públicos pela via electrónica. Para as Alfândegas, este imperativo impôs-se mais cedo que para as outras administrações. É normal que as Alfândegas, tendo em conta as suas responsabilidades importantes em matéria de controle das mercadorias, de arrecadação de receitas e de fiscalização das fronteiras, utilizem em uma primeira fase sistemas informáticos para controlar a inspecção e verificação das mercadorias, bem como a arrecadação das receitas conexas.

As administrações aduaneiras, em seguida, começam a utilizar as TIC para passar da inspecção de mercadorias para as informações relevantes contidas nas declarações de importação e exportação em papel. Constatou-se que elas podem igualmente reduzir a obrigação das empresas de apresentar numerosas exemplares de documentos "originais" sobre papel, desde que as principais informações estejam contidas num sistema informático que poderia não só validar e processar dados, mas também o armazenar a um custo inferior ao do armazenamento dos registos em papel.

No entanto, no estado rudimentar das TIC, as Alfândegas precisavam sempre que os documentos lhes fossem apresentados materialmente pelo declarante ou pelos seus representantes em um local ou um momento que lhes conviesse e que elas próprias especificavam. Depois, as evoluções das TI ofereceram a possibilidade de comunicar de maneira instantânea e directa. Essas tecnologias transformaram as estruturas e as regras de procedimento correntes. Por exemplo, as Alfândegas podem separar a liberação do desalfandegamento. As informações electrónicas, recebidas muito antes da chegada das mercadorias permitem às Alfândegas dispor de todas as informações necessárias para fins de controles.

As Administrações Aduaneiras modernas são bastante dependentes da aplicação das TIC. A exigência das partes interessadas de uma melhoria da eficácia em matéria de facilitação das trocas e de um cumprimento da legislação continua a incitar os gestores das Alfândegas a investir em projectos e iniciativas baseadas nas TI. Os sistemas avançados de gestão dos riscos e de Janela Única necessitam a utilização de tecnologias sofisticadas e obrigam a realização de investimentos complexos e maciços em material/*hardware*, serviços e *softwares*.

Em determinado número de Administrações Aduaneiras, os sistemas herdados de períodos anteriores continuam a ser utilizados por diversas razões. Mesmo se alguns desses sistemas não beneficiam de mais nenhuma assistência por parte dos fornecedores, as

Administrações são obrigadas a continuar e a mantê-los em bom estado a fim de preservar um nível satisfatório de desempenho em matéria de facilitação das trocas.

Segundo certas estimativas, nas principais empresas do sector dos serviços, o custo de exploração das tecnologias da informação representa a segunda despesa mais elevada depois dos recursos humanos e mobiliza 5 a 7% do total dos custos de exploração (fonte: Gartner Consulting – Worldwide IT Benchmark Services).

As TIC foram durante muito tempo consideradas como um serviço de apoio ou de acompanhamento. Este ponto de vista evoluiu recentemente e as TIC são agora reconhecidas como um elemento impulsionador das transformações e como um meio para beneficiar de uma vantagem competitiva.

Os gestores devem perceber os processos através dos quais as TI criam valor para a Instituição. A esse respeito, é necessário adoptar quadros de governação trazendo clareza e transparência, explicando às partes interessadas qual é a ligação entre os resultados obtidos e os investimentos efectuados nas TIC. As realizações devidas às TIC devem ser explicadas em termos operacionais.

É neste contexto que se desenvolveu a nova disciplina de Governação da Tecnologia da Informação, baseando-se essencialmente nos princípios de responsabilidade dos gestores e de controle estratégico, aos quais acrescem-se um certo número de estruturas e de competências profissionais que respondem às necessidades dos gestores administrativos e dos responsáveis operacionais.

A questão dos processos decisórios ligados às TI, considerada como uma questão estratégica no seio da instituição, foi incluída nas Directivas. Convém descrever o método que as Administrações Aduaneiras devem desenvolver para ligar os objectivos estratégicos da instituição com os processos de TI em causa.

Este trabalho ajudará as Alfândegas a reforçar as suas missões de capacitação nos processos de TI mais importantes. É igualmente nesta parte que deve ser abordada a questão da pertinência da Arquitectura empresarial na gestão dos investimentos estratégicos destinados à TI.

Qualquer Administração Aduaneira tem como objectivo preservar o valor na cadeia logística internacional melhorando a eficácia dos controles transfronteiriços de maneira a não interromper o fluxo das mercadorias, preservar a segurança das fronteiras e impedir qualquer fuga de receitas fiscais. Os Gestores das Alfândegas e das empresas vêem este valor em termos de eficácia dos controles e de eficiência da cadeia logística. As TIC devem contribuir para esses esforços e tanto as Alfândegas como as empresas devem atingir os objectivos operacionais apoiando-se sobre as capacidades constantemente renovadas das TIC.

Os investimentos em TIC aumentaram de forma considerável durante a última década mas o retorno do investimento não é uniforme. Não é raro ver Gestores adoptar uma atitude crítica em relação aos trabalhos realizados no seio da instituição em matéria de TI e de fazer prova de pouco entusiasmo diante dos resultados obtidos. Outros Gestores, que compreendem o valor geral do investimento proposto, não estão em condições de estabelecer um elo entre esses investimentos e os resultados obtidos. É necessário dispor de uma estrutura que ajude os Gestores a fiscalizar o valor realmente acrescido pelos investimentos em matéria de TIC e que permita ter uma garantia credível que os objectos da instituição estão conformes aos projectos e serviços das Tecnologias da Informação. O Quadro «COBIT» para a Governação e Controle das TI é uma ferramenta importante que divide o conceito de governação de TI nos «objectivos de controle» mencionados abaixo:

Planificar e organizar

PO1: definir um plano estratégico informático.

PO2: definir a arquitectura da informação.

PO3: determinar a orientação tecnológica.

PO4: definir os processos, a organização e as relações laborais.

PO5: gerir os investimentos informáticos.

PO6: divulgar os objectivos e as orientações da gestão.

PO7: gerir os recursos humanos da informática.

PO8: gerir a qualidade.

PO9: avaliar e gerir os riscos.

PO10: gerir os projectos.

Adquirir e implementar

AI1: encontrar soluções informáticas.

AI2: adquirir aplicativos e garantir a sua manutenção.

AI3: adquirir a infra-estrutura técnica e garantir a sua manutenção.

AI4: facilitar o funcionamento e a utilização.

AI5: adquirir recursos informáticos.

AI6: gerir as mudanças.

AI7: Instalar e validar soluções e modificações.

Entregar e apoiar

DS1: definir e gerir os níveis de serviço.

DS2: gerir os serviços terceirizados

DS3: gerir o desempenho e a capacidade.

DS4:. assegurar um serviço contínuo

DS5:. garantir a segurança dos sistemas

DS6:. identificar e imputar os custos

DS7: instruir e formar os utilizadores.

DS8: gerir o serviço de assistência ao cliente e os acidentes.

DS9:. gerir a configuração

DS10: gerir os problemas

DS11: gerir os dados.

DS12: gerir o ambiente físico.

DS13: gerir a exploração.

Fiscalizar e avaliar

ME1: fiscalizar e avaliar o desempenho das TI

ME2:. fiscalizar e avaliar o controle interno

ME3: assegurar a conformidade com os regulamentos

ME4: implementar a governação das TI.

Este Quadro faz-se acompanhar de um conjunto de ferramentas graças às quais os Gestores podem ter em conta as exigências ligadas aos controles, as questões técnicas e os riscos operacionais. Aborda de forma extensiva/completa a governância das TI e abrange um leque amplo de questões que um Gestor das Alfândegas deve controlar. As Directivas sobre a TI abordam a maioria dessas questões em secções diferentes.

- melhorar a arrecadação das receitas e a gestão da política comercial na importação e exportação ;

- acelerar a saída de mercadorias na importação e exportação e oferecer outros procedimentos preferenciais aos clientes que consideram como sendo os mais fiáveis em matéria de cumprimento da legislação e, portanto, como representando menos riscos para a arrecadação de receitas e outras responsabilidades aduaneiras;

- responder às preocupações do governo e dos utilizadores que desejam que as mercadorias proibidas, as espécies ameaçadas de extinção, os direitos da propriedade intelectual, etc. sejam objecto de controles eficazes ; e

- assegurar a integridade e eficácia da gestão do movimento das mercadorias e dos viajantes.

As Administrações Aduaneiras modernas devem fazer face, a nível internacional, a uma serie de inovações comerciais diversas que se baseiam em aplicativos de TI, nomeadamente serviços de transporte expresso e outros serviços globais de transporte multimodal, e uma rede crescente de sistemas mundiais de abastecimento, produção e distribuição alimentados por redes logísticas de gestão *just-in-time*.

Garantir que as práticas utilizadas pelas Alfândegas permaneçam ao diapasão desses desenvolvimentos comerciais requererá mudanças igualmente inovadoras nos princípios de base da gestão administrativa.

Enquanto que numerosas Administrações utilizam ou consideram a possibilidade de utilizar as TIC para melhorar as suas operações, a maioria dos procedimentos actualmente utilizados pelas Alfândegas ainda baseiam-se na recepção de equivalentes electrónicos dos documentos antigos trocados. As declarações em suporte papel foram simplesmente substituídas por mensagens EDI.

As Administrações que actualmente consideram a possibilidade de conceber ou melhorar os seus aplicativos de TI deveriam dar um novo passo ao constatar que praticamente todos os dados que as Alfândegas precisam já existem nos sistemas de informação comercial utilizados para efectuar as transacções comerciais.

Deveriam determinar em que medida as suas próprias necessidades de dados de controle podem ser satisfeitas pelos sistemas de informação dos seus parceiros comerciais depois de eles terem sido sujeitos a uma auditoria para assegurar-se que eles são seguros, capazes de reproduzir os dados com precisão e possuem as facilidades apropriadas em matéria de conservação e arquivo dos dados.

Se, conforme é geralmente o caso hoje, esses sistemas de TI demonstram fornecer dados mais precisos e mais facilmente utilizáveis pelas Alfândegas que as trocas tradicionais de documentos em formato papel, as Administrações Aduaneiras estarão cada vez mais em condições de confiar nos sistemas informatizados dos seus parceiros comerciais autorizados que terão sido sujeitos a um controle para responder às suas próprias necessidades em matéria de dados de natureza fiscal, comercial e outra.

A maioria das Administrações Aduaneiras é hoje obrigada a suportar uma carga de trabalho crescente ligada ao controle das mercadorias e dos viajantes, e isto, com os efectivos existentes, e até por vezes reduzidos. Muitas dentre elas já demonstraram que o recurso às TIC melhorou a qualidade da introdução e da gestão das informações e que permitiu disponibilizar recursos pouco numerosos a fim de os concentrar nas principais tarefas de luta contra a fraude, nomeadamente a identificação e o controlo das pessoas e das consignações suspeitas.

As presentes Directivas recomendam às Administrações Aduaneiras que utilizam as TIC, que respeitem as normas internacionais relevantes. É indispensável que qualquer norma realmente utilizada nos aplicativos informáticos seja facilmente identificável e disponível para fins de toda e qualquer troca necessária com as outras Administrações.

Antes de adoptar um aplicativo em matéria de TI, as Administrações devem consultar as partes interessadas susceptíveis de ser afectadas, nomeadamente os outros serviços públicos bem como as empresas, os transportadores, os agentes, as empresas que exploram portos e aeroportos, a fim de assegurar-se que todas poderão aplicar facilmente a solução escolhida. Um mecanismo permanente de consulta com esses parceiros, durante todas as fases posteriores da concepção do sistema, permitir-lhes-á conceber e adaptar os seus próprios sistemas, e encorajá-los-á a fazê-lo, a fim de tirar o melhor partido das inovações das Alfândegas e de oferecer igualmente a melhor utilização possível.

As presentes Directivas têm realmente como objecto principal, chamar a atenção de todas as Administrações Aduaneiras para a utilização das TIC no âmbito das suas próprias operações, mas as Administrações deverão seguir, e ter plenamente em conta, os aplicativos paralelos e pertinentes, ligados à evolução rápida das práticas comerciais, que tiveram, e continuarão a ter repercussões profundas na gestão quotidiana.

1.3. Tendência futura

Enquanto que, no passado, a OMA concentrou a sua atenção no uso das tecnologias de

IC em operações aduaneiras convencionais, recentes discussões começaram a explorar o seu efeito na actividade aduaneira como um todo.

É óbvio que as Alfândegas precisarão de abandonar a mentalidade “um tamanho serve para todos” ligando ao Intercâmbio Electrónico de Dados (EDI), o meio inicial para a comunicação e colecta de dados comerciais informatizados, direccionadas à uma filosofa de um sistema aberto no qual serão capazes de trocar informação electronicamente por uma série de meios diferentes com os empregados, clientes comerciais e não comerciais e, nacional e internacionalmente com outros departamentos e instituições governamentais relevantes.

Ao planificar tal migração, as Alfândegas precisaram de considerar o facto de que um terço e um meio do comércio internacional consiste agora de transacções intra-empresariais, nos quais os materiais, os componentes, e os produtos parcialmente processados e/ou acabados estão a ser transportados através da fronteira nacional, ao abrigo de sistemas integrados de gestão comercial e estão a diminuir de modo crescente e a exigir prazos.

Os outros sectores comerciais que participam na compra/venda tradicionais procuram o conselho e ajuda dos provedores de serviços da cadeia logística para verificar estes sistemas de gestão de transacções, altamente eficiente e sem coerência.

As Alfândegas em toda parte, ainda tratam tais movimentos como uma série de operações separadas de importação e exportação. Todas as administrações vêem e tratam apenas metade de cada transacção internacional.

A chave para um controle aduaneiro melhorado, baseado numa maior resposta inovadora para a actual prática comercial bem estabelecida e rapidamente crescente assenta na definição e implementação de acordos bilaterais e multilaterais de Assistência Mútua entre as Administrações Aduaneiras para providenciar e aplicar uma gestão unificada de um conjunto de controles e procedimentos.

Várias Administrações Aduaneiras lançaram projectos piloto e protótipos, em colaboração com empresas interessados seleccionados para explorar e testar o conjunto de dados necessários e padrões de comunicação, identificar obstáculos legais e avaliar custos/benefícios práticos para todos os participantes.

A experiência adquirida neste âmbito, no quadro destes projectos demonstrou até ao momento que enquanto as tecnologias necessárias já estão disponíveis, os quadros legais nacionais e internacionais existentes que governam o movimento das mercadorias e a informação precisarão de um estudo e eventual revisão.

As técnicas de gestão de entrega em tempo oportuno resultaram inevitavelmente na multiplicação de consignações pequenas, repetitivas e frequentes. Em conformidade com os fins aduaneiros cada consignação tem de providenciar o seu próprio pacote de dados relevantes de controle, isto teria causado problemas sérios de processamento da informação.

Felizmente, os transportadores especializados em todos os meios de transporte já estão a usar tecnologias de IC para maximizar a eficiência logística e as Alfândegas através do uso de sistemas de *e-commerce* (EC) apropriados e de uma série de técnicas de intercâmbio electrónico de dados (EDI) podem tirar vantagem deste fluxo de dados bem gerido para alimentar os seus próprios procedimentos de gestão de riscos e de desalfandegamento. Numerosos serviços aduaneiros adoptaram, ou irão implementar as aplicações de EDI através de formatos de mensagens padronizadas, e principalmente os da UN / EDIFACT. Para garantir a compatibilidade dessas mensagens, recomenda-se a desenvolver todos os sistemas EDIFACT sobre a base de cartões EDIFACT do Modelo de Dados da OMA.

As normas UN / EDIFACT que definem as estruturas de dados para, praticamente, todos os tipos de actividades e documentos oficiais utilizados no quadro do comércio internacional ainda são a única autoridade a nível mundial. A linguagem de marcas extensíveis (Extensible Mark-up Language ou XML) também surgiu como um padrão dominante. As estruturas de dados e os vocabulários XML são enriquecidos por diferentes organismos de normalização, incluindo a OMA. As novas tecnologias e as infra-estruturas de telecomunicações, tais como as oferecidas pela Internet, oferecem às Alfândegas custos baixos nos meios de recepção e disseminação da informação, incluindo a Linguagem de Marcas Extensíveis (XML), publicação de base de dados, publicação de documentos e formulários electrónicos. Consultas apropriadas com os parceiros comerciais permitirão às Alfândegas oferecer as suas comunidades comerciais uma vasta gama de opções de troca de informação. Algumas destas estão estabelecidas no Apêndice 1.

A rápida evolução do modelo de tecnologia das operações de negócios actuais e serviços tradicionais electronicamente são negligenciados. Em função das suas prioridades estratégicas, cada administração aduaneira concentra-se de forma diferente sobre a necessidade de ficar em contacto com os desenvolvimentos tecnológicos e qualquer nova utilização de TI é justificada por uma situação particular.

Vários grandes desenvolvimentos em TI ocorrem simultaneamente, os quais irão alterar o modo de prestação de serviços nos próximos anos. Alguns deles são mencionados a seguir:

1. Os dispositivos portáteis do utilizador final: utilizadores finais estão melhor equipados do ponto de vista tecnológico e, hoje em dia, eles têm acesso aos dispositivos, em bons mercados, aos computadores que apenas tinham há apenas alguns anos. Esses dispositivos apresentam-se em diferentes formas e tamanhos para atender às necessidades específicas de cada utilizador. Os *smartphones* e *tablets* são duas grandes categorias de tais dispositivos e os *tablets* podem às vezes ser transformados em computadores de escritório.

2. Internet a partir de qualquer lugar: os dispositivos móveis estão agora conectados à rede Internet sem fios e pode estar em permanência "*online*". O acesso à internet de rápida velocidade em dispositivos móveis é uma realidade nos países industrializados, mas os países menos desenvolvidos também estão tentando recuperar esse atraso. Os governos podem melhorar o acesso às suas aplicações através da Internet.

3. As aplicações (APP) são um novo tipo de software que funciona nos dispositivos portáteis (APP é uma abreviatura para as aplicações de software). As APP são fáceis de encontrar, comprar, instalar, lançar, a funcionar e a actualizar. A velocidade com que um consumidor pode aceder e usar as APP é inédita. A sua utilidade e facilidade de utilização representam um avanço considerável. O contributo das novas APP, úteis e inovadoras para dispositivos portáteis está constantemente a renovar-se e responde a todas as principais funções comerciais. As informações fornecidas por alguns membros da OMA sugerem que a chegada de tais aplicações para as empresas é apenas uma questão de tempo. Podemos imaginar que as Administrações Aduaneiras seriam capazes de oferecer ao utilizador final a possibilidade de dispor, de imediato, de soluções operacionais.

4. Interface do utilizador: o teclado, o rato e a interface gráfica do utilizador são concorrentes da interface táctil dos dispositivos portáteis. Esta interface força os que desenvolvem os dispositivos de software para definirem como devem converter funções operacionais dentro de gestos com os dedos num *tablet*. Por outras palavras, eles estão tentando encontrar as aplicações que sejam o mais cómodo possível para o utilizador de um dispositivo portátil. Assim, os obstáculos decorrentes da utilização da aplicação são menores para o utilizador. Por exemplo, a menos que não tenha outra escolha, o utilizador não será obrigado a apresentar os dados, resultando num elevado nível de reutilização de dados operacionais.

5. Capacidade de contextualização e de geolocalização das aplicações: Os dispositivos inteligentes já foram desenvolvidos e são capazes de revelar a localização, em tempo real, os contentores, as mercadorias, os meios de transporte, os funcionários de logística, os funcionários aduaneiros e outros interessados. Estas capacidades oferecem novas possibilidades para a criação de aplicações de maneira a que os fluxos de informações e de mercadorias circulem sempre juntos. Os dados obtidos a partir de dispositivos chamados sensores são também conhecidos por desempenharem um importante papel. Os sensores usados para rastrear os recipientes dos contentores e controlar os dispositivos de identificação por radiofrequência (RFID) instalados em selos electrónicos geram os fluxo contínuos de dados operacionais úteis.

6. Os media sociais apresentam-se na forma de um conjunto de aplicações baseados em Internet para a criação e partilha de informações por utilizadores que fazem parte de uma comunidade virtual. Os media sociais mudaram radicalmente a forma como as organizações, comunidades e indivíduos comunicam. Eles estão sendo rapidamente adoptados por empresas como um meio de comunicação com os seus clientes e com as partes interessadas. Eles fornecem às Administrações Aduaneiras a oportunidade de alcançar uma transparência e uma coerência dos controles.

7. Grandes quantidades de dados ("Big Data"): os dispositivos inteligentes, as redes sociais e as unidades de recolha dos sensores estão ligados aos sistemas das empresas, que recebem continuamente volumes importantes de dados. As tecnologias necessárias para gerir tais volumes de dados são as tecnologias "Big Data", que podem se revelar úteis para as Administrações Aduaneiras gerando informações operacionais preciosas ou ajudando a melhorar a gestão de riscos.

8. Plataforma de computação em nuvem (cloud computing) a informática em nuvem tornou-se muito importante no campo da computação empresarial. A tecnologia de informação em nuvem contribui para acondicionar e apresentar os recursos do computador disponíveis para o consumo, como os servidores ou a capacidade de armazenamento e de rede e, através do conceito de virtualização na forma de infra-estruturas como um serviço. A computação em nuvem abrange, igualmente, as abordagens tais como software como um serviço e as plataformas como um serviço. A tecnologia de informação em nuvem tornou os recursos informáticos mais acessíveis e mais rentáveis do que as soluções tradicionais. A adopção de tecnologias de informação em nuvem é necessária entre os governos, onde muitas vezes são implementados como uma "nuvem privada". Os riscos relacionados com a segurança de dados são menos importantes pois os dados residem em centros de dados que o governo gere ou faz funcionar. As administrações encontram essas soluções pelas seguintes razões:

a. A tecnologia de informação em nuvem contribui para evitar as despesas de capital, reduzindo assim os riscos ligados aos investimentos.

b. Para a redução dos custos de lançamento de projectos-piloto e de demonstração de viabilidade, que ajuda a testar e a lançar mais rápido as novas iniciativas.

c. Desde que uma aplicação esteja pronta para a produção, torna-se fácil aceder à infra-estrutura informática em nuvem que pode assegurar imediatamente a produção.

d. A informática em nuvem permite que às Administrações de consolidar os recursos informáticos e, assim, beneficiar da tecnologia enquanto controla, no seio do governo, as questões de segurança do governo e de competências sobre os dados.

e. Graças à informática em nuvem, as Administrações Aduaneiras podem esperar terceirizar os serviços informáticos "no pedido", sem se envolver na compra e no funcionamento da sua própria infra-estrutura.

f. Alguns serviços podem ser usados de modo estratégico pelo governo em vez de departamentos distintos, fazendo apelo a inúmeras partes terceiras.

No entanto, deve notar-se que o uso da informática em nuvem ainda está no início e que esta tecnologia suscita importantes preocupações em matéria de segurança. Os governos geralmente querem saber onde se encontram os dados e querem ser capazes de verificar completamente o acesso e a confidencialidade dos referidos dados. Os governos de todos os países executam as políticas formais relativas à informatização em nuvem, e para tratar de questões levantadas por esta tecnologia, e tirando partido da sua implantação. A informatização em nuvem deve ser mais amplamente implementada no contexto de projectos inteiramente novos e para fins de aplicação não essenciais à sua missão.

Em todo o mundo, os governos estão a implementar políticas oficiais de informatização em nuvem e estima-se que esta tecnologia vai ser cada vez mais implantada para novos projetos e para as aplicações que não são essenciais numa determinada missão.

Tendo em conta estas tendências futuras, as Alfândegas devem planear a mudança da sua infra-estrutura em matéria de TIC.

1.4. Âmbito

As presentes Directivas foram elaboradas para ajudar as Alfândegas a decidir como utilizar as TIC para melhorar os serviços que elas oferecem aos seus clientes e parceiros comerciais. Determinam as principais áreas dos programas oferecidos pelas Alfândegas nos quais a utilização das TIC será sem dúvida mais benéfica. Propõem e descrevem os eventuais interfaces dos parceiros comerciais, bem como vários factores que as Administrações devem ter em conta na utilização das TIC. Esses factores são nomeadamente as necessidades e as questões de ordem jurídica, os aspectos de segurança e a consulta dos clientes.

As TIC permitem às Alfândegas melhorar os seus controles e em paralelo reforçar a facilitação. Para tirar melhor proveito dessas vantagens, uma Administração Aduaneira que esteja a considerar a possibilidade de aplicação das TIC deverá previamente estudar os procedimentos que ela aplica para dispensar os seus programas, tendo em conta o facto que as TIC podem apenas oferecer ferramentas para apoiar actividades de fundo. É suposto os procedimentos terem já sido reajustados em conformidade com as Normas, Anexos e Directivas da Convenção de Quioto Revista.

As presentes Directivas não abrangem as soluções ligadas ao material/*hardware* e/ou aos *softwares* porquanto devem ser escolhidas individualmente por cada Administração tendo em conta as suas próprias necessidades e as necessidades conexas dos seus parceiros comerciais.

As presentes Directivas visam:

- Encorajar as Administrações Aduaneiras a efectuar pesquisas e a utilizar as soluções oferecidas pelas TIC para apoiar os controles e os procedimentos que elas aplicam actualmente ;

- Aconselhar e incitar as Administrações Aduaneiras que considerem a possibilidade de utilizar a informatização a respeitar um processo/plano predefinido que abranja as suas necessidades todas ;

- Promover o uso de normas internacionais nas trocas de dados electrónicos entre as Administrações Aduaneiras e os seus parceiros comerciais ; e

- Aconselhar as Administrações Aduaneiras relativamente aos factos novos actuais e futuros que poderiam melhorar a informatização das Alfândegas.

1.5. Tabela de correspondência com a Convenção de Quioto

Disposição do Anexo Geral	Parte das Directivas relativas às TI
3.11	8, 9.3, 9.4
3.18	6.4
3.21	6.4
6.9	2, 6.6, 12
6.10	4

2. Benefícios da tecnologia de informação e comunicação (TIC)

(Norma Transitória 6.9, Normas 7.1 e 7.3).

2.1. Introdução

A presente secção define as principais áreas de procedimentos onde a introdução das tecnologias de IC beneficiarão as Alfândegas e os operadores comerciais, tendo em conta que esta medida pode exercer uma grande influência nas relações de trabalho entre alfândegas/comércio e que muitos dos benefícios que as Alfândegas podem tirar da introdução das tecnologias de IC requererão um entendimento cabal, e colaboração das suas comunidades comerciais.

A planificação e o desenvolvimento da informatização, deve incluir, e ser precedida de uma análise de custo-benefício detalhada, tendo em conta os interesses comerciais relevantes, para verificar que as soluções projectadas venham a ser úteis e eficazes para todas as partes interessadas. Deve-se recordar que a introdução de certas tecnologias de IC, por exemplo EDI, pelas Alfândegas pode obrigar os empresas a investir recursos no desenvolvimento de *softwares* necessários para interfaces nos seus sistemas, com despesas adicionais associadas por exemplo, aos encargos de tráfego de rede.

A participação de representantes das empresas, sempre que possível, no processo aduaneiro de planificação e de tomada de decisão pode de ser feito de várias formas, mas a medida mais comum inclui o estabelecimento de um grupo consultivo constituído por alfândegas/comércio, apoiado por reuniões públicas, pacotes e boletins informativos. Este grupo consultivo é muito importante porque pode permitir aos que estiverem fora das Alfândegas e que sejam directamente afectados pelo sistema proposto influenciar a sua implementação e eventualmente, adquirir um sentido de responsabilidade do eventual resultado. Este grupo deve ser estabelecido logo na fase inicial de planificação do projecto e deve reunir regularmente ao longo de todo o seu ciclo de vida.

A realização de reuniões públicas abertas a todas as empresas individualmente, bem como aos seus representantes, oferece meios adequados de transmitir informações e, em contrapartida, receber opiniões de um vasto círculo comercial. Estas reuniões devem ser apoiadas pela disponibilização de *arquivos* de informação, descrevendo o sistema proposto e a forma como poderia afectar e mudar as operações comerciais, com detalhes dos requisitos relevantes do sistema do operador comercial.

2.2. Controles aduaneiros mais eficazes

As principais funções das Alfândegas são a aplicação de controles eficazes para prevenir a evasão fiscal, reprimir a fraude e o contrabando, aplicar políticas comerciais e fazer cumprir uma série de prescrições de protecção do público.

No sentido de cumprir com essas responsabilidades, as Alfândegas são obrigadas a intervir, regularmente, no movimento de mercadorias que atravessam a fronteira nacional de forma a verificá-las e/ou a examinar as informações relevantes a estas associadas.

Tendo em conta os recursos limitados à disposição das Alfândegas e as exigências actuais da actividade comercial, no que concerne aos prazos, é normalmente impossível eliminar

o risco através do controle e verificação de todas as remessas que entram e saem do território. As Alfândegas das nações líderes do comércio, tornaram-se peritas das técnicas modernas de gestão de risco, cuidadosamente elaboradas e aplicadas para seleccionar e identificar as pessoas e as remessas suspeitas

A avaliação de riscos e as rotinas de selecção para identificar as remessas para a verificação documental e física podem ser aplicadas no âmbito de um sistema manual, mas podem ser realizadas de maneira muito mais coerente, credível e melhor documentada pelas administrações que tenham informatizado os seus sistemas de controle de passageiros, dos transportadores, dos meios de transporte e carga e/ou de processamento de declarações de mercadorias.

Informações recentes, reunidas pelas Alfândegas podem ser inseridas no sistema informatizado para complementar os dados históricos, nomeadamente os antecedentes dos operadores em matéria de cumprimento da lei e orientar o processo de selecção e identificação. Esta análise sistemática, correcta e oportuna dos ficheiros pode aumentar consideravelmente as probabilidades das Alfândegas detectarem e reprimirem práticas fraudulentas. Uma das vantagens conexas da informatização é que ela contribui igualmente para detectar transacções de importação em que o valor declarado dos produtos não se enquadra nos parâmetros previamente determinados.

2.3. Desalfandegamento mais eficaz

A informatização do controle de passageiros e de mercadorias permite:

- aumentar a produtividade das Alfândegas e dos operadores comerciais;
- racionalizar a utilização dos recursos oficiais e comerciais;
- estimular os concorrentes a melhorar a sua própria capacidade, oferecendo às empresas idóneas procedimentos preferenciais que possam melhorar as suas operações comerciais e o cumprimento da lei;
- reduzir os custos suportados tanto pelas Alfândegas como pelos operadores comerciais acelerando a autorização de saída das mercadorias;
- reunir tempestivamente as informações mais precisas;
- dispor de capacidades mais seguras em matéria de combate contra a fraude;
- reduzir o congestionamento nos portos e aeroportos.

A informatização dos procedimentos aduaneiros e a troca electrónica de informação, tais como o frete e as declarações de mercadorias, abre o caminho para o processamento da informação antes da chegada e/ou antes da partida. A recolha e a verificação da informação reguladora antes da chegada das remessas de importação ou exportação, no local de controle físico pelas Alfândegas, permite às administrações proceder a uma primeira avaliação de riscos e notificar por via electrónica as decisões sobre as condições da autorização de saída das mercadorias, imediatamente após a chegada.

A utilização apropriada da tecnologia de informação e da comunicação no âmbito de acordos de cooperação concluídos entre as Alfândegas, as outras instituições oficiais e os declarantes, permite a todas as partes ligadas a uma transacção de importação/exportação utilizar o processo de Guiché Electrónico Único, através do qual as instituições oficiais fronteiriças relevantes possam partilhar os dados de controle exigidos para oferecer aos operadores comerciais um procedimento de autorização de saída/desalfandegamento racionalizado, concentrado num único ponto.

2.4. Aplicação uniforme da legislação aduaneira

Os regulamentos que regem as competências e atribuições das Alfândegas estão constantemente a aumentar quer em quantidade, quer na sua complexidade. Num ambiente de sistemas manuais, as Alfândegas podem ter dificuldades em certificar-se de que foram tidos em conta todos os regulamentos existentes durante o processamento de cada remessa de importação e de exportação. Mas, um sistema informatizado devidamente concebido e bem programado em relação a todos os requisitos reguladores relevantes, pode assegurar que todas as transacções sejam processadas de modo abrangente e compatível com todos os requisitos legais apropriados. Isto assegura uma aplicação uniforme da legislação nacional a todos os operadores comerciais. As Alfândegas podem também utilizar padrões de dados internacionais e técnicas comercias de modelagem para oferecer a mesma uniformidade e tratamento equitativo no âmbito das regras comerciais de maneira a que, quando a legislação mudar, as regras sejam igualmente alteradas.

2.5. Arrecadação mais eficiente das receitas

Em muitos países, os direitos de importação e demais imposições constituem a principal fonte de receitas, a arrecadação e a contabilização eficientes e tempestivas destas são fundamentais para a economia nacional. A informatização das Alfândegas pode ajudar a satisfazer estas necessidades. Um ambiente de reconciliações manuais de receitas devidas e pagas pode ser lento e propenso a erro. A informatização pode identificar e quantificar rapidamente e em qualquer momento, as dívidas pendentes, para a acção apropriada e imediata.

2.6. Análise mais efectiva de dados

As Alfândegas são a fonte primária de dados do comércio internacional, solicitados pelos governos para análise económica e negociações relativas às políticas comerciais, nos quais os operadores se baseiam para ajudar nas pesquisas mercado e orientar as estratégias de venda.

A devida avaliação e organização de informação tão detalhada, recolhida e mantida em sistemas manuais baseados em papel é volumosa e leva tempo. A extracção de dados úteis relacionados entre si é bastante intensa e trabalhosa.

A informatização fornece informação comercial actualizada como um subproduto virtual do processamento das exportações e importações. As Alfândegas podem oferecer os benefícios resultantes a todos os utilizadores subsequentes e podem aplicar sistemas de gestão da informação (SGI) para interpretar e explorar esta informação de modo a melhorar as suas operações a nível nacional e local, em particular no que respeita ao eficaz controle *a posteriori*.

Os operadores comerciais que utilizam as tecnologias de IC estão habilitados a enviar, tempestivamente, dados sem erros às Alfândegas que, por sua vez, podem confiar na exactidão destes dados, nesta e em qualquer fase subsequente de análise de dados, graças aos controles de validação e de credibilidade desenvolvidas no processo informatizado de recolha.

2.7. Apresentação eficiente de estatísticas do comércio externo

Quase todas as Administrações Aduaneiras são responsáveis pela recolha de dados comerciais utilizados como base para a compilação de estatísticas nacionais do comércio externo e informação para uma série de decisões políticas e económicas importantes. Os dados necessários são geralmente extraídos das declarações de importação e exportação de

mercadorias. Num sistema informatizado os dados podem ser apresentados imediatamente num formato e estrutura definidos e ter um elevado nível de exactidão, ao passo que em sistemas manuais, só se tornam disponíveis numa fase posterior do processo de autorização de saída. As estatísticas apresentadas graças aos programas informáticos das Alfândegas apresentam um bom custo/benefício e facilitam a tomada de medidas oportunas por parte de outras instituições governamentais.

2.8. Melhor qualidade dos dados

As verificações da validação de dados e de credibilidade na recolha permitem às Alfândegas resolver as discrepâncias enquanto as mercadorias estiverem ainda sob o seu controle directo e assegurar a conformidade dos dados de base principais inseridos nos sistemas informatizados das Alfândegas para todos os fins subsequentes.

A validação dos dados, que visam proteger uma aplicação informática contra a introdução de informações erradas, é de suma importância. Uma vez inseridos no sistema os dados incorrectos, os resultados de qualquer processamento serão inúteis e o investimento associado de recursos financeiros e outros será desperdiçado.

3. Decisão de informatizar

(Norma Transitória 7.1)

Por que é que uma Administração Aduaneira, ou para este efeito, qualquer organização, deseja informatizar as suas operações? Para aumentar a eficácia, resolver qualquer problema existente ou suprir uma nova necessidade nas Alfândegas, como por exemplo, a implementação da Convenção de Quioto Revista, são algumas das respostas mais usuais. Todas e qualquer uma destas são razões perfeitamente lógicas para a informatização.

Existem muitas outras, algumas menos fáceis de admitir e formular, mas pelo menos, igualmente válidas, tal como a melhoria da integridade profissional.

Todos os projectos de informatização devem ser abordados com o maior cuidado em função das perdas financeiras e de outras que possam resultar dos erros de planificação e de gestão. Esta advertência não tenciona, de maneira alguma, impedir as administrações de introduzir sistemas informatizados, mas apenas alertá-las sobre possíveis fracassos, caso não tomem cuidado no sentido de evitar estes enganos na fase inicial do processo de planificação do projecto e possam avançar com justificada confiança.

Desde que a gestão superior decida a seu favor até ao momento em que o sistema é posto em funcionamento, o processo de informatização requer uma planificação e controle especializados e intensivos, independentemente do novo sistema estar ou não a ser desenvolvido por funcionários da administração ou por consultores externos.

Dado o volume de despesas em equipamentos, serviços e pessoal, invariavelmente associado ao desenvolvimento e implementação de um sistema aduaneiro informatizado (inclusive os interfaces e os sistemas de janela única com os outros serviços governamentais), bem como as concomitantes mudanças nos procedimentos básicos e métodos de funcionamento, qualquer projecto desta natureza apresenta grandes riscos.

A planificação e o controle cuidadosos são essenciais para identificar e avaliar riscos e incertezas, reduzir ou eliminar estes riscos sempre que possível e assegurar a implementação regular sem implicações graves, em termos de custos ou tempo. O controle adequado, base para uma planificação abrangente e lógica deve permitir aos gestores superiores reconhecerem oportunamente quaisquer desvios e tomarem as medidas correctivas imediatas.

3.1. Gestão de mudança

Nas estruturas sociais modernas, todas as instituições, quer sejam governamentais, lucrativas ou não lucrativas, no domínio da saúde ou da educação, estão enfrentando pressões crescentes exercidas a favor da mudança, esperando-se que elas:

- façam mais com menos;
- o façam com mais celeridade;
- sejam flexíveis; e
- ao mesmo tempo, mantenham ou melhorem a qualidade dos produtos, dos serviços ou ambos.

Em dez anos, pelo menos um quarto de todo o conhecimento actual estará ultrapassado. A vida útil das novas tecnologias é de dezoito meses e este tempo diminui rapidamente. Os

métodos antigos de reciclagem, reformulação ou revisão de princípios convencionais já não funcionam. As Administrações Aduaneiras, em particular, devem mudar caso pretendam dar resposta razoável à evolução considerável das práticas e tendências do comércio internacional.

Devem responder às quatro questões essenciais seguintes:

1. O que valorizam realmente os utilizadores (importadores, exportadores, transportadores, declarantes)?
2. A administração deve mudar para ter em conta a resposta a esta questão?
3. Como é que as mudanças beneficiarão a instituição?
4. Como é que as mudanças nas Alfândegas irão satisfazer necessidades governamentais mais abrangentes?

3.1.1. As dez etapas na implementação de mudança

Primeira etapa: Examinar particularmente as operações práticas e não a função.

É fundamental que as Alfândegas identifiquem as funções que advêm das suas responsabilidades, mas uma vez realizada esta tarefa, a atenção deve estar virada aos procedimentos necessários para desempenhar estas funções, pois estes são os meios mediante os quais a administração interage com os seus utilizadores.

Segunda etapa: Desenvolvimento de um perfil de processo

A maior parte dos processos de uma administração não são documentados, o que torna extremamente difícil avaliar precisamente as necessidades de melhorias. Ao documentar os processos, as Alfândegas devem tratar de respeitar a regra 80–20. A aplicação deste conceito é extremamente útil quando aplicado às iniciativas de melhoria, porque:

- 20% dos processos consomem 80% dos recursos;
- 20% das actividades num processo geram 80% dos resultados; e
- 20% dos problemas num processo representam 80% das oportunidades de melhoria.

A administração pode rapidamente identificar os poucos processos essenciais que consomem mais recursos através do desenvolvimento de um perfil de processo, com diagramas de actividades e fluxos de processos.

Terceira etapa: Mapeamento dos processos

Os processos são novos ou foram evoluindo? Na maioria das Administrações Aduaneiras, os métodos de trabalho foram elaborados há anos e nunca houve tempo para revê-los ou reestruturá-los. Tudo o que tenha sido documentado já mudou há bastante tempo. Como resultado, a maioria dos funcionários nunca teve acesso a uma representação visual do seu trabalho e não sabe o que é feito antes e depois do seu trabalho. Não têm conhecimento de como se enquadram na estrutura da instituição. O mapeamento dos processos é uma imagem visual da forma como o trabalho é realizado, demonstrando:

- como são realizados os trabalhos do princípio ao fim;
- quem executa os diferentes trabalhos;
- a sucessão das diferentes tarefas e a repetição de actividades; e

- as decisões tomadas e a informação de suporte.

Quarta etapa: Avaliar os métodos de trabalho

A avaliação dos métodos de trabalho permite às Alfândegas determinar os actuais níveis de desempenho e estabelecer objectivos de melhoria quantificáveis. Existem sete critérios quantitativos que permitem determinar a eficácia da maioria dos métodos de trabalho:

- custo do método utilizado: o custo total de cada tarefa realizada;
- custo unitário das tarefas realizadas: o custo total de cada tarefa concluída;
- *(*produção concluída à primeira*)*: a percentagem de tarefas realizadas sem repetição, revisão ou rejeição;
- custo de repetição do trabalho: o custo associado ao trabalho necessário para resolver os problemas encontrados;
- prazo de tratamento: o tempo necessário para realizar uma tarefa (minutos, dias, semanas ou meses).
- prazo real de tratamento: o tempo gasto para realizar uma tarefa sem espera nem repetir o trabalho;
- *(*intervenientes no processo*)*: o número de pessoas encarregadas de realizar uma tarefa e as actividades que cada uma realiza.

Quinta etapa: Estudar os processos de outras Administrações Aduaneiras

As ideias ou os métodos de trabalho comprovados em outras Administrações Aduaneiras podem fornecer informação valiosa, poupar tempo e possivelmente evitar erros.

Sexta etapa: Reestruturar os métodos de trabalho

Utilizando a informação reunida das cinco etapas anteriores, as Alfândegas podem agora definir novos métodos de trabalho, eliminando redundâncias e duplicação de actividades.

Sétima etapa: Equilibrar os métodos de trabalho com a tecnologia

Na maioria das administrações, os sistemas de informação estão estreitamente ligados à forma como o trabalho é feito, mas a tecnologia deve ser vista como uma ferramenta e não como o motor da mudança. Informatizar um processo manual não tornará necessariamente a Administração Aduaneira mais produtiva e informatizar um processo ineficaz conduz simplesmente à obtenção mais rápida de fracos resultados. Ao melhorar os processos e ao explorar as tecnologias, as Alfândegas devem assegurar-se de que a revisão dos referidos processos seja feita previamente, para que as recomendações tecnológicas sejam baseadas nas suas constatações.

Oitava etapa: Gerir a mudança de métodos de trabalho

As Alfândegas devem gerir a mudança mediante identificação e avaliação prévias dos riscos associados. A mudança pode ter várias consequências e as Alfândegas devem concentrar-se naquelas que são:

- altamente desejáveis, mas improváveis caso não sejam tomadas certas medidas;
- altamente indesejáveis, mas muito prováveis caso não seja prestada a atenção

suficiente.

Nona etapa: Preparar os funcionários e os utilizadores para a mudança

Não há administração tão má que alguém não goste dela tal como é. A maior parte das pessoas resiste à mudança com receio do que o futuro possa trazer, e não por estarem realmente apegadas ao passado ou aos métodos de trabalho actuais. O papel dos que dirigem a mudança é difícil e ingrato. Há poucos cursos de formação disponíveis e poucos modelos em que se possam apoiar. Os funcionários podem precisar de ser dirigidos através de um processo de três fases antes da aceitação incondicional de uma iniciativa de mudança.

1.CABEÇA:

As pessoas entendem racionalmente a necessidade de mudança com base nos dados de suporte. Uma participação tão ampla quanto possível ajudará a compreendê-la melhor.

2. CORAÇÃO:

As pessoas estão emocionalmente envolvidas na mudança, porque vêem as possibilidades de desempenho.

3.PÉS:

As pessoas envolvem-se mais enquanto participantes e não tanto como observadores.

A duração de cada fase irá variar dependendo do indivíduo e da situação.

Décima fase: Continuar a melhoria dos métodos de trabalho

A redefinição dos métodos de trabalho é morosa, onerosa e árdua. Apesar de, por vezes, a mudança se impor, uma cultura de melhorias contínuas aos métodos de trabalho assegurará que pequenas melhorias ocorram frequentemente e as grandes mudanças ocorram com menos frequência. As tarefas de todos os funcionários devem incluir:

- ponderação contínua da situação, avaliando os métodos de trabalho tendo em conta o ponto de vista do utilizador;
- identificação de oportunidades de melhoria, concentrando-se nas melhorias que permitam obter os melhores resultados;
- acção imediata quando as oportunidades de melhoria são identificadas e oferecem resultados concretos e rápidos;
- avaliação dos resultados, transformando as mudanças introduzidas aos métodos da trabalho em resultados quantificáveis.

Não existe fórmula mágica para a criação e manutenção de uma boa gestão de mudança. As Alfândegas devem estar constantemente em alerta visando a melhoria tendo em conta os desafios e oportunidades do dia-a-dia.

3.1.2. Porque é que a mudança falha

Informação e comunicação inadequada – a baixa qualidade de comunicação e da partilha de informações com as partes interessadas são muitas vezes a origem na falha da gestão da mudança.

As mudanças levam muito tempo e custam caro: quando a mudança arrasta-se por um longo período de tempo, perde-se o foco, o financiamento e o ímpeto.

Os riscos são desconhecidos: todas as mudanças significativas apresentam riscos. Se estes não forem claramente identificados, criará um sentido de incerteza, ambiguidade, e receio de falhar.

A metodologia não é comprovada: a mudança é difícil e complicada. É pouco provável que a mudança seja bem sucedida se o processo seguido for desconhecido e os seus agentes aprenderem na medida em que prosseguem.

Os recursos são insuficientes: uma mudança bem sucedida requer um Plano de Gestão de Recursos para assegurar-se de que o número dos recursos exigidos seja identificado e um Plano de Recrutamento para assegurar-se de que os melhores recursos disponíveis sejam utilizados. Contudo, estes recursos são por vezes os mais difíceis de obter.

O foco é interno: muitas mudanças são influenciadas por factores internos e não externos. Se não se tiver em conta as necessidades dos utilizadores, existe muito pouca oportunidade de êxito.

A mudança causa interrupções: no passado, algumas administrações podiam suspender a realização de determinadas operações enquanto realizavam as mudanças. Hoje, dado o ritmo acelerado que a alfândega enfrenta, todos devemos operar continuamente, pois é impossível parar o trabalho enquanto são feitas alterações nos métodos de trabalho. Daqui resulta que é importante fornecer pessoal suficiente para que nada seja alterado enquanto as novas operações também continuarem. Pode-se argumentar que os resultados não são bons quando a mudança interrompe a actividade normal e a produtividade sofre, ou se os funcionários não participam das mudanças, ou seja, eles não podem realizá-las. tarefas antigas ou novas tarefas.

3.1.3. Como assegurar que a mudança tenha êxito

Acelerar o ritmo: as pessoas que dirigem a mudança, bem como as pessoas afectadas pela mesma, devem observar rapidamente resultados concretos.

Utilizar uma metodologia comprovada: uma metodologia comprovada com agentes de mudança experientes evita que o processo de mudança avance às cegas. Os benefícios são claramente definidos e comunicados e as pessoas trabalham mais para ultrapassar as barreiras da mudança quando vêem os seus esforços resultar em benefícios concretos.

Foco no utilizador: o utilizador será o maior crítico para com a administração. Assim, se ele valorizar a mudança da administração isto significará que a mudança teve êxito.

Assegurar-se de que as interrupções sejam minimizadas: a mudança mal gerida e sem recursos pode ser tão perturbadora a ponto de paralisar a capacidade de funcionamento da administração.

Em resumo, no sentido de assegurar-se de que qualquer mudança terá êxito, devem ser respeitados os seguintes imperativos:

- articulação da necessidade da mudança para a administração;
- uso de um quadro estruturado;
- criação de equipas de suporte para gerir e implementar a mudança;

- selecção dos métodos de trabalho correctos que devem ser alterados;
- entendimento dos riscos e preparação de planos de contingência; e
- envolvimento e educação do pessoal e dos utilizadores no processo de mudança.

3.2. Quem deve desenvolver o sistema?

A introdução da informatização numa Administração Aduaneira é uma tarefa complexa e altamente especializada. Assumindo que pode haver falta de pessoal devidamente qualificado e formado na administração, deverá ser cuidadosamente considerada a questão de quem realmente fará o trabalho.

Existem geralmente três possibilidades: recrutar pessoal devidamente qualificado, formar os funcionários aduaneiros já existentes ou contratar consultores externos. Existem prós e contras para cada uma destas escolhas.

O recrutamento de pessoal qualificado em informática apresenta muitos problemas, porém permite que o trabalho projectado seja realizado relativamente rápido. Os níveis salariais devem ser bastante competitivos para atrair pessoal suficientemente qualificado. Isto pode ser uma fonte de tensões entre os novos peritos informáticos e o pessoal operacional existente que pode exercer uma influência nociva sobre o êxito do projecto.

Formar funcionários aduaneiros existentes como analistas de sistemas informáticos, programadores e operadores pode oferecer melhores soluções na medida em que poderão transportar a sua experiência aduaneira para apoiá-los a resolver os problemas que possam encontrar. Contudo, pode ser difícil manter estes funcionários logo que estejam qualificados como profissionais informáticos após um investimento público considerável no recrutamento e formação. Será necessário uma política salarial apropriada para evitar o desvio do pessoal assim formado para as empresas privadas.

A última possibilidade é a contratação de uma empresa de consultoria externa para apoiar e aconselhar em estudos de viabilidade, selecção de equipamentos, configuração de sistemas e programação.

As organizações que se informatizam pela primeira vez optam geralmente por uma solução *"chave na mão"* e realizam concursos públicos, baseados num estudo de viabilidade para um sistema operacional completo.

As administrações com pessoal próprio e especializado em TI podem realizar concursos para o fornecimento de *hardware,* sistemas de comunicações e *softwares*, mas podem optar pelo desenvolvimento das suas próprias aplicações de *software*.

Nestas situações os concursos públicos estariam abertos:

- aos fabricantes de computadores com *softwares*;
- aos fabricantes de computadores sem *softwares*;
- às empresas de *softwares*;
- às empresas de sistemas;
- aos serviços de tratamento de dados em lote;
- aos serviços que funcionam em tempo partilhado;
- a uma combinação do que foi mencionado acima.

As propostas a serem submetidas devem incluir:

- uma estimativa do custo da configuração detalhada do sistema;
- uma estimativa do custo da programação dos computadores;
- custos de formação (para os técnicos de manutenção do sistema);
- custos de *hardware*;
- custos de comunicação;
- custos de manutenção;
- um calendário para a implementação;
- historial e experiência da empresa.

Em seguida, os gestores das Administrações Aduaneiras precisarão de avaliar as diversas propostas e seleccionar uma empresa para configurar, programar, testar, instalar e implementar o novo sistema. O controle por um comité directivo é essencial em todas as fases do processo de desenvolvimento. A melhor escolha para a instalação de um sistema *"chave na mão"* será usualmente uma empresa devidamente estabelecida com reputação internacional. Enquanto que a opção *"chave na mão"* tem a probabilidade de ser cara mas os resultados poderão surgir mais cedo em relação às duas outras soluções internas.

De modo geral é conveniente estabelecer uma secção de TI na administração mesmo quando a informatização estiver a ser desenvolvida por consultores externos em bases de *"chave na mão"*. Esta secção, composta por funcionários aduaneiros, deve assegurar a ligação entre os consultores e o pessoal aduaneiro operacional. Logo que o sistema estiver instalado e os consultores tenham partido, a secção de TI será responsável pela manutenção. Portanto, é importante que o pessoal da respectiva secção seja devidamente formado em TI pelos consultores externos ou por quaisquer outros.

3.2.1 Escolha de uma empresa de consultoria

Nos casos em que as Alfândegas decidam contratar consultores, o processo de selecção deve merecer consideração cuidadosa. Uma escolha errada pode vincular a administração a um contrato prolongado, com resultados pouco rentáveis em relação aos valores investidos. A maioria das firmas internacionais de consultoria de gestão já fazem consultoria em informática como parte dos seus serviços e tais firmas provavelmente oferecem a opção mais segura. O seu principal trabalho é de aconselhamento, ajuda na escolha de um sistema específico e, possivelmente, elaboração do *software*. Podem também ajudar na concepção dos contratos a serem adjudicados por concurso público e na avaliação das propostas. Ajudam a recrutar pessoal e podem manter a sua colaboração até que o sistema seja finalmente implementado.

Os consultores externos podem evitar o envolvimento nas políticas internas de uma administração que pode muitas vezes dificultar ou atrasar o trabalho das equipas internas de desenvolvimento de sistemas. Os consultores externos devem, além disso, ser informados de maneira apropriada, e em tempo oportuno, para que se possam adaptar à complexidade do ambiente aduaneiro.

Os bons consultores não são baratos, mas podem tornar-se rentáveis para as administrações sem a capacidade necessária. Os termos do contrato devem assegurar que, no momento da partida dos consultores, o pessoal de TI da administração esteja devidamente formado para substituí-los.

3.3. O Comité Directivo

Uma componente essencial no processo de planificação é um Comité Directivo de Projecto que tem por função iniciar, orientar e rever os projectos de informatização. O Comité Directivo deve ter representantes de todas as áreas da administração susceptíveis de serem afectadas. O gestor de processamento de dados, se houver um disponível na administração, deve ser membro, juntamente com o gestor superior, proveniente de uma secção do departamento de finanças e contabilidade. O Presidente do Comité Directivo deve ser um membro da gestão superior, de preferência, o Director-Geral das Alfândegas ou o seu adjunto, uma vez que as decisões de informatização devem ser entendidas e apoiadas ao mais alto nível, caso se pretenda que sejam implementadas satisfatoriamente.

Em muitas administrações, os representantes da gestão no Comité Directivo podem não possuir qualquer conhecimento técnico pormenorizado dos problemas e necessidades de processamento de dados. Portanto, pode ser conveniente para o pessoal sénior participar em sessões formais de formação em TI, particularmente destinadas para a gestão e o pessoal nas áreas do utilizador, para ajudá-los a apreciar o tipo de problemas prováveis de ocorrer nas operações de TI. Pode também ser necessário contratar um consultor independente para integrar o Comité Directivo no sentido de aconselhar a gestão em várias fases de desenvolvimento do sistema.

3.4. Tipos de planificação

Na maioria das administrações, incluindo as Alfândegas, a planificação para fins de TI pode ser dividida em três categorias:

1. Planificação estratégica …… (ponto 3.4.1)

2. Planificação de projecto …….. (ponto 3.4.2)

3. Planificação da continuidade das actividades …… (ponto 3.4.3)

3.4.1. Planificação estratégica

Em todas as Administrações Aduaneiras existe um conjunto de regras de funcionamento que reflectem os processos das actividades aduaneiras**.** Estas regras de funcionamento determinam a execução de todos os processos e influenciam a estrutura organizacional da Administração Aduaneira.

A estrutura organizacional deve garantir que a aplicação de todas as regras institucionais sejam realizadas de uma maneira controlada, por exemplo controle de actividades, controle de finanças, controle de pessoal, organização de infra-estrutura de chaves públicas (ICP), etc. A estrutura organizacional influencia a segurança de TIC da Administração Aduaneira.

A planificação estratégica implica o desenvolvimento do plano da administração de informatização a longo prazo. As aplicações individuais podem ser informatizadas sem qualquer plano de longo prazo, mas não pode haver garantia de que resolverão os problemas da administração da maneira mais eficaz ou de que serão compatíveis com qualquer outro sistema interno que possa ser desenvolvido futuramente. Uma vez que uma administração opte por uma determinada via e se torne cada vez mais dependente de um sistema informático, ela poderá considerar muito difícil e oneroso mudar de direcção. Visto que na maioria das administrações, a introdução de sistemas informáticos afectará grande parte da organização, é essencial que se adopte uma política integrada caso se pretenda que a informatização prossiga de uma maneira lógica e coerente, evitando sobreposição de sistemas e minimizando os custos.

O plano estratégico ou o plano de longo prazo da administração, que faz geralmente parte do estudo de viabilidade ou é apresentado imediatamente após a sua conclusão, deve ser submetido ao Comité Directivo para apreciação e aprovação. Uma vez aprovado o plano, o Comité será responsável pela monitorização e orientação da sua implementação. Este definirá prioridades aos diversos projectos definidos no plano e avaliará os pedidos formulados pelos utilizadores ou a inclusão de novos projectos.

O plano estabelecerá os objectivos de políticas de TI da administração e identificará as aplicações informáticas necessárias para o alcance destes objectivos, juntamente com uma sequência lógica para o seu desenvolvimento e uma descrição dos seus limites e interfaces mútuos. Serão igualmente especificados aspectos técnicos de *hardware*, linguagens de programação, etc.

3.4.2. Planificação de projectos

O plano estratégico ou de longo prazo compreenderá vários projectos, cada um dos quais necessitará de uma planificação e controle individuais. Os projectos serão frequentemente atribuídos a equipas individuais de projectos, devendo os seus líderes informar periodicamente o Comité Directivo. Alguns Comités de projectos podem trabalhar sob a presidência do líder de projecto que prestará contas ao Comité Directivo. Quando uma equipa de projecto tiver concluído um plano/projecto de longo prazo, ser-lhe-á atribuído um novo projecto pelo Comité Directivo.

A planificação de projectos individuas é necessária para:

- definir com precisão os objectivos do projecto e identificar quaisquer obstáculos;
- estabelecer os limites do projecto;
- identificar a relação com os outros projectos ou sistemas quer existentes, quer propostos;
- estabelecer um calendário a especificar o que tem de ser feito, por quem e quando e qual será o custo.

A maneira mais fácil de planificar e controlar um projecto de informatização é dividi-lo em fases mais fáceis de gerir. A maioria dos projectos de informatização compreenderá três fases essenciais:

1. Fase de iniciação do projecto;
2. Fase de desenvolvimento;
3. Fase pós implementação.

A fase de iniciação geralmente compreende o estudo preliminar e o estudo de viabilidade descrito no Capítulo 5. Esta fase termina quando o Comité Directivo autoriza o início do projecto.

A fase de desenvolvimento compreende as etapas seguintes:

- investigação e análise detalhadas do sistema actual ……(ponto 5.1)
- descrição detalhada do sistema ……(ponto 5.2)
- programação ……(ponto 5.3)
- aquisição e instalação de hardware ……(ponto 5.4)
- implementação do sistema ……(ponto 5.5)
- avaliação ……...(ponto 5.6)

Muitas das etapas acima mencionadas são levadas a cabo sequencialmente e outras em paralelo. Por exemplo, a aquisição e o teste de *hardware* serão efectuados durante as fases de configuração detalhada e de programação, embora a aquisição e a instalação de *hardware* possam ser projectos individuais

A fase pós implementação abrange a manutenção contínua do sistema e a avaliação pós implementação.

A planificação efectiva de um projecto de informatização requer que uma determinada quantidade de recursos seja atribuída em cada etapa, devendo incluir prazos acordados e distribuições de recursos para sua execução. O progresso do projecto é examinado em relação aos seus pontos-chave ao longo de todo o seu desenvolvimento. Quaisquer desvios do plano são identificados e são tomadas medidas para os rectificar. O Líder de Projecto (ou Comité de Projecto) avaliará constantemente o progresso em relação ao plano e informará o Comité Directivo em intervalos previamente acordados. Em algumas ocasiões o Comité Directivo pode apenas destinar mais recursos ao projecto se as fases anteriores foram cumpridas correcta e tempestivamente.

A planificação de um projecto de informatização não é uma tarefa fácil. É particularmente difícil em organizações que introduzam as tecnologias de IC pela primeira vez. Qualquer administração que leve a cabo um processo de informatização sem um plano de acção claro, quer a longo prazo, quer a nível do projecto individual, irá muito rapidamente notar que perdeu a sua trajectória e desperdiçou um montante considerável de dinheiro público. Embora a planificação e o controle de projectos não garantam o êxito, permitem que a gestão mantenha um controle rigoroso dos recursos atribuídos e minimizam o risco de custos avultados ou desperdícios de tempo.

Aconselha-se as Alfândegas a ponderar a utilização de quadros padronizados para gerir os projectos, e nomeadamente os projectos de TIC a grande escala. Além das iniciativas tradicionais de gestão dos projectos, diversas metodologias e quadros foram desenvolvidos, apoiados por peritos acreditados. O PRINCE2 é um exemplo de iniciativa estruturada de gestão dos projectos. Quadros como o HERMES podem ser utilizados para gerir projectos de programas informáticos.

3.4.3. Planificação de continuidade das actividades

A planificação de continuidade das actividades constitui o processo global de desenvolvimento de um plano de acção de modo a garantir a continuação das actividades na eventualidade de uma indisponibilidade inesperada de um sistema ou instalação crucial. Para as Alfândegas significa a capacidade de uma administração manter a arrecadação dos direitos e demais imposições, o controle das mercadorias e pessoas que atravessam fronteiras e a autorização de saída ininterrupta e célere de pessoas e bens no comércio e tráfego internacionais.

As Administrações Aduaneiras devem sempre preocupar-se com a continuidade das actividades, caso os sistemas ou processos aduaneiros de TI não sejam capazes de funcionar:

- as mercadorias não desembaraçadas podem obstruir partes essenciais da infra-estrutura de um país;
- a impossibilidade de avaliar os riscos pode representar um risco específico para a sociedade;
- podem aumentar as tentativas de importação de mercadorias sujeitas a restrições;
- o público e os operadores comerciais podem ser incapazes de obter a informação que necessitam;

- o cálculo dos direitos e demais imposições pode ser errado; e
- pode haver erros na arrecadação e na contabilização dos direitos e demais imposições.

Por estas e muitas outras razões as administrações aduaneiras precisam de implementar planos de continuidade sólidos. Caso contrário, os transtornos para os operadores comerciais e a comunidade em geral prejudicariam em grande parte a economia nacional ou regional e restringiriam a aplicação da lei e a disponibilidade de bens essenciais para a população.

Embora a planificação da continuidade de actividades deva, como é de se esperar, ser parte integrante da gestão de uma Administração Aduaneira, nem todas as administrações implementaram o referido plano.

Um plano de continuidade de actividades irá requerer uma série de planos de contingência para cada actividade fulcral do processo e componente de infra-estrutura. Cada plano deve fornecer uma descrição dos recursos necessários, o papel de todas as categorias do pessoal, prazos e procedimentos necessários para a sua implementação. O processo abrange quatro etapas:

- Iniciação
- Análise de risco e impacto sobre a actividade
- Desenvolvimento de planos individuais
- Gestão dos planos

Etapa 1: Iniciação

- Obter o compromisso da gestão superior
- Estabelecer as políticas e o âmbito para a gestão de continuidade das actividades
- Estabelecer um Grupo de Trabalho de Planificação de Continuidade das Actividades
- Desenvolver um programa geral com metas

Etapa 2: Análise de risco e impacto sobre a actividade

- Definir cenários de possível falha
- Definir os níveis mínimos de resultados aceitáveis para cada actividade fulcral do processo
- Avaliar os impactos e os potenciais riscos desses cenários sobre as actividades
- Identificar e avaliar opções

Etapa 3: Desenvolvimento de planos individuais

- Identificar e documentar planos de contingência e modos de implementação
- Definir mecanismos para a activação dos planos
- Atribuir recursos para cada actividade fulcral do processo
- Obter aprovação dos gestores e alocação de recursos

Etapa 4:Gestão dos planos

- Distribuir os planos a todos os intervenientes relevantes
- Manter actualizados planos, procedimentos e estratégias
- Prestar atenção à formação e à sensibilização, rever os planos e os riscos, testar os planos e controlar as mudanças de estratégia e de planos para que estes sejam compatíveis
- Formar o pessoal para apresentar estratégias e planos, bem como realizar as acções incorporadas no plano
- Garantir a qualidade e aplicabilidade em relação à adaptabilidade, exactidão, qualidade de dados, eficiência, facilidade de implementação/manuseio (muito importante visto que o plano só será usado em momentos de caos ou falha), sustentabilidade, portabilidade, fiabilidade, resistência, segurança, possibilidade de ser testado e aplicado em tempo oportuno, bem como a aprovação dos gestores.

As Administrações Aduaneiras precisam de obter o compromisso dos Ministros e dos responsáveis dos serviços, reconhecendo os elementos essenciais da Planificação de Continuidade das Actividades.

Precisa de haver um Gestor de Plano de contingência com responsabilidade global pelo plano de continuidade de actividade. Visto que o plano afecta a sobrevivência de toda a organização, o gestor tem de ser um funcionário superior com autoridade suficiente para garantir que as actividades sejam realizadas, obter e distribuir os recursos necessários e coordenar as diferentes medidas. Os pormenores do plano devem ser providenciados a partir de áreas individuais de actividades.

Pode ser necessário indicar coordenadores regionais ou de áreas para gerir as diferentes medidas de âmbito local se e quando o plano de continuidade das actividades for invocado. Os planos individuais irão prescrever as acções para combater riscos específicos. É aconselhável identificar indivíduos com competência técnica apropriada para gerir estas actividades.

Os detalhes sobre como levar a cabo a planificação de continuidade das actividades podem ser obtidos das Directivas de Planificação de Continuidade da OMA.

3.5. Elaboração de uma arquitectura empresarial

A decisão de informatizar carece de uma planificação escrupulosa por parte dos diferentes níveis da organização. A Secção 3.4 evoca os diferentes tipos de planificação, e nomeadamente a planificação estratégica, a planificação de projectos e a planificação da continuidade das actividades. A elaboração da «arquitectura empresarial» faz parte da planificação estratégica que visa introduzir a Tecnologia da Informação e da Comunicação. A fim de contribuir para o processo de gestão estratégica da «empresa», é necessário produzir e actualizar os planos de organização pertinentes.

A arquitectura empresarial visa estabelecer ligações directas entre os imperativos comerciais da empresa e as inovações tecnológicas. Por intermédio da implementação dessas ligações, a organização trata de alinhar os seus objectivos comerciais e as soluções das tecnologias da informação. Isto favorece uma utilização optimizada dos recursos e a identificação dos recursos que não contribuem para os objectivos comerciais da organização. A ausência de solução arquitectural pode conduzir à proliferação de projectos que não resolvem os problemas da organização, de soluções que se sobrepõem de infra-estruturas inúteis que não contribuem

em nada para a materialização dos objectivos da instituição. A arquitectura empresarial permite uma utilização mais eficaz das TIC, garantindo um melhor rendimento dos activos e um custo total de propriedade menor. Por natureza, é arriscado investir nas tecnologias da informação sem dispor de uma arquitectura empresarial.

A arquitectura empresarial tem diferentes perspectivas e descrições arquitecturais que sustentam a planificação de alto nível para soluções prevendo o recurso às Tecnologias da Informação. Diferentes quadros padronizados oferecem uma descrição dos pontos de vista arquitecturais. Por exemplo, o modelo de arquitectura do Departamento Americano da Defesa (chamado DODAF) utiliza três pontos de vista: trata i) o *ponto de vista das operações* que identifica as actividades por realizar e quem as realiza, ii) o *ponto de vista dos sistemas* que define os sistemas que respondam às necessidades operacionais focando-se nas trocas de informações, e iii) o *ponto de vista das normas técnicas* que define as normas, notações e convenções técnicas aplicáveis. Esses três pontos de vista são interdependentes e contribuem, em conjunto, para o quadro final.

As descrições da arquitectura da empresa têm a *arquitectura operacional* ou de *empresa* que descreve as funções da organização e a maneira como as tarefas são realizadas. Por exemplo, onde e como um funcionário aduaneiro realiza a verificação documental e a inspecção das mercadorias? Quem se encarrega do controle na Estância Aduaneira e que ferramentas utiliza? Como é que essas actividades beneficiam a organização? A arquitectura da informação dá uma imagem global do fluxo da informação tanto no interior da empresa como entre as diferentes empresas. Ela tem também o modelo conceitual subjacente de dados. O inventário dos aplicativos de *software* que permitem atingir os objectivos e as missões operacionais da organização faz parte da *arquitectura de aplicação*.

Esta abordagem da arquitectura descreve como os aplicativos articulam-se entre si e inscrevem-se no objectivo operacional global da organização. A plataforma de *software* que se encarrega da mediação entre os aplicativos é chamada *middleware* ou *software* das camadas intermediárias e fornece o ambiente de *software* necessário para a execução dos aplicativos. A *arquitectura tecnológica* gere esses problemas e rege outras arquitecturas como as que estão ligadas à segurança e aos *softwares*. Estes pontos de vista arquitecturais podem ajudar a aproximar diversos grupos no seio de uma organização e contribuir para a criação de um consenso relativamente às necessidades comuns. Ajudam os participantes no projecto a compreender elementos concretos quanto ao que foi convencionado para o futuro e quanto à maneira de proceder.

O Quadro «*Open Group Architecture*» (TOGAF) é um quadro de arquitectura empresarial que oferece uma abordagem global para a concepção, a planificação, a implementação e para governar uma arquitectura de informação de empresa. No âmbito da implementação da Janela Única, um documento produzido pela CESAP/ONU e a CEE foi desenvolvido com base no conceito *TOGAF Enterprise Architecture*. O TOGAF é uma disciplina bem conhecida sustentada por um corpo/grupo vasto e diversificado de profissionais.

As presentes Directivas recomendam que, no âmbito da planificação estratégica da informatização, as Administrações Aduaneiras invistam na arquitectura empresarial e façam conhecer aos planificadores/planejadores do projecto e das operações as descrições e os pontos de vista arquitecturais pertinentes. Trocas profundas sobre o conceito e a aplicação da arquitectura empresarial podem ser consultadas no Capítulo 8 do Compêndio da OMA referente ao reforço das capacidades (publicado pela OMA em 2009) bem como no Capítulo 6 do Volume 2 do Compêndio da OMA intitulado «Como construir um ambiente de Janela Única» (publicado em 2011).

4. A importância das consultas

(Normas Transitórias 6.10 e 7.1)

Os sistemas aduaneiros informatizados não podem ser desenvolvidos com êxito sem a cooperação e boa vontade de um grande número de pessoas. É particularmente importante consultar dois grupos antes, durante e depois do desenvolvimento de um sistema aduaneiro – a comunidade empresarial e o pessoal aduaneiro que fará uso do novo sistema.

4.1. A comunidade empresarial

Uma vez que a maioria dos sistemas aduaneiros informatizados exercerá um grande impacto sobre os operadores comerciais, a consulta a estes é essencial para garantir maiores benefícios. Pode ser formado um Comité Consultivo ou de Aconselhamento formal para opinar sobre questões práticas e manter os parceiros comerciais informados sobre os planos das Alfândegas. Outras administrações governamentais interessadas, importadores, exportadores, transportadores, transitários (agentes de carga), despachantes, autoridades portuárias e aeroportuárias, etc, devem estar representados neste Comité.

4.2. Pessoal Aduaneiro

Qualquer sistema informatizado novo pode encontrar resistência do utilizador baseada numa reacção humana natural que resiste à mudança e tenta preservar oestado *quo*. Isto é facilmente ultrapassável e a eficácia cabal do sistema é obtida da melhor maneira mediante o asseguramento da participação e colaboração dos utilizadores em todas as fases introdutórias. Se um novo sistema é mal utilizado, geralmente é porque os utilizadores não o entendem devidamente ou porque não querem que funcione.

Se os utilizadores sentirem que o sistema não satisfaz às suas necessidades, a causa normalmente é devida a uma investigação inadequada do sistema ou à fraca percepção das necessidades dos utilizadores pelos analistas do sistema. Portanto, a participação dos utilizadores no desenvolvimento do sistema é de crucial importância visto que promove uma análise e uma configuração de sistema eficazes, facilita o entendimento e a confiança do utilizador e pode evidenciar potenciais áreas de dificuldades. Apesar da necessidade de participação do utilizador ser clara, a sua concretização não é tão simples.

Para que os utilizadores colaborem eficazmente devem saber que os seus empregos estão garantidos. Qualquer problema de ansiedade devido a esta questão deve ser dissipado de imediato. Os utilizadores devem confiar nos analistas de sistemas e acreditar nas suas capacidades. Por sua vez, os analistas de sistemas devem confiar nos utilizadores e estar preparados para aceitar as suas ideias.

Os utilizadores devem ser mantidos informados dos desenvolvimentos ao longo de todo o projecto. A falta de informação suscita rumores e descontentamento, criando um ambiente pouco favorável para a introdução de um novo sistema informático.

É necessário manter contactos regulares para garantir a confiança e colaboração do utilizador. Os utilizadores devem ser devidamente representados nas equipas e comités de projectos. Devem ser mantidas reuniões regulares de grupos de trabalho para encorajar os utilizadores a participarem na concepção do novo sistema. O seu conhecimento profundo e

entendimento dos sistemas manuais existentes permitirão fazer contribuições importantes em diversas áreas, por exemplo, disposição de escritórios, concepção de formulários, procedimento de rectificação de erros, apresentação de imagens em tela e de relatórios.

A educação é igualmente um elemento importante no fomento da confiança e colaboração do utilizador. A educação do utilizador assenta em duas categorias, a primeira é o conhecimento geral sobre tecnologia de informação e conceitos básicos de informática e a segunda é a formação detalhada sobre o sistema que está a ser desenvolvido. Nos casos em que uma empresa externa estiver a desenvolver o sistema, a formação do utilizador deve fazer parte das suas responsabilidades.

O êxito ou fracasso de um sistema depende em larga medida da colaboração do utilizador. Se os utilizadores forem informados, tranquilizados e envolvidos na configuração do sistema, as oportunidades de êxito são melhoradas de forma correspondente. Se forem alienados, o sistema fica condenado ao fracasso.

5. O processo de desenvolvimento do sistema

(Normas Transitórias 1.3, 6.8 e 7.3)

Uma vez adoptada uma solução determinada baseada no Estudo de Viabilidade e obtida a necessária aprovação financeira, o projecto segue para a fase de desenvolvimento e evolui de um sistema teórico para um sistema pronto a operar. A decisão sobre a quem compete a fase de desenvolvimento do sistema dependerá das disposições em vigor na administração relativamente ao pessoal da TI (ver 5.1).

Durante esta etapa, bem como em todas as outras, de desenvolvimento do sistema, a gestão deve exercer um controle rigoroso através do Comité Directivo, para assegurar-se de que o projecto prossegue conforme os prazos acordados e dentro do orçamento. Deve manter para além disso o referido controle sobre o produto obtido no final da etapa de desenvolvimento, isto é, os programas informáticos e a sua documentação de suporte.

Os programas informáticos reflectirão em pormenor os procedimentos que actualmente são realizados no ambiente de um sistema manual, por conseguinte, é essencial que sejam dados os passos necessários para assegurar-se de que estes reflictam exactamente estes procedimentos caso contrário, o sistema final não satisfará as necessidades do utilizador.

A fase de desenvolvimento do projecto deve ser dividida em sub-etapas para facilitar a participação do utilizador e o controle de gestão. O resultado de cada sub-etapa deve ser revisto pelo Comité de Projecto e pelo Comité Directivo antes da autorização para prosseguir para a sub-etapa seguinte. As diversas etapas deste processo são descritas mais adiante neste Capítulo.

5.1. Investigação detalhada e análise do sistema existente

Esta investigação dos procedimentos existentes não significa que a pesquisa inicial, realizada como parte do Estudo de Viabilidade foi imprecisa, mas precisará de ser mais aprofundada para fornecer bases de análise e de concepção detalhadas do novo sistema.

Nesta investigação detalhada, as tarefas principais do analista de sistemas serão entrevistar o pessoal a todos os níveis da administração e consultar manuais de procedimentos e qualquer outra documentação relevante e disponível. Uma vez reunidos todos os factos, ele analisará a informação reunida e elaborará uma Especificação de Sistema de Utilizador para ser submetida ao Comité de Projecto e, por último, ao Comité Directivo. Este documento descreverá em linhas gerais as características principais do novo sistema e como este afectará a gestão e o pessoal.

Nesta fase, o Comité de Projecto precisará de envolver totalmente os utilizadores do sistema no processo de desenvolvimento, para verificar a exactidão das informações reunidas pelos analistas de sistemas e que a configuração detalhada do novo sistema possa prosseguir sem necessidade de introduzir modificações posteriormente. Com efeito, o utilizador final do sistema precisará de dizer ao analista se o sistema a ser concebido responde às suas necessidades.

A Especificação do Sistema do Utilizador deve ser aprovada pelo Comité Directivo antes do início do trabalho pormenorizado de configuração e, uma vez acordado o conteúdo, não será necessário actualizá-lo. A Especificação do Sistema do Utilizador é muitas vezes a última

oportunidade do utilizador solicitar mudanças nos casos em que a configuração não satisfaça as suas necessidades. Uma vez aceite, a especificação é frequentemente "congelada" para que não sejam aceites modificações durante a fase final do projecto.

5.2. Configuração detalhada do sistema

A configuração detalhada do sistema começa logo que, após as análises, o Comité Directivo autoriza o desenvolvimento de um novo sistema.

As autorizações serão baseadas na configuração do sistema descrito no Relatório de Viabilidade acompanhado do levantamento das necessidades do utilizador na Especificação do Sistema do Utilizador. A configuração incluirá a especificação detalhada dos requisitos do processamento manual e informatizado, inserções feitas no sistema e os resultados obtidos, arquivos informáticos usados para armazenar informação e segmentação do processamento em programas.

O analista de sistemas apresentará os resultados deste trabalho de configuração em vários documentos, nomeadamente:

- Especificação do sistema
- Manual do utilizador
- Manual do administrador do sistema
- Dados de teste
- Instruções para migração do sistema

A especificação do sistema fornece aos programadores informáticos toda a informação sobre as funções informáticas necessárias para conceber os programas.

O Manual do Utilizador instruirá os departamentos de utilizadores sobre as operações correntes exigidas para o bom funcionamento do sistema e as medidas a serem tomadas em caso de falha ou erro. O Manual do Utilizador deve estar disponível para fins de consulta durante a vida operacional do sistema. Este deve sempre reflectir o actual estado do sistema e por conseguinte, precisará de ser actualizado quando forem feitas mudanças que afectem os procedimentos dos utilizadores. Os utilizadores que não tenham experiência em sistemas informáticos, geralmente não estão conscientes da importância do cumprimento rigoroso das instruções contidas no Manual do Utilizador. Deve-se ter cuidado para garantir tal consciência.

O Manual do Administrador é o documento de consulta permanente de que depende o departamento de operações informáticas, para a obtenção de informação sobre o sistema a ser implementado e as tarefas a serem realizadas para a sua operação de rotina.

Logo que os programas estejam concebidos e os utilizadores familiarizados com os novos procedimentos, o sistema precisará de ser testado para assegurar-se de que esteja a operar devidamente ao abrigo de todas as condições prováveis e que produzirá os resultados esperados. Serão necessários Dados de Teste para verificar se o sistema concluído satisfaz os técnicos e os utilizadores.

Por último, serão necessários dois tipos de instruções de migração; um para os departamentos de utilizadores e outro para o administrador do sistema. Isto especificará detalhadamente, os procedimentos necessários para a migração dos sistemas antigos para os novos.

Todos estes documentos serão revistos pelo Comité de Projecto e pelo Comité Directivo antes da autorização para o início da programação.

5.3. Programação

A tarefa de programação incluirá a configuração da estrutura do programa, configuração e documentação da lógica detalhada do programa, codificação, preparação de um plano de teste e dados de teste, teste (parte técnica) e localização e eliminação dos erros dos programas e preparação da documentação final.

O ponto de partida para a programação é a Especificação do Sistema que foi elaborada como parte da configuração detalhada do sistema. O programador testará os seus programas até certo ponto, mas todo o sistema, incluindo todos os programas, precisarão de ter as suas partes funcionais testadas e aceites pelo utilizador e, por último, aprovadas pelo Comité de Projecto e pelo Comité Directivo antes do início do sistema (ver Capítulo 12). Do ponto de vista da gestão, é essencial assegurar-se de que os programas informáticos sejam devidamente documentados. Em circunstância alguma devem ser aceites programas não documentados. Sem a documentação de suporte, os programas são praticamente ilegíveis e não podem ser modificados excepto pela pessoa que os concebeu.

Não se pode deixar de realçar que a documentação é uma parte fundamental de qualquer sistema. Existe também a necessidade dos programadores cumprirem com os padrões de programação acordados, caso contrário a manutenção pode se tornar um problema. Deve-se realçar aos programadores de que o necessário é que os programas funcionem devidamente e que possam ser facilmente modificados caso haja necessidade.

5.4. Aquisição e instalação de *hardware*

5.4.1. Aquisição

O *hardware* informático no qual o novo sistema será operado não foi mencionado com profundidade até ao momento. A aquisição de computadores não deve ser feita antes do Estudo de Viabilidade ou análise detalhada nem depois do sistema ter sido configurado e programado. Se for necessário um novo *hardware*, a aquisição é geralmente efectuada em paralelo com a fase de configuração do sistema.

As administrações devem ter cautela ao adquirir material de *hardware* caro antes de realizar um exame pormenorizado das suas necessidades em termos de informatização. A probabilidade é de que este equipamento não satisfará as suas necessidades e será simplesmente um ónus para as administrações. De igual modo, não é prudente adiar a aquisição para depois da programação do sistema. Isto prolongará simplesmente o programa de implementação do sistema informatizado. A maioria das organizações almeja ter o *hardware* informático disponível e instalado para coincidir com a etapa de programação até ao ponto em que os computadores sejam necessários.

Portanto, as administrações devem realizar o processo de aquisição de *hardware* com tempo suficiente de antecedência para garantir a disponibilidade de tempo. Adquirir um sistema informático significa adquirir três componentes básicos: *hardware*, *software* (sistemas e aplicações) e comunicações. Algumas Administrações Aduaneiras (em particular as que lidam com as tecnologias de IC pela primeira vez) optarão pela instalação de um sistema informatizado completo em bases *“chave na mão”.* O processo de aquisição de *hardware*, *software* de sistemas

e comunicações é discutido aqui independentemente do *software* de aplicação e não como parte de um pacote geral implícito na abordagem "*chave na mão*".

5.4.2. Pedido de Proposta (PP)

No sentido de adquirir o equipamento necessário, é usual que as administrações emitam um Pedido de Proposta (PP) a uma lista de vendedores identificados como capazes de estarem em condições de submeter propostas sérias. Contudo, antes de o fazer, será necessário elaborar um documento especificando as funções que o equipamento deve ser capaz de executar. Este documento é denominado Especificação Funcional. Em alguns casos, o Relatório do Estudo de Viabilidade pode conter já informação suficiente. Portanto, se não tiver, será necessário complementá-lo de forma a se assegurar de que contenha o mínimo da informação seguinte:

→ Requisitos obrigatórios

- Uma lista de todas as tarefas que o sistema informático deve poder realizar, incluindo os requisitos estabelecidos para estar em conformidade com os padrões informáticos;
- Requisitos de compatibilidade – se o sistema tiver de ser usado em conjunto com um outro sistema;
- Capacidade de actualização – se o volume de trabalho tiver probabilidade de aumentar ao longo do ciclo de vida do sistema;
- Recuperação do sistema na eventualidade de falha;
- Requisitos de segurança etc;
- Compiladores, *assemblers*, outras funcionalidades;
- Todos os requisitos de *software* de sistemas devem ser descritos.

→ Registo pormenorizado do volume de trabalho

- Uma descrição dos processos que serão realizados; volume de dados a introduzir; volumes de processamento; volume de armazenagem; tipo de armazenagem; (*on-line*, *off-line*); tempo de armazenagem; volumes máximos de actividades (para sistemas *on-line*); requisitos do tempo de resposta (para sistemas *on-line*); tempo de retorno (para sistemas em lote).
- Responsabilidades do vendedor
- Indicação de todas as responsabilidades do vendedor: planificação do local, instalações eléctricas, ar condicionado, prevenção de incêndios, fornecimento de corrente auxiliar, programas de instalação, tempo de informatização pré-instalação, demonstração de linhas de teste, pessoal de apoio no local de trabalho, necessidades de formação, e muito mais importante – requisitos de manutenção.

→ Fiabilidade

- A fiabilidade é geralmente expressa em termos da percentagem de tempo de operação programada. Se esta percentagem for muito elevada, por exemplo 99%; o vendedor terá que provavelmente propor um sistema duplo. Isto significará um grande aumento do custo, em particular se o contrato inclui uma cláusula de penalidade substancial para falhas excessivas. Por conseguinte, é melhor determinar a duração da falha (tempo de indisponibilidade) que seria aceitável no âmbito dos critérios de um sistema operacional sensível. É importante incluir penalidades no contrato para assegurar que o vendedor

providencie a manutenção e o equipamento adequados para se manter dentro dos critérios de fiabilidade estabelecidos.

→ Disposições contratuais

- Estas devem especificar as obrigações contratuais formais que deverão ser estabelecidas entre a administração e o vendedor escolhido. Especificarão questões como datas exactas de entrega, datas de pagamento, penalidades, resolução de litígios, serviços pós-venda, etc.

Para além das especificações funcionais que contêm todos os requisitos acima mencionados, será necessário submeter vários problemas "padrão de avaliação" aos potenciais fornecedores para assegurar-se de que o equipamento proposto para ser fornecido satisfaça realmente os padrões de desempenho exigidos. Um problema padrão de avaliação é uma versão simulada de uma aplicação informática típica que o vendedor pode operar no computador a ser fornecido. Os resultados farão parte da sua proposta final.

5.4.3. Avaliação das respostas aos PP

As propostas recebidas dos potenciais fornecedores são avaliadas pelo Comité Directivo (caso seja necessário com o aconselhamento profissional de um consultor especializado em avaliações das respostas) sob os títulos seguintes:

- Avaliação técnica
- Avaliação de custos
- Avaliação do padrão de avaliação

A avaliação técnica exigirá a análise das propostas para assegurar se estão de acordo com os requisitos obrigatórios estabelecidos no Pedido de Proposta.

A avaliação de custos irá comparar as ofertas dos fornecedores para: compra, arrendamento e arrendamento com a opção de compra. As várias opções de aquisição para cada fornecedor precisam de ser analisadas detalhadamente no sentido de identificar a solução mais económica. Os testes e as demonstrações ao vivo devem ser efectuados com cada fornecedor aprovado na avaliação técnica. Durante os referidos testes os dados de avaliação devem ser processados e os resultados devem ser recolhidos e apreciados.

Ao adjudicar contratos, devem apenas ser considerados aqueles cujo equipamento é aprovado nos testes de referência e que satisfaçam os requisitos técnicos obrigatórios. Devem ser realizadas negociações com cada um destes fornecedores com vista a garantir o melhor preço possível.

Depois de uma avaliação completa de todas as propostas, a administração deve estar em condições de seleccionar um fornecedor e o equipamento. Quando chegar o momento de elaboração do contrato, a administração deve insistir no sentido de que todas as circunstâncias especiais e ofertas de assistência e apoio técnico, bem como a manutenção do equipamento sejam incluídas no contrato. Se o fornecedor seleccionado prometer apoio adicional em etapas pós instalação, isto deve também ser cuidadosamente definido e incluído.

Enquanto que o método normal de pagamento do equipamento informático tem sido por locação financeira a partir do fabricante (*leasing*), estão também disponíveis planos de compra e de locação financeira junto de empresas financeiras independentes (*lease-back*). Os responsáveis superiores pelos serviços financeiros devem analisar cuidadosamente o impacto

financeiro destas várias opções sobre a organização. Para além disso, o contrato deve ser revisto por um jurista para assegurar se o mesmo oferece protecção adequada dos interesses da administração.

5.4.4. Instalação

A instalação dos computadores pode ser complexa e morosa. É fácil subestimar o tempo e os recursos necessários para realizar com êxito esta instalação. Os fabricantes de computadores podem fornecer uma lista abrangente das acções que precisarão de ser realizadas antes da entrega do *hardware*. Usando esta lista como base, deve ser estabelecido um plano para as actividades de pré-instalação necessárias demonstrando todas as suas interdependências relevantes. Estas actividades incluem:

- Plano de preparação do local
- Plano de colocação do pessoal
- Plano de comunicações de dados
- Programa de entrega
- Plano de apoio logístico

O plano de preparação dos locais inclui a determinação do centro de informática e os requisitos do espaço de armazenamento *(backups)*, a definição das necessidades de temperatura e humidade, de corrente eléctrica e de telefones e a definição de todos os requisitos especiais de meios informáticos tais como dispositivos anti-incêndio, protecções contra interferências eléctricas, protecções de segurança electrónica, fornecimento de corrente auxiliar, etc. Inclui igualmente a identificação das referidas necessidades de suporte, tais como mobiliário, porta-cassetes, tapetes, plataforma de observação para supervisão, equipamento de elaboração de relatórios.

O plano de necessidades de pessoal identifica todo o pessoal necessário para operar o centro de informática, quando deve iniciar as suas funções e as medidas de recrutamento e as acções necessárias para este efeito. Um centro de processamento de dados normalmente inclui: um gestor do centro de dados, operadores informáticos e supervisores, pessoal de apoio à programação de *software*, pessoal de preparação de dados, pessoal de controle técnico (se a aplicação informática incluir comunicações extensivas de dados) e operadores de máquinas de inserção de dados.

O plano de necessidades de pessoal mostra também quando terá início: a acção de recrutamento de novo pessoal, a capacitação do pessoal já existente, o enquadramento efectivo do pessoal e o desempenho das suas funções. O plano de necessidades de pessoal deve ser coordenado com o de aquisição do sistema informático, para garantir a disponibilidade do pessoal quando este for necessário.

O plano de comunicação de dados representa os requisitos de transmissão de dados e mostra quando e como é que os circuitos de dados, *modems* e concentradores serão instalados no sentido de suportar a operação do sistema.

Elabora-se um plano de apoio logístico para indicar as necessidades e a data a partir da qual elas deverão ser satisfeitas, nomeadamente para lidar com pessoal (recrutamento), transportes e mudanças, instalação de equipamento, assistência jurídica, etc.

A instalação do sistema é normalmente da responsabilidade do fornecedor do equipamento informático. Contudo, a preparação dos locais é normalmente da responsabilidade única da Administração Aduaneira e se o local não estiver pronto, o fornecedor do equipamento informático não será responsabilizado pelo atraso da instalação. De igual modo, se a preparação do local não estiver de acordo com as especificações do fornecedor e as diferenças forem significativas, geralmente, aquele não instalará o sistema até que as correcções do local sejam concluídas.

Uma vez instalado, o computador não será considerado operacional até que seja realizada uma série de testes para assegurar de que este opera a níveis satisfatórios por um período determinado. Este teste de aceitação é uma actividade fundamental que exige pessoal altamente qualificado. Se o referido pessoal não existir na administração é aconselhável que se contrate um consultor independente para a realização desta tarefa. Uma vez aprovado pelo teste de aceitação, o computador pode ser declarado “operacional”.

5.5. Implementação do sistema

O processo de desenvolvimento do sistema já atingiu uma fase em que o equipamento está instalado e os programas foram concebidos. A fase seguinte do processo é a “implementação”. Esta é, com efeito, composta por várias actividades ou sub-fases:

- Teste do sistema
- Conversão de arquivo
- Formação do utilizador
- Transição

5.5.1. Teste do sistema

Quando os programadores concluírem o seu trabalho, os programas e a documentação serão entregues às equipas de sistema para testar a parte técnica. Os testes de sistemas têm por objectivo principal identificar e corrigir quaisquer falhas que possam permanecer nos programas informáticos. Algumas falhas podem ser devido ao desentendimento entre o analista e o utilizador ou entre o analista e o programador. Se muitas falhas existirem devido à especificação incorrecta, é sinal de que as tarefas de investigação, análise e configuração não foram realizadas com a devida exactidão.

O plano e o programa de trabalho de testes do sistema devem ser elaborados pelos analistas de sistemas e aprovados pelo Comité de Projecto. Nos casos em que o sistema estiver a ser desenvolvido para as Alfândegas por consultores externos, o pessoal aduaneiro deve estar totalmente envolvido para se assegurar de que o sistema supre as suas necessidades. Os dados de teste preparados pelos analistas de sistemas durante a fase de concepção do sistema e que simularão com a maior proximidade possível as condições actuais de operação serão processados pelo computador. Os resultados do teste da parte funcional serão seguidamente comparados com os resultados esperados e quaisquer discrepâncias identificadas serão acompanhadas até à obtenção de resultados visíveis e eliminação de erros. Mesmo quando os testes de sistemas forem realizados para a satisfação de todos, pode ainda ser necessária a realização de testes adicionais no ambiente real.

5.5.2. Conversão de ficheiros

Esta é a tarefa de conversão de arquivos manuais em arquivos electrónicos, por outras palavras, trata-se de converter os dados de referência e outros, por exemplo; a pauta aduaneira, num formato electrónico legível. Esta é uma tarefa fundamental.

Eis alguns exemplos dos tipos de arquivos electrónicos que podem ser estabelecidos num sistema aduaneiro:

- Arquivo da pauta
- Arquivo de quotas
- Arquivo de moedas
- Arquivo de países
- Arquivo de importadores

Quando estes arquivos forem criados, serão necessárias actualizações constantes até que o sistema entre em produção e devem continuar a ser actualizados durante o ciclo de vida do sistema. Normalmente, o processo de conversão de arquivos exigirá a transcrição dos dados de origem numa forma adequada para inserção no computador. Após a criação dos arquivos deve-se verificar a sua exactidão visto que nada pode dificultar tanto o início de produção de um novo sistema como os dados errados nos arquivos principais. Este processo todo, que é oneroso e moroso, deve ser planificado cuidadosamente visto que condiciona o êxito de todo o sistema.

5.5.3. Formação do utilizador

Para que um sistema prove a sua eficácia, as pessoas que o operam devem ser devidamente capacitadas. A analogia com “o elo mais fraco da cadeia” é a mais apropriada aqui.

A formação dos utilizadores pode ser da responsabilidade da equipa de sistemas (nos casos em que o sistema é desenvolvido internamente), pode ser partilhada com o departamento de pessoal da administração ou pode ser da responsabilidade dos consultores externos encarregados pelo desenvolvimento do sistema.

São necessários dois níveis de formação do utilizador:

1. Conhecimento geral de informática;
2. Capacitação no uso do novo sistema.

Nos casos em que os utilizadores não possuem experiência em informática, a sua formação geral deve ter início o mais breve possível (quando o Relatório de Viabilidade for aprovado). A capacitação no uso do novo sistema deve ser ministrada o mais tardar possível para que os novos métodos e técnicas não sejam esquecidos antes da sua implementação. A duração máxima recomendada entre a formação técnica e a aplicação dos conhecimentos é de duas semanas.

A formação sobre o uso do novo sistema deve incluir:

- Visão geral da lógica do sistema.
- Inserção de dados.
- Interpretação dos resultados.
- Limitações e dificuldades do sistema.
- Medidas a tomar logo que os erros sejam detectados.
- Prática de uso de utilização de dados e arquivos de teste

5.5.4. Estratégia de transição

O sistema foi concebido, programado e testado, os arquivos foram convertidos e os utilizadores foram capacitados. É chegado o momento de utilizar o sistema em ambiente real.

Existem três estratégias básicas para mudar para o funcionamento real:

1. Funcionamento paralelo
2. Funcionamento piloto
3. Transição directa

O funcionamento paralelo é frequentemente o método de escolha para um sistema informatizado que substitui em todas as funções essenciais, um sistema manual em suporte papel. O sistema manual continua a operar inalterado quando o sistema informático é instalado pela primeira vez. O resultado dos dois sistemas é comparado, ponto por ponto, até que todas as discrepâncias sejam resolvidas. Este método é apenas possível se os dois sistemas forem idênticos em todos os resultados principais, e se o pessoal estiver disponível para continuar a explorar o sistema antigo enquanto que ao mesmo tempo prepara a inserção do novo e verifica os resultados.

O funcionamento piloto é muitas vezes o método preferido caso o novo sistema tenha de ser eventualmente instalado em vários locais – como ocorre muitas vezes nas Alfândegas. É escolhido um local típico para o funcionamento piloto, nos casos em que o departamento de processamento de dados e, em particular, a equipa de sistemas pode concentrar os seus recursos até que o sistema tenha sido testado sob condições reais de vida e todos os problemas maiores tenham sido resolvidos. O sistema pode, então, ser progressivamente introduzido em outros locais.

A mudança directa é a única alternativa, se nenhum dos outros métodos for adequado, para terminar um sistema antigo num dia e começar um novo no dia seguinte. Para que este seja bem sucedido, existem dois pré-requisitos. O primeiro é de que o sistema informatizado tenha sido muito bem testado antes de ser autorizado para operar com os dados. O segundo é de que existam planos de contingência em caso de falha do novo sistema. Isto pode incluir precauções como guardar cópias dos dados digitados, listar todos os arquivos principais em cada actualização, e manter o pessoal no departamento do utilizador até que o novo sistema seja provado fiável.

Há vantagens e desvantagens em cada abordagem. Em caso de transição directa, o utilizador e o sistema são apenas moderadamente solicitados, mas as consequências de uma falha podem ser catastróficas. Os riscos de falhas com o funcionamento paralelo e o piloto são consideravelmente mais baixos, mas ambos os métodos requerem maior esforço do sistema e do utilizador. Para a implementação de um grande sistema, pode ser aconselhável, implementá-lo com o funcionamento paralelo num único local piloto. Esta é provavelmente a opção mais segura numa área sensível onde o custo da falha poderia ser elevado. O funcionamento paralelo e o piloto oferecem uma oportunidade de baixo risco para testar as partes do sistema que ainda não foram testadas, tais como, os procedimentos dos operadores, os procedimentos de preparação de dados, procedimentos do departamento do utilizador, etc. Estes procedimentos já terão sido estabelecidos nos manuais do utilizador e do operador pelos analistas de sistemas durante a configuração do sistema e precisarão ser testadas sob condições reais de funcionamento. Quando o sistema novo (quer os sub-sistemas informáticos, quer os manuais) operar satisfatoriamente por um período razoável, o Comité Directivo dará instrução para pôr fim ao uso do antigo sistema manual.

5.6. Avaliação pós implementação

(Normas Transitórias 7.1)

A avaliação pós implementação é um acompanhamento essencial para qualquer projecto de informatização. As razões principais para a realização de tais avaliações são:

- Determinar em que medida o sistema informático alcançou os objectivos pretendidos
- Assegurar-se de que os benefícios, tangíveis e intangíveis, tenham sido realizados;
- Comparar os custos e os benefícios reais com os projectados na fase do Estudo de Viabilidade;
- Identificar quaisquer debilidades do sistema e recomendar as melhorias necessárias.

A avaliação pós implementação é um elemento essencial no controle efectivo de projectos. Isto proporciona à Administração Aduaneira uma justificação independente dos custos de desenvolvimento juntamente com uma certificação dos benefícios efectivamente alcançados.

As avaliações pós implementação são muitas vezes realizadas em nome do Comité Directivo de informática pelo Comité de Projecto embora, em algumas ocasiões, pode ser encarregada uma equipa de avaliação independente ou a tarefa pode ser realizada por uma outra administração, tal como o Ministério das Finanças ou o Tesouro que pode exigir uma justificação formal para as despesas efectuadas. Tipicamente, uma avaliação pós implementação deve ser realizada aproximadamente 6 a 9 meses depois do início do sistema. Isto dá oportunidade suficiente para que quaisquer dificuldades iniciais sejam resolvidas e para que os utilizadores se acostumem à mudança de procedimentos. Estas avaliações não devem estar confinadas a apenas uma ocasião mas devem ser repetidas num intervalo de 2 a 3 anos para que a operacionalidade do sistema seja mantida em revisão constante.

Mesmo que pequenas modificações, melhorias ou adaptações possam, por vezes, ser recomendadas depois de uma avaliação pós implementação, é raro ver os projectos abandonados ou essencialmente modificados, a menos que os mecanismos de planificação e de controle não tenham sido devidamente implementados.

Durante a avaliação, podem ser identificados alguns problemas que podem tornar a tarefa de avaliação mais difícil. Acontece muitas vezes faltarem dados históricos suficientes e bem documentados sobre o sistema manual antigo para proceder a uma comparação válida com o novo sistema. Algumas informações sobre o sistema manual estarão contidas no Relatório do Estudo de Viabilidade mas estas são frequentemente insuficientes. Outra dificuldade pode surgir das expectativas pouco realistas dos utilizadores relativamente ao novo sistema. Se não lhes forem devidamente transmitidos os conhecimentos básicos de informática, os utilizadores podem acreditar que os sistemas informáticos são capazes de resolver todos os seus problemas com o pressionar de uma tecla. Isto raramente acontece na realidade. A mudança dos requisitos do utilizador pode também causar dificuldades. Por vezes os utilizadores não reconhecem que o sistema informático só pode ser concebido com base na situação do momento. Se as exigências mudarem, o sistema informático deve ser mudado ou reconfigurado.

Frequentemente surge um outro problema relacionado com a quantificação de certos benefícios do sistema. Por exemplo, seria difícil quantificar o benefício da informatização das Alfândegas para a economia de um país como um todo, embora seja seguro afirmar que alguns benefícios serão obtidos. Por último, nos casos em que o sistema estiver a ser avaliado por um avaliador independente que não faça parte da Administração Aduaneira, podem surgir problemas resultantes da falta de conhecimento da área funcional em análise. Isto pode, por vezes, levar a mal-entendidos e, portanto, deve-se ter cuidado no sentido de evitar erros de facto no relatório do avaliador.

Apesar das dificuldades, uma avaliação pós implementação traz muitos benefícios. Em primeiro lugar, dá aos utilizadores a oportunidade de expressarem os seus pontos de vista em relação ao sistema, bem como indicar se as suas necessidades estão ou não a ser satisfeitas. Se tiverem críticas justificáveis, o relatório do avaliador fornecerá uma base para rectificar quaisquer deficiências do sistema. Dará também a oportunidade de analisar as vantagens de futuras melhorias do sistema, bem como avaliar prioridades para futuros desenvolvimentos. Por último, fornecerá uma justificação independente para os custos de desenvolvimento.

5.7. Manutenção do sistema

5.7.1. Motivos para a manutenção

Nada é permanente, em particular, quando se trata de computadores ou sistemas informáticos. Serão necessárias mudanças desde o primeiro dia da operação. Os motivos, entre outros, podem ser os seguintes:

- Falhas não detectadas anteriormente são inevitáveis. Mesmo que um sistema funcione regularmente por muitos anos, não há garantias de que não existam falhas. Pode se dar o caso em que a combinação particular de circunstâncias, que possa evidenciar a falha, não tenha ainda ocorrido. As rotinas de fim-de-ano podem comportar falhas que só se manifestarão passados 12 meses. Dentro de um sistema novo as falhas manifestam-se inevitavelmente nos primeiros ciclos.

- Após utilizar e observar algumas vezes o sistema em operação real os responsáveis do sistema e o operador informático podem estar em condições de sugerir mudanças adequadas para acelerar as operações e reduzir os custos. O utilizador pode constatar, à luz da prática actual, que os modelos e os procedimentos podem ser melhorados para tornar o seu uso mais fácil.

- A mudança mais radical seria a aquisição de um computador novo e diferente; neste

caso o sistema teria de ser reconfigurado. É mais provável que faça sentido mudar o sistema para tirar proveito de um novo tipo de periférico ou características de um novo software.

- Mudanças dos volumes de transacções a serem processadas para além das previsões. Isto pode exigir a melhoria do hardware.

- Mudanças legislativas, por exemplo, mudança das taxas de direitos e demais imposições, mudanças da pauta aduaneira (a introdução do sistema harmonizado trará mudanças consideráveis aos sistemas existentes), nova política de comércio (quotas, restrições), novas taxas (tais como o imposto sobre o valor acrescentado) na importação.

- Implementação de sistemas relacionados, por exemplo, se uma administração dispõe já de um sistema de processamento de declarações e pretender introduzir um sistema de controle de carga, o primeiro sistema precisará de ser parcialmente reestruturado para incluir o *interface* com o novo sistema de controle de carga.

5.7.2. Tipos de manutenção

Quase todo o trabalho de manutenção de sistemas pode ser dividido pelas seguintes categorias:

- Modificações (urgentes ou não) que não requerem grandes mudanças à lógica do sistema.
- Revisões que requerem uma nova configuração e programação, por exemplo, mudanças nas especificações de entrada e saída – novas formas de inserção, novos relatórios.

A reformulação do desenvolvimento exige uma nova configuração dos sistemas, programação e testes de grande envergadura, por exemplo, mudanças significativas à lógica de processamento como resultado de novos requisitos. Pode ser inadequado tratar desta questão no âmbito da “Manutenção” visto que a referida reformulação pode passar por todas as fases de um novo projecto (da viabilidade à implementação).

Mesmo as pequenas mudanças ao sistema devem ser devidamente testadas antes da entrada em produção.

5.7.3. Responsabilidade pela manutenção

Nos casos em que os sistemas aduaneiros são desenvolvidos por consultores externos, o contrato do sistema deve especificar a assistência técnica pelo menos a curto prazo. O pessoal aduaneiro (da divisão de TI) deve trabalhar juntamente com os consultores, durante o desenvolvimento do projecto, no sentido de assegurar-se de que esteja completamente familiarizado com todos os aspectos do sistema. A divisão de TI será então responsável pela manutenção de rotina do sistema.

Para uma reformulação do desenvolvimento mais extensiva pode ser necessário contratar novamente os consultores externos, salvo se a divisão de TI já tiver experiência e pessoal suficiente para realizar esse trabalho.

Nos casos em que os sistemas aduaneiros forem desenvolvidos internamente, a divisão de TI das Alfândegas terá conhecimentos e experiência suficientes para manter qualquer sistema que tenha desenvolvido.

5.8. Estabelecimento de um Serviço de Apoio

5.8.1 Compromissos de serviço com os clientes das Alfândegas

Quem são os nossos clientes? É fácil identificar clientes. Os importadores, exportadores, despachantes, passageiros e operadores de armazéns, transportadores, etc. obviamente são os primeiros que vêm à mente. Contudo, uma abordagem rigorosa à identificação dos clientes envolve a análise da base de dados das Alfândegas. A base de dados da OMA contém uma secção denominada "pessoas e partes" que é apenas uma lista parcial dos clientes das Alfândegas. As outras instituições públicas e, sobretudo, os clientes internos devem igualmente ser tidos em conta. Embora seja bom estar em condições de prestar serviços a todos os clientes, revela-se útil identificar os sectores prioritários.

Requisitos do Serviço e Canais de Entrega: a identificação dos requisitos dos serviços começa quando os mesmos estiverem a ser modelados na fase de concepção. Alguns dos "actores" nos diagramas de casos de uso são os beneficiários dos serviços, enquanto que há outros que são os produtores. Os requisitos do serviço ao cliente e os meios correspondentes para a satisfação destes requisitos podem ser extraídos das especificações de caso de uso.

Por exemplo, os importadores, exportadores e seus agentes/despachantes procuram informação sobre a logística de carga, autorização de saída e outras informações comerciais (requisito de serviço), que precisam de receber por via electrónica (meios de prestação de serviço). Os canais de entrega de serviços por via electrónica que as administrações aduaneiras normalmente asseguram estão previstos nas Directivas da Convenção de Quioto sobre as TIC. O Serviço de Apoio é um dos canais de prestação de serviço. Trabalha em conjunto e, frequentemente, em apoio aos outros canais.

Áreas de Serviço e Pedidos de Serviço: As Alfândegas possuem uma vasta clientela e também uma grande responsabilidade. Portanto, é necessário distinguir as diferentes Áreas de Serviço. Cada Área de Serviço trataria de uma lista habitual de "Pedidos de Serviço", a qual deve ser distribuída entre as pessoas que processarão esses pedidos. Eis alguns exemplos para ilustrar esta questão:

Enquanto que a importação, a exportação e o trânsito podem ser áreas de serviço diferentes, um atraso ou um problema em receber uma reclamação de draubaqueseria um Pedido de Serviço.

A infra-estrutura de TI é normalmente complementada por um Serviço de Apoio. Esta infra-estrutura de TI surge para assegurar o cumprimento de um ciclo de prestação de serviço (por exemplo, a emissão de uma autorização de saída feita após a declaração do cliente). A infra-estrutura completa pode ser dividida em áreas de serviço e a cada uma destas pode corresponder um Pedido de Serviço.

Padrões de serviço e compromissos de serviço: é fácil identificar os requisitos dos serviços quando os padrões de serviços são conhecidos e estabelecidos. Os padrões de serviço são geralmente derivados das expectativas dos clientes. Estes são normalmente parâmetros mensuráveis das ofertas de serviço – tal como o tempo de espera para a análise de uma

documentação ou o tempo necessário para a obtenção de um reembolso. Outros padrões de serviço são intangíveis – tais como a qualidade da informação no *website* e a cortesia demonstrada pelo inspector aduaneiro. No entanto, todos os padrões de serviço são comportamentos mensuráveis de um indivíduo, grupo e sistemas. Diz-se muitas vezes que os padrões de serviço conduzem a configuração de sistemas. O inverso é igualmente verdade. Os sistemas estabelecidos podem limitar a capacidade de resposta das Alfândegas, por exemplo, não se pode esperar que um procedimento manual seja tão rápido quanto um sistema informatizado. Portanto, as Alfândegas devem declarar os seus compromissos de serviço tendo em mente as limitações dos seus sistemas. Algumas administrações publicam os seus compromissos de serviço nas Cartas dos Cidadãos**.**

5.8.2. As Alfândegas precisam de um Serviço de Apoio?

Todos os modelos organizacionais que contemplam a prestação de serviços à distância requerem recursos de suporte à distância. Com a introdução das Tecnologia de Informação e de Comunicação (TIC) nas Alfândegas, a maioria das administrações aduaneiras precisa de um Serviço de Apoio de alguma magnitude. O tipo de Serviço de Apoio (tamanho e características dos resultados) é determinado por estimativas do nível de exigências e reclamações dos serviços. É normalmente fácil estimar as necessidades de serviços dos clientes por categorias. No entanto, estima-se que os níveis de serviços tenham um certo impacto sobre o respeito das regras pelos clientes. O Serviço de Apoio pode aumentar a eficácia na prestação de serviço? Certamente, um Serviço de Apoio eficaz alteraria a percepção do cliente relativamente à prestação de serviços pelas Alfândegas.

Tendo em conta a posição de monopólio das Alfândegas, as questões ligadas à preservação das actividades não se colocam (ao contrário das organizações comerciais). Não podemos perder os nossos clientes a favor da concorrência. Contudo, a nossa eficácia pode aumentar a produtividade dos nossos clientes e aumentar a confiança dos operadores comerciais no ambiente operacional. Se um determinado equipamento ou uma parte da rede estiver inoperante poderá haver perda de produtividade. O Serviço de Apoio pode formalmente rastrear esta perda no sentido de melhorar a produtividade de um determinado activo, tanto para os clientes internos como para os externos.

5.8.3. Várias dimensões de Serviço de Apoio

5.8.3.1. Conceito de Serviço de Apoio:

O termo “Serviço de Apoio” refere-se ao conceito de ter um ponto único de interface numa organização, para gerir os pedidos de serviço. Em todos os sectores de serviço, existem operações da “linha da frente” e da “retaguarda”. Esta última é uma rede complexa de operações envolvidas na criação e prestação de serviços e, normalmente, não é visível aos clientes internos e externos. Para os clientes, o uso de serviços deve ser uma experiência agradável e satisfatória. O Serviço de Apoio, sendo o primeiro ponto de contacto, é a linha da frente dos serviços que regista os pedidos dos clientes, os traduz em problemas técnicos e operacionais para os quais se deve encontrar uma solução. Posteriormente, o Serviço de Apoio procura a solução mantendo-se na retaguarda para apresentar os resultados em relação aos pedidos e comunica-os ao cliente numa linguagem que lhe é familiar. A actividade do Serviço de Apoio é produtiva, se puder resolver e concluir o pedido para a satisfação do cliente. O Serviço de Apoio é a face amiga de uma organização, que permite alargar os limites dos principais procedimentos desta organização. De modo geral, é um centro de comunicações e de transferência de conhecimentos.

5.8.3.2. Contactos com os serviços e "momentos da verdade":

As Alfândegas, na qualidade de uma autoridade de arrecadação de receitas e uma instituição de aplicação da lei não é especialmente destinada a agradar aos clientes. Contudo, enfrenta os seus "momentos de verdade" nos vários pontos de contacto com os seus clientes nas operações do dia-a-dia. Estes "momentos de verdade" constituem para o cliente toda a sua experiência de serviço. É da competência do pessoal do Serviço de Apoio produzir e controlar esta experiência de serviço e o nível de satisfação resultante do contacto com o serviço.

5.8.3.3. Recuperação de serviço

De facto, na medida em que a organização aduaneira lança o seu sistema informatizado económicos e seus utilizadores internos, o Serviço de Apoio é a primeira e última linha de defesa contra as falhas do serviço. Na eventualidade de uma falha de serviço, normalmente, o Serviço de Apoio não está em condições de gerir esta situação e caberá, então, à gestão superior intervir para realizar as operações de controle dos danos ou "recuperação de serviço".

5.8.4. O Serviço de Apoio como meio de prestação de valor

Tal como é a natureza do serviço, o mérito ou valor do Serviço de Apoio à prestação de serviços das Alfândegas é também oculto e intangível. É difícil determinar, mas as ligações podem ser estabelecidas com factores mensuráveis tais como (i) continuidade de actividades (ii) reclamações (iii) preferências nas opções de serviços (iv) melhorias nos prazos dos ciclos (v) perda de produtividade devido a questões técnicas.

A eficácia do Serviço de Apoio é indissociável à imagem das Alfândegas como um serviço eficaz. Os processos e funções relevantes que estão relacionados com o Serviço de Apoio mas são integrantes da prestação de serviço são:

- Gestão do conteúdo da *web*: a popularização da Internet como um meio, transformou-a na primeira escolha da administração para levar a informação ao cliente. É uma ferramenta assíncrona – o cliente pode usar esta ferramenta à vontade e sozinho sem ter que falar com ninguém. As operações e processos do Serviço de Apoio devem complementar o *website* e fazer parte dos instrumentos das comunicações em conjunto com o conteúdo da *web* e outros elementos do plano da comunicação e da publicidade. O Serviço de Apoio é normalmente a última linha de defesa numa estratégia de prestação de serviços, mas poderia, de forma permanente, ser incluído nas *FAQs* e outras ferramentas tutorais incluídas na oferta de serviços.

- Auto-aprendizagem do cliente: frequentemente, as Administrações Aduaneiras tiveram de lutar enquanto introduziam novos serviços à distância, tais como o EDI ou arquivos à distância. Independentemente das contribuições de formação dadas e dos *workshops* organizados para formar os utilizadores, existem sempre erros iniciais que causam falhas dos serviços. A autoaprendizagem pelo cliente ocorre em ciclos de aprendizagem e melhoria contínua. A auto-aprendizagem do cliente é uma meta e o Serviço de Apoio uma parte integrante da estratégia.

- Gestão da mudança: O Serviço de Apoio pode desempenhar um papel de linha da frente na gestão de mudança. A orientação do processo de actividades e da tecnologia num cenário em mudança é um desafio. Sempre que seja necessário introduzir uma nova tecnologia/processo de actividade, os agentes do Serviço de Apoio seriam os

pontos centrais na actividade de planificação estratégica e do plano geral de assistência do cliente. O Serviço de Apoio pode trabalhar proactivamente no sentido de minimizar os riscos de activação de serviços mesmo que apenas os serviços testados sejam implementados. O Serviço de Apoio desempenha um papel fundamental na construção e teste de novos serviços e no momento de "saída para a produção" . Os Serviços de Apoio são capazes de identificar lacunas em todo o sistema de serviço que tenha sido planificado.

- Gestão de conhecimento: o Serviço de Apoio é um dispositivo que permite tanto a aquisição de conhecimentos, como também testar novas soluções. Se uma questão do tipo "quais são as três principais fontes de irritação dos utilizadores?" for lançada ao Serviço de Apoio, os problemas que afectam os serviços seriam imediatamente identificados. A área de gestão de chamadas pode controlar o número e o nível de chamadas em diferentes áreas de serviços. Os pedidos podem ser categorizados e "as soluções que funcionaram" podem ser documentadas na base de dados do Serviço de Apoio. Isto pouparia tempo aos agentes do Serviço de Apoio e aos clientes das Alfândegas mediante acesso directo às soluções da base de conhecimentos.

- Gestão dos níveis de serviço: Apesar do Serviço de Apoio ser um componente essencial dos relatórios sobre os serviços prestados, trabalha frequentemente com outras ferramentas e fontes que reúnem informação relativa à interrupção dos serviços. Muitas vezes, as ferramentas informáticas são introduzidas para monitorizar a disponibilidade dos dispositivos de TIC, serviços e processos. São úteis para reagrupar os dados que permitem a criação de um quadro que representa os níveis dos serviços prestados.

5.8.5. Como criar um Serviço de Apoio

Um Serviço de Apoio requer cinco componentes:

(1) A Componente de TIC: para activar o Serviço de Apoio, são necessários alguns componentes de Tecnologia de Informação e da Comunicação. Estas componentes permitem aos agentes do Serviço de Apoio ter acesso a informação relevante para responder aos pedidos em tempo oportuno. Actualmente, a maioria dos componentes de *hardware* e *software* proporciona uma facilidade para a monitorização à distância. Adicionalmente, há necessidade de linha telefónica com resposta interactiva de voz, a qual seria apoiada por um agente de chamada. Para manusear o direccionamento apropriado e gestão do volume de todas das chamadas, há várias soluções do centro de chamadas, as quais garantem a produtividade do agente de chamada. Estas soluções são uma mistura de *hardware* e *software*. Para maior eficácia, as chamadas devem ser consignadas, resolvidas e controladas.

(2) A componente Humana: os provedores de serviços do Serviço de Apoio são pessoas que entrariam em contacto com os clientes para prestar informação e serviços. Existem duas formas de aquisição de provedores. (a) Terceirização (*out-sourcing*), o que implica a celebração de contrato com um provedor de serviços especializado na concepção e implementação de Serviços de Apoio. É normalmente referida como Terceirização de Processos de Actividades. Geralmente é alinhada com uma estratégia de terceirização da gestão das instalações e dos serviços. (b) aquisição de serviços internos (*in-sourcing*) se os serviços forem prestados pelo pessoal interno.

As Alfândegas em todo o mundo estão a usar cada vez mais as TIC para ganhos na produtividade e oportunidade para a redistribuição de recursos humanos. A referida oportunidade pode ser usada no estabelecimento de uma função de Serviço de Apoio dentro da estrutura organizacional. A TIC pode, por exemplo, iniciar uma função de apoio aos serviços informáticos. Posteriormente, toda a clientela (interna e externa) pode ser abrangida.

(3) A componente do conhecimento: a informação sobre os processos essenciais que contribuem para os ciclos de prestação de serviços deve estar disponível à distância para o Serviço de Apoio. Os incidentes que podem conduzir a falha de serviços devem ser representados em diagramas do tipo causa-efeito (diagramas *Ishikawa*) e todas as causas de falhas de serviços que surgirem de problemas de equipamento ou *software* devem ser monitorizadas e resolvidas à distância a partir do Serviço de Apoio. Ao longo do tempo, os ciclos de resolução de chamadas conduzem à criação de uma base de conhecimentos de soluções bem sucedidas, as quais poderiam ser usadas em incidentes futuros da mesma natureza.

(4) Um modelo de Serviço de Apoio: a maior preocupação na criação de um Serviço de Apoio é a uniformização do Serviço de Apoio com as outras actividades. O modelo de Serviço de Apoio deve estar baseado na premissa de serviço ao cliente de que os utilizadores devem ter um Ponto de Contacto Único (PCU) que compreenda as necessidades dos clientes e quais os objectivos dos serviços (que devem ser identificadas). O cliente pode ter problemas ligados à sua actividade ou de comunicação. O Serviço de Apoio deve estar apto a resolver ambos.

(5) Formação: o pessoal dos PCU deve ser formado para que seja confiável, paciente e capaz de se manter sereno e calmo em situações de tensão, em particular quando estiver a lidar com um cliente irritado. A formação deve incluir a descrição apropriada dos objectivos dos serviços para que a resolução de chamadas seja devidamente direccionada e o tempo de resolução reduzido. Os especialistas podem apoiar os PCU, em último recurso. O registo de chamadas seria a última opção a ser usada pelos especialistas e apenas nos casos em que os seus esforços de tempo real falharem. O modelo de Serviço de Apoio compreende a gestão do fluxo de chamadas, uma matriz de apoio e uma matriz de escala de chamadas.

A planificação das capacidades do Serviço de Apoio exige que se tenha em consideração a variedade e o volume de chamadas. A variedade depende da diversidade dos serviços envolvidos (necessidades comerciais) e da especialização necessária entre os agentes, mas pode, por vezes, ser resolvido se os agentes possuírem múltiplas qualificações. A existência de qualificações múltiplas por parte dos agentes conduziria a um tratamento homogéneo das questões comerciais e técnicas. Contudo, é difícil prever os volumes de chamadas, bem como os padrões de chegada de chamadas. As regras normais para o dimensionamento dos serviços aplicam-se igualmente na determinação do número de vagas a serem preenchidas, excepto devido ao facto de os utilizadores serem pouco tolerantes em relação ao tempo de espera em um ambiente de prestação de serviços à distância. Os aumentos repentinos no número de chamadas (picos de actividade), as horas de cobertura, as situações de novos processos de actividades e a introdução de tecnologia devem ser levadas em conta.

A arquitectura do Serviço de Apoio pode ser centralizada ou distribuída. Contudo, os agentes que operam os Serviços de Apoio devem estar em condições de rastrear e gerir os pedidos dos clientes submetidos por telefone, *e-mail*, *web* ou por dispositivos sem fio (PDA). Ao agente deve ser proporcionado um processo de trabalho simples e fácil de gerir. O fluxo de trabalho deve ser governado por regras de funcionamento e de procedimentos automatizados, uma vez que a resposta oportuna aos clientes é essencial. A informação requerida pelos clientes ou necessária para a prestação do serviço solicitado deve estar disponível instantaneamente e, na medida do possível, deve estar em harmonia com o que consta no serviço web onde os clientes decidem resolver os seus próprios problemas ou contactar o Serviço de Apoio. A unidade de atendimento à distância pode igualmente ser configurada.

5.8.6. Como avaliar o desempenho do Serviço de Apoio?

É muito difícil determinar o desempenho do Serviço de Apoio visto que lidamos com vários acontecimentos intangíveis e momentâneos na prestação de serviço à distância. Contudo, precisamos de determinar o grau de êxito do Serviço de Apoio. Critérios objectivos e orientados ao resultado devem ser desenvolvidos para avaliar os factores de sucesso do Serviço de Apoio, conforme o quadro seguinte:

	CRITÉRIO	**MÉTODO DE AVALIAÇÃO**
1.	Credibilidade, sinceridade e cortesia	Pesquisa entre os clientes
2.	Tempo de resposta	Amostragem de chamadas, encaminhamento de chamadas e monitorização
3.	Tempo de resolução de chamadas	➢ Número de chamadas / incidentes ➢ Número de resoluções ➢ Tempo gasto em chamadas ➢ Número de clientes únicos atendidos ➢ Número bruto de resoluções no primeiro contacto ➢ A partir da data e hora constantes na base de dados de gestão e encaminhamento das chamadas
4.	Duração das chamadas *versus* tempo inactivo	Ver acima
5.	Utilização eficaz das oportunidades de formação do cliente	➢ Relatórios de agentes de chamada ➢ Pesquisa entre clientes
6.	Promoção da auto-aprendizagem do cliente	Número de *FAQs*; redução de chamadas sobre o assunto.

5.8.7. Impacto do Serviço de Apoio nas operações das Alfândegas

Há necessidade de integrar programas de assistência ao cliente no Serviço de Apoio porque a informação dos clientes permite favorecer e reforçar o cumprimento espontâneo das disposições. Um serviço profissional e estruturado de apoio ao cliente pode melhorar os níveis de cumprimento das disposições, facilitando consideravelmente o respeito dessas disposições pelos clientes. Os clientes saberiam então que têm voz e que alguém os ouve. A tecnologia moderna pode levar toda a informação ao computador do cliente, porém a realidade é que os clientes ainda preferem comunicar com pessoas que podem ter empatia e resolver as suas questões. O conceito de um Serviço de Apoio acompanha sempre a necessidade de melhorar o apoio e pode ser usado como o factor inovador para a gestão de mudança.

6. Resumo das principais áreas de aplicação

(Norma 7.1)

6.1. Introdução

Existem muitas áreas nas quais a introdução das tecnologias de IC pode beneficiar às Alfândegas. A secção seguinte descreve os principais processos e procedimentos aduaneiros nos quais a TI pode ter um impacto significativo. As principais áreas são:

- Controle de inventário da carga;
- Processamento da declaração de mercadorias (importação e exportação, trânsito, aperfeiçoamento activo, etc.);
- Nota de Autorização de Saída;
- Luta contra a fraude aduaneira;
- Selectividade;
- Controle antecipado de passageiros (Processamento de viajantes);
- Contabilização da receita;
- Estatísticas do comércio externo;
- Sistema de Gestão da Informação (SGI); e
- Relatórios;
- Armazenagem de dados;
- Registo de Parceiros Comerciais;
- Informatização dos escritórios;
- Intranet e Extranet das Alfândegas.

Idealmente, um sistema informatizado das Alfândegas deve estar em condições de desempenhar todas estas funções. Alguns países implementaram sistemas abrangentes desta natureza, mas em muitos outros apenas algumas funções foram informatizadas ou a informatização está confinada a um número limitado de portos, aeroportos, etc. de elevado volume. Muitas das aplicações mencionadas têm suporte de outras aplicações. Por exemplo, os dados captados a partir da declaração de mercadorias em um sistema de processamento de declarações de mercadorias pode ser usado por um sistema de contabilização de receitas para efectuar contabilizações e por um sistema de estatísticas comerciais externo para efectuar estatísticas. De igual modo, a informação armazenada num sistema de aplicação da lei pode ser usada por um sistema de controle de inventário da carga, por um sistema de processamento de declarações de mercadorias ou por um sistema de processamento de passageiros para efeitos de controles aduaneiros. Em muitos casos os sistemas partilham os *hardwares* (processador central, VDUs - terminais de monitores de visualização, impressoras, rede de telecomunicações) e arquivos informáticos.

Nem sempre é viável ou prático desenvolver um sistema aduaneiro informatizado abrangente que abarque todos os processos e procedimentos de uma só vez. Contudo, quando um sistema estiver a ser concebido, todos os aspectos precisam de ser identificados, incluindo os processos, as bases de dados, as interacções entre os vários processos e dados. O sistema deve ser concebido em base modular. Isto permite que diferentes partes sejam desenvolvidas em fases diferentes e integradas com outras partes ou outros sistemas, conforme necessário.

6.2 Validação de dados

Os sistemas informáticos devem identificar e informar:

- Detectar e assinalar os erros mais graves; e
- Detectar e assinalar os erros potenciais (isto é, aplicar critérios de julgamento aos dados).
- Os erros podem ser detectados em duas fases:
- A primeira é no momento da introdução de dados. Esta é por vezes referida como a validação de dados e trata normalmente com erros absolutos;
- A segunda é durante a actualização. Além de detectar os erros absolutos, o sistema pode realizar alguns testes de controle de credibilidade usando os dados dos arquivos principais para efeitos de comparação.

É possível combinar estas duas fases mas para tal, os arquivos principais devem estar disponíveis no momento da introdução dos dados.

As verificações típicas da fase de introdução de dados são as seguintes:

Tipo	Explicação	Exemplos
Presença	Verifica se todos os campos necessários ou obrigatórios estão presentes. Isto é particularmente importante se houver campos opcionais que podem se tornar obrigatórios se outros dados opcionais forem fornecidos	O "número do operador comercial" deve estar presente caso se solicite o adiamento do pagamento dos direitos e demais imposições.
Tamanho	Verifica se o número correcto de caracteres consta de um campo	Se o campo "número do código pautal" tiver um comprimento fixo de 8 dígitos, então os dados deste campo serão rejeitados se não forem inseridos os 8 dígitos
Controle de conformidade	Verifica se os números e os códigos estão contidos na lista de códigos prescrita	Se uma lista de códigos for atribuída na escala 7000-7999, então tudo o que estiver fora disto será rejeitado. O país de origem deve estar em conformidade com o código de países ISO 3166.
Verificação de caracteres	Os campos são verificados para assegurar-se de que contenham apenas o tipo de caracteres correctos	Se o dado "País de Origem" deve estar no formato alfa de dois caracteres, os dados serão rejeitados se forem detectados quaisquer caracteres numéricos.
Dígitos de controle	Este é um número de auto verificação criado por uma fórmula matemática ou algoritmo geralmente conhecido como um modulus. É usado para identificar quer números falsos ou números que têm erros de transcrição ou de transposição.	A validade de um número de registo do operador comercial pode ser verificada sujeitando-a ao mesmo cálculo que criou o dígito de controle original.
Razoabilidade	Antes do processamento, as quantidades são verificadas para certificar se são exageradamente elevadas ou baixas.	É razoável que um super petroleiro que transporte petróleo bruto, declare 100 toneladas?

No momento da actualização podem ser efectuadas as seguintes verificações:

Registos novos	Se estiver a ser inserido um registo completamente novo no arquivo principal, haverá uma verificação para assegurar que não haja duplicação.
Registos eliminados	Se for marcado um registo para eliminação haverá uma verificação para averiguar se o registo existe. Se não existir será assinalado um erro.
Compatibilidade	Antes de se alterar um arquivo principal, será feita uma verificação para certificar-se de que os novos dados são compatíveis com os que já se encontram no arquivo principal. Por exemplo; quando o arquivo principal da folha de pagamento for actualizado com os pagamentos das horas extras, será feita uma verificação para confirmar se o funcionário tem direito a horas extras.

Outras verificações conhecidas como verificações de credibilidade (a razoabilidade serve de exemplo), que dependem de parâmetros preestabelecidos são usadas para determinar a qualidade dos dados introduzidos. Estas são geralmente verificações de comparação que tentam identificar dados incompatíveis (por exemplo, é pouco provável que um navio que parte de Nova Iorque descarregue em *Heathrow*; o preço de uma determinada mercadoria de um país específico seja mais baixo do que o esperado, etc).

Quando se detecta um erro, o procedimento normal é como se segue. No momento da introdução dos dados no sistema, os erros causarão rejeições e deverão ser corrigidos e inseridos novamente. As verificações de credibilidade nem sempre são fatais e, normalmente, é permitido que o processamento continue, mas a situação é informada para investigações subsequentes antes da aceitação ou rejeição final. Pode ser incluído um subsistema informatizado de monitorização para assegurar-se de que os erros reportados sejam corrigidos dentro de um determinado prazo. O sistema pode também rejeitar ou aceitar automaticamente quaisquer erros reportados não corrigidos dentro do prazo previsto e produzir relatórios de auditoria sobre os erros e como eles foram resolvidos.

6.3. Controle de inventário da carga

O controle da carga, desde o momento da sua chegada até ao pagamento ou garantia dos direitos e demais imposições e a autorização de saída, representa muitos problemas para as administrações. As Alfândegas devem assegurar-se de que toda a carga que chega ao seu território pode ser devidamente controlada. O processo de conferência manual dos registos em papel para este efeito é complexo, propenso ao erro e dispendioso. Em um sistema informatizado de controle de carga, os dados do manifesto e da declaração aduaneira podem ser comparados automaticamente. Os dados podem ser alterados no sentido de registar quaisquer excessos ou faltas de mercadorias após a verificação aduaneira. Os dados da carga podem ser analisados minuciosamente em função de critérios de selecção predeterminados no sentido de alertar os funcionários aduaneiros sobre as remessas de alto risco. Após a apresentação da declaração das mercadorias em questão o sistema apura automaticamente o registo de inventário da carga ou produz um relatório de discrepâncias para acção de acompanhamento. Os relatórios da carga não declarada dentro dos prazos previstos são normalmente produzidos para investigações subsequentes.

Em algumas circunstâncias, as Alfândegas não dispõem do seu próprio sistema informatizado de controle de inventário da carga, mas confiam nos sistemas informatizados dos transportadores, autoridades portuárias, etc. As Alfândegas mantêm controle sobre estes sistemas mediante auditorias. Esta abordagem ao controle de inventário da carga pode oferecer uma solução económica para as Alfândegas em particular, na medida que a maioria dos transportadores e autoridades portuárias é informatizada.

A aceitação da informação electrónica de manifestos de carga no sistema, antes da chegada das mercadorias, permite às Alfândegas a realização de uma avaliação inicial do risco, que estas remessas representam. Nos casos de mercadorias de valor reduzido e não sujeitas a qualquer restrição poderá não ser necessário efectuar qualquer avaliação adicional.

6.4. Processamento de declarações de mercadorias (importação e exportação)

(Normas Transitórias 3.18 e 3.21)

O processamento de declarações de mercadorias para a importação e exportação é uma das principais tarefas de qualquer Administração Aduaneira e muitas administrações já obtiveram ganhos consideráveis de produtividade através da informatização deste procedimento.

Os dados podem ser captados das seguintes formas:

- Inserção de dados pelos funcionários aduaneiros;
- Inserção de dados através da digitação electrónica directamente pelo Importador (DTI), pelos parceiros comerciais ou prestadores de serviços; e/ou
- Leitura de códigos de barras, dispositivos de auto-identificação e de reconhecimento óptico dos caracteres (ROC)
- Outras capturas e dispositivos de geolocalização
- Transmissão de dados

Uma vez inseridos os dados da declaração de mercadorias no sistema informatizado, estes estarão sujeitos a várias operações. As principais operações são:

- Validação de dados (ver 6.2 acima);
- Classificação e origem;
- Avaliação de riscos e de selecção
- Controle de valor;
- Cálculo dos direitos e demais imposições;
- Cobrança de direitos (direitos aduaneiros, IVA, impostos indirectos, etc.)

A implementação de uma base de dados pautal integrada permitirá que quaisquer restrições ou preferências ligadas a declaração sejam rápida e correctamente identificadas e assegurará a aplicação das taxas pautais correctas.

A determinação correcta do valor aduaneiro das mercadorias, incluindo as medidas nacionais e internacionais é a base para um cálculo correcto dos direitos e demais imposições. Uma base de dados actualizada, relativa ao valor aduaneiro, pode ser usada para identificar valores aceitáveis para mercadorias específicas provenientes de determinados países. A base de dados pode também destacar o valor aduaneiro que não se enquadra nos limites aceitáveis.

Uma vez calculados os direitos e demais imposições (incluindo a conversão da moeda), a informação pode ser transmitida para o sistema de contabilização de receitas.

Durante estas operações o utilizador é notificado de quaisquer erros através de mensagens geradas pelo sistema e tem a oportunidade de fazer correcções. É também notificado sobre qualquer documentação de suporte que possa ser necessária antes das mercadorias serem desembaraçadas, por exemplo, licenças, certificados de origem, etc. As Alfândegas poderiam, em vez de pedir copias sob o formato papel dos documentos de suporte, proceder a uma verificação das informações contidas nos documentos de suporte. Se não for possível, os documentos de suporte podem ser recebidos por via electrónica para fins de verificação automática. (Queiram consultar a Recomendação da OMA relativa a desmaterialização dos documentos de suporte).

Uma vez as formalidades realizadas, o sistema pode igualmente gerar a Nota de Desalfandegamento (ver igualmente o parágrafo 6.6). Quando o controle do inventário da carga foi igualmente informatizado, uma aproximação é geralmente estabelecida entre os dados concernentes à carga e os que figuram na declaração de mercadorias, o inventário é de seguida apurado.

Os sistemas de processamento das declarações de mercadorias podem igualmente produzir para as empresas, extractos periódicos que listam os montantes devidos a título de pagamento a posterior, a fim de assegurar a transferência electrónica dos fundos entre as contas do operador comercial e as Alfândegas.

A possibilidade de receber as informações da declaração aduaneira antes da chegada ou partida das mercadorias permite às Alfândegas proceder às formalidades exigidas, inclusive à liquidação dos direitos, antes da chegada material das mercadorias ao território aduaneiro. Em caso de exportação, trata-se das mercadorias que saem do território aduaneiro. Os erros podem ser comunicados à empresa com antecedência; as rectificações necessárias podem então ser realizadas, o que reduz os eventuais atrasos nas formalidades de desembaraço.

6.4.1 Processamento antes da chegada / partida das mercadorias

As informações da declaração aduaneira comunicadas antes da chegada da mercadoria ou antes da sua partida são processadas da mesma maneira que a declaração de mercadorias conforme descrito na Secção 6.4. A informação recebida antes da chegada das mercadorias ajuda as Alfândegas a tomar decisões relativas à admissibilidade e ao desalfandegamento das mercadorias.

6.4.2. Gestão de licenças, alvarás, certificados e outro tipo de autorizações

A importação e exportação de certas mercadorias estão regulamentadas. Para implementar e gerir essas restrições, as autoridades emitem licenças, alvarás, certificados, autorizações, etc. Esses documentos contêm uma descrição das mercadorias em causa e especificam quais são as categorias, a quantidade e o valor das mercadorias susceptíveis de serem importadas ou exportadas. Os procedimentos ligados ao ciclo de vida das licenças, alvarás, certificados e outro tipo de autorizações podem ser geridos eficazmente graças aos sistemas de TIC. Esses procedimentos incluem a emissão, a utilização, a anulação e a expiração de diversas autorizações. A manipulação por via electrónica das informações contidas nesses documentos contribui para a melhoria da gestão dos controles transfronteiriços e nomeadamente das restrições não-tarifárias. Este aplicativo é particularmente importante no contexto de uma abordagem de Janela Única, onde vários outros organismos de regulamentação dos fluxos transfronteiriços têm a incumbência de gerir o ciclo de vida das licenças, alvarás, certificados e outro tipo de autorizações.

6.5. Reconciliação de dados

A reconciliação ou confrontação electrónica de dados, por exemplo, os que estão nos sistemas de controle de inventário e de processamento da declaração de mercadorias, é uma das operações mais importantes para as Alfândegas. Qualquer discrepância entre os dados conferidos pode ser destacada e o sistema emite um relatório de sub/sobre declarações.

As técnicas informáticas de reconciliação de dados podem também ser aplicáveis ao regime aduaneiro de "importação temporária sujeita a reexportação no mesmo estado".

Como parte da informatização do sistema de contabilidade de receitas, os direitos devidos, conforme extraídos da informação referente à declaração das mercadorias, podem ser comparados com os registos, para produzir informação contabilística correcta e tempestiva. Nos casos que dizem respeito ao draubaque, o sistema de contabilidade pode ser usado para validar os pedidos.

6.6. Notificação da autorização de saída

(Norma Transitória 6.9)

Embora o processamento de declaração de mercadorias seja definitivamente uma área adequada para a informatização, a nota de autorização de saída electrónica pode ser implementada como uma iniciativa separada. Há muitas vantagens na interacção com os sistemas electrónicos de autorização de saída existentes e captação da referida informação de autorização de saída para distribuição via *internet* ou correio electrónico para um ou mais operadores comerciais. Ademais, pode ser implementado um sistema de notificação de autorização de saída electrónico mesmo que todas as transacções sejam processadas em papel. A distribuição tempestiva das autorizações de saída electrónicas pode trazer benefícios quer para as Alfândegas, quer para os operadores comerciais, em termos de redução do tempo para a autorização de saída.

6.7. Luta contra a fraude aduaneira

(Norma Transitória 6.9)

A vantagem da utilização das tecnologias de IC para efeitos de controle aduaneiro consiste na capacidade de tornar a informação acessível a todos os funcionários aduaneiros autorizados. A informatização permite examinar as informações contidas nas bases de dados de outros serviços de prevenção e de repressão, tais como os registos de polícia, arquivos de imigração, etc. A aplicação das tecnologias de IC permite também aos funcionários aduaneiros consultar de forma rápida e precisa vários dados, tais como os critérios de selecção, no intuito de identificar a sua utilidade e ajudá-los, assim, a reagir rapidamente em circunstâncias de mudança. Contudo, importa instaurar um equilíbrio apropriado entre, por um lado, a aplicação das disposições que sancionam operadores comerciais que infringem as leis e regulamentos em vigor e, por outro lado, a necessidade de oferecer aos demais, a maior transparência possível.

Para assegurar o cumprimento dos regulamentos aduaneiros, no sentido de fazer o uso eficiente dos escassos recursos, as Alfândegas devem empregar técnicas de selecção e de avaliação de riscos. Apesar destas técnicas não serem necessariamente dependentes da tecnologia de informação para a sua implementação, não podem realmente ser aplicadas eficiente e coerentemente sem esta tecnologia. Num ambiente informatizado, os mesmos princípios de selecção e de avaliação de riscos podem ser aplicados quer às mercadorias, quer aos viajantes.

6.8. Selecção

Entende-se por selecção a operação que consiste em determinar se as Alfândegas devem submeter uma remessa ou um viajante, em particular, a um controle mais rigoroso. Em um ambiente informatizado podem ser aplicados quatro “filtros” de selecção, a saber, os perfis internacionais, nacionais, locais e um sistema de selecção aleatória.

Os dois primeiros baseiam-se num sistema de perfis desenvolvidos tendo em conta os conhecimentos dos funcionários das Alfândegas (a nível internacional) e através de sistemas de análise de dados para avaliar o risco de perdas fiscais e o não cumprimento da legislação. A inteligência artificial e os sistemas especialistas tais como o sistema de reconhecimento de padrões podem ser muito úteis para facilitar a avaliação de riscos e a criação de perfis. (A identificação de riscos e os dados que constam habitualmente nos perfis são abordados em detalhe na Directiva da OMA relativa ao Controle Aduaneiro).

O criador do sistema deve estar ciente de que para a criação de um conjunto de perfis o sistema precisa de ser flexível e capaz de processar não apenas simples dados individuais mas também, combinações de dados relativamente complexas. O uso de combinações permite às Alfândegas refinar as suas capacidades de selecção. Por conseguinte, as Alfândegas podem, por exemplo, seleccionar apenas uma determinada remessa se proveniente de um país particular e não de um outro país. O Apêndice 2 e 3 a este documento descrevem a abordagem conceptual de um sistema de selecção.

A principal diferença entre os perfis internacionais/nacionais e locais é de que os internacionais/nacionais são obrigatórios para todas as estâncias aduaneiras ao passo que os perfis locais interessam apenas uma única estância aduaneira ou um pequeno grupo de estâncias aduaneiras. Contudo, a informação dos perfis locais deve ser usada como parte da análise geral de riscos e, quando for apropriado, integrada nos perfis nacionais. Todos os perfis devem ser revistos regularmente. Por razões de segurança, devem ser tomadas medidas para identificar as pessoas autorizadas a mudar os perfis, em ambos os níveis.

O sistema de selecção aleatório utiliza um algoritmo para seleccionar uma declaração para verificação adicional pelas Alfândegas.

É também importante que o sistema permita a monitorização da interacção coordenada entre os três níveis de selecção para que o número de verificações previsto não seja excedido.

O sistema terá que ser concebido de forma a garantir que todos os dados sejam avaliados tendo em conta os perfis internacionais/nacionais, mas apenas os dados próprios de uma região ou estância aduaneira devem ser avaliados à luz dos perfis locais. Geralmente incluem-se dispositivos que permitem aos gestores autorizados suspender, temporariamente, a aplicação de um perfil.

6.8.1. Gestão de Riscos

A gestão de riscos é fundamental para a selecção eficaz de remessas a verificar. (As metodologias necessárias para realizar a gestão de riscos estão descritas nas Directivas da OMA sobre Gestão de Risco).

«*Sistema integrado de gestão de riscos da Coreia*»

A gestão dos riscos baseando-se na tecnologia da informação e da comunicação é um elemento essencial para responder aos desafios das transacções transfronteiriças. As Alfândegas da Coreia (KCS) seleccionam e inspeccionam os viajantes, as mercadorias e os meios de transporte de alto risco com base nos resultados de uma análise de riscos. As KCS efectuam habitualmente uma análise dos riscos para verificar a posterior as transacções ilegais e os casos de evasão fiscal, e, além disso, elas implementaram em 2002 um armazém aduaneiro de dados. Os dados recolhidos provêm não só dos serviços aduaneiros mas também de outras instituições do Estado como o Ministério da Justiça, a Direcção Nacional de Impostos governamentais, o Ministério dos Negócios Estrangeiros e do Comércio. O Ministério dos Transportes Terrestres e das Questões Marítimas. A partir de 2008, as KCS começaram a implementar um sistema integrado de gestão de riscos com diversas funções:

- Integração e segmentação automáticas dos dados;
- Inclusão de informações personalizadas (por exemplo, para todos os funcionários séniores, médios ou operativos;
- difusão das informações e dos critérios de selecção; e
- combinação dos factores de risco por meio de indicadores complexos de selecção dos alvos.

(Fonte : Compêndio 2011 da OMA sobre a gestão dos riscos).

Os perfis de selecção dependem da qualidade da informação neles contida. A revisão regular dos perfis indicará aos funcionários aduaneiros que elementos de dados e que combinações de elementos de dados detectaram com êxito declarações fraudulentas. A análise da informação da declaração, propriamente dita, permite igualmente traçar tendências e identificar potenciais remessas de alto risco.

6.9. Controle antecipado de passageiros

A Informação Antecipada sobre o Passageiro (IAP) permite às Alfândegas acelerar o controle do passageiro. Os benefícios da IAP não podem ser obtidos nem esta pode ser usada eficientemente sem a cooperação entre as agências de controle fronteiriço (Alfândegas, polícia, imigração) e os transportadores (companhias aéreas e marítimas, etc.) As Directivas Conjuntas da IATA/CCA (Associação Internacional de Transporte Aéreo/Conselho de Cooperação Aduaneira) sobre a IAP especificam as informações máximas que as Alfândegas podem exigir, bem como os padrões a serem utilizados. Já existem os padrões internacionais de mensagens que permitem o intercâmbio de dados da IAP.

6.10. Contabilidade das receitas

Muitas Administrações Aduaneiras têm a arrecadação de receitas como uma das suas funções principais. Portanto, a informatização do processo de contabilidade das receitas é parte essencial de qualquer sistema aduaneiro integrado de TI. Um sistema de contabilidade de receitas deve:

- ❖ Contabilizar os direitos arrecadados e reembolsados;
- ❖ Proporcionar um mecanismo para a cobrança e reembolso dos direitos no momento do desembaraço aduaneiro;
- ❖ Proporcionar um mecanismo para o diferimento do pagamento dos direitos por um período especificado.

A aplicação de um sistema de pagamento diferido exige o estabelecimento de um sistema de registo dos operadores comerciais. Este sistema deve controlar as garantias e identificar as receitas a pagar por um período de tempo especificado. Os detalhes de um sistema de registo do operador comercial estão estabelecidos na secção 6.13 do presente documento.

Em um sistema de contabilidade das receitas as tarefas seguintes são adequadas à aplicação de TI:

- Controle informatizado da garantia dos direitos;
- Manutenção da contabilidade do pagamento diferido pelos operadores económicos; e
- Cálculo rápido e preciso das receitas.

No momento do desembaraço aduaneiro, os direitos e demais imposições podem ser arrecadados mediante aceitação de numerário, cheques, saques bancários, cartões de crédito e cartões de débito do declarante e/ou mediante o uso de métodos de pagamento por transferência electrónica de fundos (TEF), em tempo real.

As Alfândegas devem estar em condições de reconciliar os direitos realmente arrecadados com total dos direitos calculados pelo sistema de tratamento das declarações de mercadorias. Em princípio, o sistema deve registar o montante de direitos arrecadados por cada transacção efectuada correspondente ao número de declaração atribuído pelas Alfândegas e os meios de pagamento. Normalmente, os montantes pagos por tipo de direitos e taxas (imposto, direitos aduaneiros, taxas de exportação, etc.) são igualmente registados, permitindo, desta forma, que a autoridade aduaneira determine, para cada declaração, o montante arrecadado por tipo de direito.

A aceitação de cartões de pagamento significa que as Alfândegas devem instalar a tecnologia necessária de ligação entre as estâncias aduaneiras e o sistema bancário, no sentido de validar os detalhes do cartão e assegurar o pagamento dos montantes totais dos direitos.

Existe uma diferença significativa entre um sistema de pagamentos diferido e a cobrança dos direitos e taxas no momento do desembaraço das mercadorias. Os referidos sistemas são baseados na manutenção de informação individual de contabilidade para cada declarante ou operador comercial autorizado. Normalmente, acorda-se um limite máximo de direitos cujo pagamento é diferido entre o operador comercial, Alfândegas e o banco do operador comercial por meio da prestação de uma garantia. Os detalhes deste montante, juntamente com os detalhes de cada transacção (número da declaração aduaneira e montante dos direitos a pagar) são mantidos numa base de dados ligada ao sistema de registo do operador comercial. O controle e a gestão de um tal sistema manual requer vastos recursos e estão mais propícios à fraude e ao erro. Além disso, não é prático operar um sistema manual de pagamento diferido numa base nacional (isto é; uma conta para cada operador comercial para cobrir as transacções de todos os locais). Contudo, a implementação de um sistema informatizado de arrecadação de receitas facilita o funcionamento de um sistema nacional de pagamentos diferidos.

Num ambiente informatizado, o balanço de contabilidade mais recente dos pagamentos diferidos está sempre acessível, ao passo que num ambiente manual isto não pode ser garantido. Além disso, num ambiente manual subsiste sempre o risco dos montantes dos direitos diferidos excederem o montante da garantia. Isto pode expor as Alfândegas à perda de receitas. Por outro lado, um sistema informatizado de contabilidade de receitas não permitirá aos operadores comerciais exceder o limite da garantia. Se os montantes dos direitos de uma transacção particular forem superiores ao saldo da garantia, o sistema alertará as Alfândegas.

Nos casos de troca electrónica de dados o sistema das Alfândegas enviará uma mensagem de resposta ao operador comercial indicando que os direitos não podem ser diferidos

devido a insuficiência de crédito. O operador comercial, em qualquer momento, pode solicitar informação relativa ao saldo da conta dos pagamentos diferidos ou obter um extracto dessa conta.

Quando os direitos se tornam exigíveis, o montante total devido por cada um dos operadores comerciais autorizados juntamente com os seus dados bancários (número de conta, código da agência, etc.) devem ser transferidos para o banco relevante. A este respeito deverá haver um acordo entre as Alfândegas e os bancos relativamente ao padrão de troca da informação e ao meio para a referida troca (EDI, cassete, disco, *internet*). Os padrões internacionais de mensagens concebidos para serem usados em ambientes de EDI estão disponíveis para a transmissão da informação de pagamento.

6.11. Estatísticas do comércio externo

Sendo a base de dados de declarações a principal fonte de estatísticas do comércio externo, os requisitos nesse domínio devem ser tomados em consideração durante a fase da sua concepção.

6.12. Sistema de Gestão da Informação (SGI)

Uma vez gravados electronicamente, os dados podem ser analisados mediante o uso de *softwares* proprietários ou programas concebidos internamente. Antes de se escolher uma destas opções é essencial realizar uma análise dos tipos de consultas e de relatórios necessários. As ferramentas de análise de dados podem ser usadas para fazer operações simples, tais como extrair todas as ocorrências relativas a um nome, ou complexas, como cruzar dados relacionados a partir de vários arquivos para produzir um relatório não disponível de outra forma.

Estas técnicas são de grande valor na investigação e luta contra a fraude. Contudo, o SGI também pode ser usado pelos gestores para assegurar que os recursos sejam utilizados eficazmente. Os relatórios podem ser produzidos tendo como base o número de declarações processadas numa determinada estância aduaneira, a identificação de picos e baixas no fluxo de trabalho, tipos de remessas, etc.

6.13. Realização de relatórios

Ao criar um sistema aduaneiro informatizado, as Administrações Aduaneiras precisam de desenvolver um meio automatizado de produzir posteriormente relatórios pré-formatados em base diária, semanal, mensal ou anual. Pode também ser conveniente desenvolver uma ferramenta de relatórios *ad-hoc* que permita aos funcionários e gestores criar os seus próprios relatórios. Um sistema bem concebido de realização de relatórios permite às Alfândegas criar os seus próprios relatórios com base nos vários tipos de dados contidos nos seus sistemas.

6.14. Armazenagem de dados

As administrações precisam de ter em consideração os requisitos legais para a armazenagem de dados. Os dados armazenados podem também facilitar a concepção de relatórios, bem como ser útil para a criação de ferramentas de luta contra a fraude e de avaliação de riscos.

Existem várias formas para armazenar dados, incluindo em discos magnéticos tais como discos rígidos e fitas magnéticas. As novas tecnologias permitem também que os dados sejam armazenados em discos ópticos (CD e DVD).

6.14.1 Recuperação de dados

Um sistema de recuperação de informação permite às Alfândegas o acesso *on-line* aos dados de natureza histórica. Os dados da declaração que tenham sido inseridos ou transmitidos por EDI podem ser consultados *on-line* ao nível de cabeçalho/rodapé, subtítulo e da linha de entrada. Um sistema de recuperação eficaz permitirá ao utilizador consultar todas as versões dos dados introduzidos sendo a versão actual a primeira a ser apresentada.

6.14.2. Exploração de dados

A exploração de dados pode ser descrita como uma tecnologia de informação que emprega várias técnicas para extrair informação compreensível, útil e oculta de uma quantidade de dados armazenados.

A exploração de dados torna possível a descoberta de tendências e padrões ocultos em grandes quantidades de dados e por esta razão é muito útil para a avaliação de riscos. O resultado pode tomar a forma de tendências ou padrões implícitos nos dados armazenados.

6.15. Sistema de registo dos operadores comerciais

Os Sistemas de Registo dos Operadores Comerciais são frequentemente desenvolvidos como parte de um sistema contabilidade de pagamento diferido mas podem ser usados para outros fins, por exemplo; identificar as facilidades especiais atribuídas pelas Alfândegas a um ou a outro operador comercial. Estes sistemas contêm habitualmente as informações de base relativas aos operadores comerciais, tais como:

- número único de registo do operador comercial (comum em todas as instituições, onde for possível);
- avaliação dos operadores comerciais
- dados dos operadores comerciais (nome, endereço, número de telefone, etc.);
- dados da conta bancária (nome do banco, endereço, número da conta);
- montante da garantia (o valor monetário máximo garantido pelo banco do operador comercial);
- data do débito dos direitos (data em que os direitos devem ser debitados da conta do operador comercial);
- facilidades especiais dos procedimentos aduaneiros (declarações periódicas, armazém afiançado, etc.);
- uma lista de relações com uma filial e/ou agências, onde estas existirem.

O declarante deverá indicar o número de registo em todas as declarações. Assim, poderão ser comparadas as informações relativas aos direitos com conta de pagamento diferido, ou uma medida ou um regime aduaneiro particular poderá ser implementado. Cada conta individual deve ter um número de declaração e data juntamente com o montante total de direitos da declaração. Deve-se também manter um balanço corrente do montante actual da garantia.

O sistema de registo do operador comercial deve estar acessível apenas a outros sistemas aduaneiros e, devido aos imperativos em matéria de protecção de dados confidenciais, o acesso às Alfândegas deve ser rigorosamente controlado com medidas de segurança apropriadas e autorizações de acesso.

6.16. Trânsito aduaneiro

O trânsito aduaneiro tem como princípio básico, permitir que as mercadorias sejam transferidas de uma estância aduaneira para outra, no mesmo território aduaneiro ou em outro, sem a cobrança dos direitos ou taxas aplicáveis sob a condição de que todas as obrigações relacionadas com a selagem aduaneira, prazos, segurança, etc, sejam satisfeitas.

O Intercâmbio Electrónico de Dados melhoraria a eficiência e a eficácia do trânsito aduaneiro. Os movimentos de trânsito e transbordo podem ser mais facilmente controlados num ambiente informatizado. A informação da declaração pode ser captada no momento da entrada e depois verificada e apurada quando as mercadorias abandonam o território aduaneiro. Realizam-se verificações de credibilidade e de validação básica dos dados e o sistema atribui um número à declaração. As Alfândegas do ponto de partida têm acesso aos dados originais mediante o número da declaração.

O uso de sistemas informatizados permite que qualquer movimento de trânsito incompleto ou incoerente seja identificado de uma maneira tempestiva e mais eficiente.

O controle em matéria de trânsito de trânsito beneficiaria consideravelmente do intercâmbio de informação entre as Administrações Aduaneiras. O intercâmbio tempestivo da referida informação ajudaria a reduzir os riscos de fraude no trânsito. Os benefícios do uso das tecnologias de IC no trânsito nacional aplicam-se, igualmente, ao trânsito internacional.

O uso do EDI em procedimentos de trânsito conhece actualmente novos desenvolvimentos. O novo sistema de trânsito informatizado (NCTS) da CE e o sistema que está a ser desenvolvido pela União Internacional de Transporte Rodoviário, o TIR Seguro, constituem dois exemplos recentes. A CEE / ONU desenvolveu um padrão electrónico para o TIR (eTIR).

6.17. Outras aplicações

(Normas Transitórias 9.3 e 9.4)

Além das áreas de aplicação já mencionadas, as outras funções aduaneiras que podem ser informatizadas incluem:

- o reembolso dos direitos aduaneiros já pagos (draubaque);
- o controle de contingentes;
- a gestão das multas aduaneiras, penalidades, etc;
- Informação Pautal Vinculativa (IPV);
- as decisões em matéria de classificação;
- o entreposto e a armazenagem sob controle aduaneiro;
- aceitação da declaração (manifesto confirmado por declarações subsequentes, declarações de transporte confirmadas pela chegada das mercadorias, etc.).e
- as aplicações de gestão de recursos humanos

6.18. Informatização de escritórios

Como todas as organizações, as Alfândegas exercem um certo número de funções

administrativas. A "informatização de escritórios" vem apoiar uniformemente as operações administrativas gerais e rotineiras, a seguir mencionados:

Operações de Base	Operações Administrativas	Sistema de Apoio
Registo de cartas, documentos, etc.	Registo de dados Recolha de dados	Base de dados *Software* de pesquisa
Armazenagem e distribuição	Arquivos Recuperação Reprodução Processamento de texto Comunicação verbal Gestão de documentos electrónicos	*Scanning*/gerador de palavras-chave Disco óptico/base de dados Procura por palavras-chave em disco óptico/base de dados Difusão por correio electrónico externo, fax, produção de discos ópticos, impressão automática em impressoras de rede Processador de texto Telefone
Comunicação e planificação	Comunicação de dados	Correio electrónico *e* agenda electrónica, fax, telefone.
Uso da informação	Análise da informação Funções aritméticas	Folha de cálculo de ferramentas de pesquisa
Apresentação	Apresentação de dados	GUI (Interface Gráfica do Utilizador) Pacotes de *softwares* integrados

A informatização de escritórios deve incluir um conjunto equilibrado de ferramentas, seleccionadas para satisfazer os requisitos do utilizador final. É importante introduzir um ambiente padrão de informatização de escritórios, constituído normalmente por, pelo menos, uma Interface Gráfica do Utilizador (GUI), um processador de texto e um de folha de cálculo.

O telefone na qualidade de ferramenta da tecnologia de IC pode ser de grande valor. As administrações aduaneiras estão cada vez mais a introduzir infra-estruturas telefónicas para apoiar a execução dos seus programas e a fornecer aos seus clientes respostas relacionadas com as questões dos programas. Trata-se de uma ferramenta tecnológica valiosa que pode ser introduzida num programa sem custos elevados para a administração.

6.19. Intranet e Extranet das Alfândegas

O aparecimento do comércio electrónico teve também um impacto nos serviços aduaneiros. Com efeito, as Alfândegas estão, cada vez mais, a tornar-se parte da rede electrónica dos poderes públicos (*e-Government)* oferecendo os seus serviços aos seus clientes, por meio da *internet. e-Government* diz respeito às comunicações internas e externas e pode facilitar bastante a difusão das informações oficiais, quer a nível interno, quer externo. Se implementado correctamente, o conceito de Alfândegas *on-line* melhoraria significativamente os serviços prestados aos operadores comerciais e ao público. Contudo, tal como na introdução da tecnologia de informação em geral, os benefícios totais de um sistema informatizado só podem ser alcançados se os procedimentos e processos internos forem revistos e, onde for necessário, emendados ou mesmo abolidos antes da sua implementação.

Um sítio das Alfândegas na Internet ao qual o público tem acesso ajudará a administração a facilitar o acesso e a difusão das informações da regulamentação aduaneira do domínio público, em particular para os viajantes e os operadores do comércio internacional. O sítio *web* garantirá também que as informações relevantes sejam disponibilizadas ao público de uma maneira rentável e facilmente acessível.

Uma *Intranet* abrangendo toda a organização garantirá o acesso a todos os sistemas a partir de um único terminal (PC) e a gestão centralizada de todas as ferramentas e bases de dados relevantes. A *Intranet*, sítio onde toda a informação e documentação recebida e preparada pela organização se encontra disponível electronicamente, reduz a circulação de documentos em papel e o seu arquivo, melhorando o fluxo de trabalho interno.

Em 1999, o Conselho da OMA adoptou uma Recomendação sobre o uso da WWW (Rede de Alcance Mundial) para as Alfândegas. Trata-se do primeiro passo muito importante no processo do encorajamento das Administrações Aduaneiras para a entrada *on-line* (Ver Apêndice 10). A partir de Novembro de 2003, o Sítio da OMA estabeleceu ligações com mais de 140 Administrações Aduaneiras em todo o mundo.

7. Terceirização das funções aduaneiras

7.1 Visão

A terceirização intervém quando uma entidade compra produtos ou serviços ou delega parte das suas funções a uma entidade externa, geralmente especializada na terceirização desses produtos, serviços ou actividades, em vez de realizar ela própria essas tarefas.

7.1.1 Terceirização, deslocalização e internalização

A deslocalização é outro termo utilizado no contexto da terceirização, quando a actividade que decidiram terceirizar é realizada noutro país. A terceirização pode intervir no país ou no estrangeiro.

Qualquer função que não seja uma competência de base pode ser externada junto de outras entidades habilitadas a realizá-la. Por vezes, para evitar perder o controle de uma actividade, as entidades contratam recursos exteriores, que fazem de seguida, parte da equipa. Neste caso, o objectivo é tirar partido das competências do recurso externo que, embora não esteja inscrito na folha de pagamentos do serviço, adoptará os valores e a cultura do serviço e participará plenamente nas suas actividades quotidianas. Esta actividade, denominada internalização, é diferente da terceirização. Estima-se geralmente que as actividades ou os serviços terceirizados não devem ter valor estratégico para a entidade e que, para atrair as competências que tenham uma importância estratégica, é preferível recorrer à internalização.

7.1.2 Crescimento da terceirização

O crescimento da terceirização, nestes últimos anos, deve-se em parte a uma mudança generalizada da filosofia das empresas, resultante nomeadamente em uma larga medida do aparecimento e da utilização das TIC, e da necessidade de dispor de um especialista da TI que não faça necessariamente parte das funções principais ou das funções essenciais da entidade.

As entidades esforçaram-se portanto para identificar uma “competência de base”, uma combinação única de experiencia e de conhecimentos relativos às actividades principais da entidade. Todos os aspectos operacionais da entidade estão organizados em torno das funções de base, e qualquer actividade ou função que não seja necessária para apoiar as actividades principais é então terceirizada.

Hoje, a terceirização é utilizada, não só, pelas empresas, mas começa igualmente a ser utilizada pelos poderes públicos.

As funções de uma entidade podem ser terceirizadas na íntegra ou de maneira selectiva. A terceirização total pode causar o desmantelamento de divisões ou de serviços inteiros e a transferência a um vendedor externo da totalidade das responsabilidades ligadas a um produto, um serviço ou uma função. A terceirização selectiva pode, por outro lado, ser centrada em uma tarefa ou função única, para a qual existem competências mais eficientes fora da entidade que podem ser geridas mais eficientemente por um especialista externo.

A decisão de terceirizar é de natureza estratégica pois tem uma incidência sobre a concepção da organização administrativa e corresponde à escolha essencial, em relação à organização administrativa, das funções para as quais conhecimentos são desenvolvidos e alimentados a nível interno, e das funções para as quais esses conhecimentos são comprados. Os motivos para a terceirização podem incluir, não só, a diminuição dos custos, mas igualmente a reorientação dos recursos para áreas que interessem a entidade em primeira instância e que

estão harmonizados com as competências actuais e de base. Para as funções não essenciais, é aconselhável, de um ponto de vista comercial, utilizar os recursos humanos mais experientes disponíveis fora da entidade, por uma questão de eficácia e de rentabilidade.

Estima-se que a vantagem real reside na possibilidade de reafectar os recursos às funções mais importantes das Alfândegas, eventualmente dando mais importância às competências de base dos funcionários aduaneiros.

7.2 A terceirização no seio das Alfândegas e áreas que podem ser terceirizadas: actividades essenciais e actividades não essenciais.

O papel das Alfândegas nas trocas internacionais não cessou de evoluir. O comércio mundial assenta cada vez mais na circulação rápida dos bens e dos serviços nas fronteiras. A facilitação das trocas é considerada como um elemento importante da política económica de um país.

A utilização dos progressos das TIC permite reorganizar os procedimentos com flexibilidade. As empresas esperam serviços melhores e desejam poder trabalhar a partir dos seus locais.

As Alfândegas desempenham um papel essencial na cadeia logística internacional. Espera-se que as Alfândegas reduzam o custo das transacções e da gestão de existências numa base "*just-in-time*", com vista a garantir a competitividade. As Alfândegas devem portanto responder a essas expectativas oferecendo os seus serviços atempadamente.

Estes últimos anos, a importância acrescida dada à segurança das trocas obrigou as Alfândegas a redefinir a sua maneira de trabalhar. Elas devem portanto elaborar um método que permita não só satisfazer as necessidades divergentes da luta contra a fraude e da facilitação de maneira mais rentável, mas igualmente oferecer de maneira simples às empresas internacionais serviços de qualidade e garantir a circulação ininterrupta dos bens e dos serviços nas fronteiras. O papel das Alfândegas foi portanto alargado e inclui o de prestador de serviços.

Não se espera das Alfândegas que terceirizem as suas funções essenciais na área da segurança, do respeito das proibições e das restrições, da protecção da sociedade ou da arrecadação de receitas; para os mecanismos de entrega, a terceirização pode ser o complemento das capacidades internas. A maioria dos serviços oferecidos requerem a utilização das TIC, o que exige competências profissionais em matéria de TIC que não fazem parte das competências das Alfândegas. De facto, a terceirização como uma opção torna-se necessária quando a qualidade do serviço é da máxima importância. Neste contexto, a terceirização garante não só a eficácia, mas constitui igualmente um valor acrescentado para as empresas. As actividades aduaneiras que podem ser terceirizadas, permitindo as Alfândegas centrar-se nas suas funções essenciais, são nomeadamente as seguintes :

i) Gestão e funcionamento da infra-estrutura das Alfândegas em matéria de TI;

ii) Difusão da informação;

iii) Actualização do sítio *web*;

iv) Gestão das instalações;

v) Gestão e actualização dos aplicativos;

vi) Serviço de assistência e serviços de ajuda;

vii) Publicidade e relações públicas;

viii) Segurança da TI e auditoria das áreas de avaliação da segurança, da política em matéria de segurança e dos serviços geridos e seguidos, segurança dos locais.

7.3 Vantagens da terceirização

7.3.1 Regresso às actividades essenciais

Ao terceirizar as funções não essenciais junto de uma entidade externa, as Alfândegas podem centrar-se nas áreas sob sua jurisdição e cumprir a sua missão em matéria de gestão da luta contra a fraude e de facilitação.

A terceirização permite recorrer a conhecimentos e a uma perícia que o serviço não possui, e contribui directamente para a qualidade e a eficácia dos serviços que esperam os meios comerciais internacionais.

7.3.2 Responsabilidade

A terceirização assenta sobre o princípio, partilhado pela empresa e o vendedor, segundo o qual esses acordos requerem um serviço de qualidade em troca de um pagamento. Esta responsabilidade, definida no quadro de acordos sobre o nível de serviço, é prática e legal, e tem uma incidência financeira. O mesmo não se aplica quando o serviço é prestado por recursos internos.

7.3.3 Qualidade

O facto de não contratar recursos internos para tarefas para as quais não existem recursos no seio da entidade, permite evitar o problema dos comportamentos pouco eficientes e dos maus resultados.

7.4 Desafios da terceirização

7.4.1 Questões ligadas à qualidade dos serviços

Em qualquer situação onde tarefas ou actividades são externadas, existe sempre o risco de um controle de qualidade mau. Isto é particularmente verdade se uma actividade deve ser realizada pelas Alfândegas e pelo vendedor, sendo portanto as responsabilidades partilhadas. A terceirização funciona melhor quando uma actividade completa é terceirizada e que a responsabilidade impende portanto apenas sobre uma única entidade. Mais importante ainda, a capacidade do vendedor de se adaptar rapidamente à modificação da legislação e dos procedimentos, na sequência de uma decisão de ordem política, afecta a prestação do serviço e o custo do serviço. O desafio consiste em determinar o tipo de relações em matéria de terceirização, que responderá melhor às necessidades e a defini-lo nos acordos sobre o nível de serviço.

Outro aspecto importante da terceirização, muitas vezes negligenciado, é que a responsabilidade global do serviço prestado pelo vendedor recai sobre as Alfândegas. Não há cessão da responsabilidade pela simples razão que a tarefa foi confiada a uma outra entidade. O vendedor presta o serviço aos clientes em nome das Alfândegas e uma ligação estreita entre as Alfândegas e o vendedor é indispensável para respeitar as normas de prestação de serviços. Convém, portanto, avaliar regularmente a maneira como o vendedor realiza as suas tarefas.

7.4.2 Questões ligadas aos recursos humanos

Certos argumentos opõem-se à terceirização do ponto de vista dos recursos humanos. Teme-se de facto que a terceirização leve a uma perda de conhecimentos no seio da entidade e de lealdade por parte do pessoal. A menos que o serviço terceirizado seja um bem – regularmente disponível ou um serviço fácil de substituir – é preferível fazê-lo no seio da entidade.

Se os recursos humanos são indispensáveis para o sucesso da entidade, tem que se investir nesses recursos. Mais vale incorrer despesas para formar novamente o pessoal que realizar poupanças reduzindo as despesas de terceirização. Recursos humanos formados e informados assegurarão a perenidade do conhecimento das operações no seio da entidade.

As possibilidades de internalização podem igualmente ser examinadas quando os conhecimentos necessários estão temporariamente indisponíveis.

A terceirização e a internalização apresentam igualmente um desafio do ponto de vista da deslocalização do emprego além das fronteiras nacionais.

No entanto, a terceirização pode, igualmente, permitir reduzir a carga de trabalho dos empregados, nomeadamente quando as Alfândegas são confrontadas com uma multiplicação das suas responsabilidades, mas sem beneficiar de um acréscimo dos seus recursos humanos. Ao libertar os funcionários das Alfândegas de tarefas entediantes, abrem-se novas oportunidades de formação profissional.

7.4.3 Questões ligadas à segurança

A terceirização dos serviços cria fluxos de informações e de conhecimentos fora da entidade. Preocupações de segurança nascem quando os dados ou as informações sensíveis de clientes são transmitidos sem autorização, violando a legislação nacional. O carácter confidencial e a protecção dos dados não são necessariamente infracções tão graves no estrangeiro. O roubo de dados pode afectar o cliente no plano financeiro e obrigar a entidade que terceiriza, responsabilidades inaceitáveis no plano legal podendo ir até à fraude. Limitar o aceso às fontes de informações postas à disposição do vendedor constitui um problema técnico. Compromissos podem afectar a entidade de uma maneira inaceitável.

Convém limitar o acesso às informações ao pessoal autorizado, em função das responsabilidades. Mecanismos de controle apropriado devem ser concebidos com cuidado para dar acesso segundo as necessidades; o princípio da recusa do acesso a todas as informações, salvo se for absolutamente necessário para as tarefas do pessoal do vendedor, deve por exemplo ser aplicado de maneira estrita. O acesso às informações deve, igualmente, ser controlado e verificado periodicamente.

7.5 Conclusão: como estabelecer o equilíbrio apropriado

Face à multiplicação constante das responsabilidades, das restrições em matéria de custos e de recursos humanos, da necessidade de dispor de competências técnicas especializadas para oferecer serviços de qualidade, e das oportunidades que oferecem os progressos da tecnologia da informação, a terceirização é a via a seguir.

Para que a terceirização seja eficaz, convém definir as necessidades do serviço e identificar um vendedor capaz de integrar eficazmente todas as funções terceirizadas de maneira a não ter que procurar vendedores individuais para cada função.

A terceirização não deve ser considerada como a simples delegação de uma tarefa a uma entidade externa, mas como uma relação da parceria mutuamente vantajosa, na qual as Alfândegas e o vendedor se envolvem, quotidianamente, para oferecer serviços em função de normas determinadas previamente e de maneira duradoura.

O contrato de terceirização deve definir claramente as responsabilidades e os critérios de desempenho, as regras de confidencialidade e os direitos de propriedade das ideias ou técnicas novas. Os acordos referentes ao nível de serviço constituem um meio concreto de avaliar os resultados obtidos em matéria de desempenho. O contrato deve igualmente comportar um meio de pôr fim às relações se o serviço prestado não responde às expectativas.

8. Interfaces entre as aplicações de TI

As Alfândegas devem conceber os seus sistemas informáticos segundo uma arquitectura informática integrada podendo compreender os subsistemas de aplicativos e as bases de dados abaixo. Quando os interfaces são desenvolvidos no seio dos subsistemas explorados pelas Administrações Aduaneiras, conduzem a uma integração mais estreita entre as diferentes funções da instituição. Para construir um ambiente de Janela Única para o comércio, pode ser necessário construir interfaces com os sistemas de outras instituições governamentais interessadas pelos controles transfronteiriços. Interfaces de sistemas podem igualmente ser desenvolvidos para sustentar a troca de informações com outras Administrações Aduaneiras (por exemplo, as Alfândegas em Rede Internacional).

Subsistemas de aplicação:

- Sistema de processamento da declaração de importação;
- Sistema de processamento da declaração de exportação;
- Sistema de processamento da declaração de trânsito;
- Sistema de processamento da declaração de impostos indirectos;
- Sistema do movimento e controle de impostos indirectos;
- Sistema de draubaque;
- Sistema de gestão de riscos;
- Sistema de luta contra a fraude.

Estes sistemas de informação apoiam os principais regimes aduaneiros aplicáveis às mercadorias São necessários interfaces para permitir que se comuniquem. Por exemplo; os sistemas de trânsito precisam de interfaces com sistemas de exportação e importação.

Base de dados de administração

- Base de dados de registo dos operadores comerciais
- Esta base de dados pode conter dados do operador comercial, as garantias prestadas, para que fim, até que montante, por que banco – e acordos aduaneiros especiais, tais como procedimentos simplificados;
- Base de dados da pauta integrada (nomenclatura)
- Incluindo as medidas nacionais e internacionais;
- Base de dados de contabilidade das receitas;
- Base de dados de selecção;
- Base de dados de declarações;
- Base de dados de pagamentos diferidos.

A arquitectura de informação deve garantir o uso comum de dados armazenados nas Alfândegas. Cada base de dados pode ser usada por vários subsistemas de aplicação.

Para efeitos de gestão de bases de dados recomenda-se que os dados estreitamente relacionados com os outros sejam armazenados numa base de dados única. Isto significa que os dados primários e os dados de gestão relevantes devem ser armazenados na base de dados da mesma administração, sempre que seja possível. A identificação de relações de dados e a organização de dados deve fazer parte da análise inicial dos sistemas.

Recomenda-se que, no momento da concepção dos sistemas de informação, a parte logística dos procedimentos aduaneiros (processamento) seja separada dos dados relacionados com a aplicação aduaneira (arquivos, bases de dados). Isto facilita a reutilização dos componentes funcionais do sistema e torna mais eficiente e eficaz a actualização dos sistemas de informação. O Apêndice 4 dá um exemplo das relações entre alguns dos principais procedimentos e as correspondentes bases de dados.

Em um ambiente de Janela Única, os interfaces servem frequentemente para ligar os sistemas aduaneiros aos explorados por outras instituições do Estado. (Queiram consultar o Compêndio da OMA relativamente à forma de construir um ambiente de Janela Única). Os interfaces electrónicos podem igualmente ser integrados para comunicar com as outras Administrações Aduaneiras. Para uma descrição inicial das Alfândegas em Rede Internacional (DRI), queiram consultar a Secção 9.3.

8.1 Arquitectura orientada para os serviços

A facilidade com que diferentes aplicativos são elaborados e integrados depende da maneira como foram construídos e montados. Cada aplicativo ou módulo contribui para dispensar um conjunto de serviços que visam assegurar as funções essenciais de controle das importações, das exportações e do trânsito mas também facilitar as trocas.

A arquitectura orientada para os serviços (ou SOA, isto é, «*Service-Oriented Architecture»*) realça antes de mais os serviços para as empresas. Ela não enfatiza a infra-estrutura técnica (servidores, armazenagem, etc.) nem os serviços técnicos conexos. A SOA é uma abordagem de arquitectura tecnologicamente neutra. Esta abordagem está solidamente ancorada nos serviços às empresas e constitui uma escolha razoável para conceber a arquitectura de soluções de TI onde devem estar integrados diferentes elementos de aplicação .

A arquitectura orientada para os serviços pode facilitar a implementação de mudanças em sistemas de informação, e ligar módulos e funcionalidades diferentes. Os sistemas informáticos tradicionais foram constituídos integrando de forma rígida material/*hardware*, *softwares* e redes, dificultando a sua implementação. A arquitectura orientada para os serviços aconselha o desenvolvimento de aplicativos de *software* utilizando componentes fáceis de juntar e desenvolver. Esses elementos constitutivos não são *softwares*, mas sim serviços para as empresas que são prestados para responder a necessidades específicas de empresas. Serviços frequentemente utilizados podem ser novamente montados para criar novos serviços. A OASIS (*Organization for the Advancement of Structured Information Standards* ou Organização para o Avanço de Padrões de Informação Estruturados) desenvolveu um modelo padrão de referência para a arquitectura orientada para os serviços (Comité técnico da OASIS sobre a SOA, 2006).

O conceito de componentes de serviços reutilizáveis/recuperáveis é extremamente útil. Apesar das diferenças nos domínios da regulamentação, a maioria das entidades reguladoras dos fluxos transfronteiriços necessita serviços operacionais comuns. Estes referem-se à inspecção da carga, da tripulação e dos meios de transporte, à verificação documental, ao registo dos resultados dos testes, à recolha de amostras, à liquidação dos direitos e demais imposições aduaneiras, ao quadro de avaliação de riscos, etc. Estas componentes de serviço são reutilizáveis/recuperáveis não só para operações comerciais, mas igualmente para os *softwares* subjacentes. Se o objectivo das inspecções pode variar entre órgãos do Estado, as etapas do processo são as mesmas, e se os parâmetros de cálculo dos direitos e demais imposições podem variar, todos estão ligados ao processo de liquidação e de arrecadação. Os serviços de pagamento podem servir para todos os pagamentos que surjam/ocorram durante o desembaraço da mercadoria.

As componentes da tecnologia da informação (TI) nas quais se baseiam os serviços reutilizáveis/recuperáveis são elementos constitutivos que podem associar-se de maneira flexível.

É precisamente o que permite a reutilização de componentes. Essas possibilidades de combinação flexível reduzem o impacto das mudanças. A arquitectura orientada para os serviços baseia-se em uma terminologia corrente onde o utilizador do serviço (que é uma componente de *software*) necessita um serviço de um prestador de serviços (uma outra componente de *software*). A troca de pedido de serviço e de prestação de serviços baseia-se em mensagens e a qualidade do serviço rege-se por contratos de serviço entre as componentes de serviço em interacção.

As características exigem que um «serviço» seja uma unidade autónoma cujo desempenho não dependa do estado dos outros serviços. Trata-se da separação lógica de funcionalidades autónomas. Este carácter autónomo de uma componente de serviço permite aos técnicos da área de desenvolvimento de *softwares* retirar, modificar e substitui-la sem que isso tenha qualquer impacto sobre outras componentes. Os serviços podem ser orquestrados. Isto implica que serviços possam ser reajustados ou reorganizados para adaptarem-se ao objectivo comercial. Trata-se de um trunfo considerável para o tratamento de processos operacionais em um ambiente de Janela Única. O esquema abaixo ilustra a capacidade de componentes SOA de estarem orquestrados como se segue:

Avaliação dos riscos/ Serviço de avaliação dos riscos/ Inspecção das mercadorias/ serviço de inspecção material/ Verificação documental/ Orquestração n.º 1

Avaliação dos riscos/ Serviço de avaliação dos riscos/ Inspecção das mercadorias/ serviço de inspecção material/ Verificação documental/ Orquestração n.º 2

A comunicação entre os diferentes serviços passa por mensagens. Para garantir a boa colaboração entre os serviços, essas mensagens devem ser interoperáveis e compatíveis com as diferentes plataformas. Essas mensagens devem ser capazes de descrever e descobrir serviços. Tudo deve ser fiável e seguro, baseando-se em normas da indústria.

Uma das formas de assegurar o interface entre os diferentes aplicativos existentes consiste em modificá-los para que eles façam parte de uma Arquitectura orientada para os serviços (SOA). Este processo chama-se «preparação para a SOA». Recomenda-se que se recorra a ele para assegurar a integração entre os aplicativos.

9. Troca de informação

(Normas 3.11 e 7.2)

9.1 Troca de informação com os operadores comerciais

O conceito de troca de informações entre as Alfândegas e os operadores comerciais evoluiu, para finalmente desembocar em uma abordagem de "Janela Única". Esta noção de Janela Única impôs-se recentemente para o comércio internacional e as trocas regulamentares transfronteiriças. A Janela Única procede à análise dos controles oficiais do ponto de vista do operador comercial e pondera todas as interacções possíveis entre os operadores comerciais e os organismos de regulamentação fazendo abstracção dos departamentos no seio da Administração. Uma tal abordagem destaca inegavelmente todas as redundâncias nos procedimentos, as repetições nas formalidades e globalmente a falta de rentabilidade no momento da realização das formalidades ligadas à regulamentação transfronteiriça. Esta abordagem analítica permite identificar uma serie de soluções para simplificar consideravelmente o interface entre a Administração e os operadores comerciais dando uma nova orientação aos procedimentos e reorganizando os dados necessários para a regulamentação.

Existem diferentes tipos de interacções entre as Alfândegas e os operadores comerciais, no entanto as principais trocas de informações entre as Alfândegas e os operadores comerciais tem a ver com a importação e exportação de mercadorias.

Existem várias normas que permitem apresentar informações electrónicas sob a forma de ficheiros informáticos. Trata-se de normas de sintaxe. A norma de sintaxe mais frequentemente utilizada é a norma EDIFACT /ONU, constituída por directórios das Nações Unidas para a Troca de dados informatizada para a Administração, o comércio e o transporte. A utilização da linguagem XML (Linguagem de Marcação Expansível) progrediu com o desenvolvimento das tecnologias da Internet. Existem normas regionais bem como normas específicas de um sector de actividade, tais como «ANSI X.12» e «CargoIMP». As sintaxes de mensagens proprietárias não padronizadas são também comummente usadas. As sintaxes proprietárias são consideradas como onerosas porquanto a sua compreensão e utilização impõem aos profissionais a alocação de recursos novos.

Já há algum tempo que as Alfândegas efectuam nas fronteiras, controles durante os quais exigem e utilizam elementos de facto sobre o transporte, a manutenção da carga, a localização das cadeias logísticas, as mercadorias, o acondicionamento, a inspecção, a avaliação, os direitos e demais imposições, etc. Apesar das evoluções tecnológicas notáveis e das inovações que conheceram os regimes aduaneiros e os procedimentos operacionais, as Alfândegas continuam mais ou menos a processar as mesmas informações operacionais de base. Esses fragmentos de informação foram incorporados metodicamente no Modelo de Dados da OMA.

O Modelo de Dados da OMA consiste em um conjunto de exigências de dados cuidadosamente combinados que se reforçam mutuamente e serão actualizados de maneira regular para responder às necessidades no plano jurídico e dos procedimentos das instituições nas fronteiras responsáveis pela regulamentação dos fluxos transfronteiriços tais como as Alfândegas, para o controle das transacções, da exportação, importação e trânsito. Este instrumento é elaborado e mantido actualizado pela Equipa de projecto encarregada do Modelo de dados e a sua promoção e garantida por intermédio de parcerias com Membros da OMA, organizações internacionais e o sector privado.

O Modelo de Dados da OMA assume a forma de uma biblioteca contendo duas partes principais : a primeira parte reveste a forma de uma compilação de componentes padronizadas e a segunda parte agrupa os Processos de informação. Os Processos de informação são

construídos a partir de componentes do modelo de dados e representam a utilização dos dados nos procedimentos operacionais. Fornecem modelos electrónicos para a troca de informações. Podem igualmente servir para ilustrar funções operacionais. O Apêndice 1 intitulado « Estruturas da informação e das telecomunicações para o comércio electrónico » oferece uma descrição detalhada dos Processos de informação.

9.2. Troca de informação com outras instituições governamentais

(Norma 7.4)

Muitas informações são trocadas entre as Alfândegas e outros Órgãos reguladores dos fluxos transfronteiriços, por exemplo, as estatísticas comerciais e as informações relativas às quotas, as restrições, aos acordos preferenciais, etc. Quando não for possível agrupar as Administrações, os prazos necessários para trocar as informações podem ser reduzidos instalando um interface informático entre os serviços interessados.

Quando as empresas podem apresentar por via electrónica as licenças de importação/exportação, os certificados sanitários/fitossanitários, etc. emitidos por outras instituições, o interface informático permite confirmar instantaneamente às Alfândegas a validade dos documentos.

Por outro lado, podemos contribuir para a celeridade do desalfandegamento de todas as mercadorias estabelecendo um procedimento que permita às empresas comunicar de uma só vez a uma «Janela Única», todas as informações regulamentares exigidas. No entanto, para garantir o bom funcionamento de tal procedimento, as empresas devem obter as informações referentes às exigências regulamentares, e isto por via electrónica. Quando decidem conceber os seus sistemas informáticos, as Alfândegas devem ter em consideração não só os interfaces com os operadores comerciais mas igualmente com as outras Administrações.

A este respeito, as normas internacionais em matéria de trocas de informações facilitam muito a concepção de interfaces Alfândegas/parceiros comerciais e Alfândegas/instituições públicas. A utilização por todos os operadores comerciais de normas idênticas permitirá reduzir consideravelmente os custos atinentes às trocas electrónicas de dados.

Empenhada em contribuir para o reforço das capacidades, a OMA elaborou um Livro intitulado «Como construir um ambiente de Janela Única». Este Livro contém dois volumes. O Volume 1, intitulado «Guia executivo», trata dos aspectos da Janela Única que dizem respeito aos Gestores. O Volume 2, chamado “O Guia prático” é um Livro de ferramentas e de técnicas destinadas a apoiar os peritos que trabalham em projectos de criação de uma Janela Única.

9.3. Intercâmbio de informações com outras administrações aduaneiras

(Norma 7.4)

As Tecnologias da Informação e da Comunicação oferecem a uma Administração Aduaneira a capacidade de trocar dados com outras Administrações Aduaneiras.

A iniciativa da OMA sobre as Alfândegas em rede internacional (DRI), visa proceder a uma análise exaustiva das possibilidades de racionalizar, harmonizar e padronizar a troca segura e eficaz de informações entre as Administrações Aduaneiras. A análise permitiu concluir que a maneira mais eficaz de tirar proveito das vantagens óptimas da cooperação Alfândegas-Alfândegas seria racionalizando os processos de trocas de informações, e isso poderia igualmente beneficiar outras partes interessadas.

Trata-se de um método padronizado, que utiliza modelos e planos genéricos, facilita e melhora esses processos acelerando a redacção e a implementação dos acordos de troca de informações. A elaboração de um catálogo de alternativas documentadas de maneira padronizada, que podem ser reproduzidas com pouco esforço, permite além disso acelerar a extensão, o desenvolvimento e o acesso às redes aduaneiras.

A nível bilateral, multilateral e plurilateral, as Administrações Aduaneiras continuam a empenhar-se em alternativas e acordos que permitam partilhar informações da maneira mais eficaz possível. A troca de informações efectua-se segundo dois eixos: um diz respeito às informações ligadas à luta contra a fraude e o outro tem a ver com as informações relativas aos fluxos comerciais de mercadorias.

Já existe uma Rede aduaneira de luta contra a fraude, que contribui para uma difusão rápida de informações sensíveis, não nominativas, no domínio da luta contra a fraude. Registam-se muitos exemplos de trocas de informações entre as Administrações Aduaneiras, em vigor aos níveis bilateral e regional. A iniciativa das Alfândegas em rede internacional apoia-se no conceito de «Bloco utilitário» para descrever a troca de informações entre as Alfândegas.

Um bloco utilitário é uma parte específica do processo operacional das Alfândegas, explicada em termos mais simples mas completos, compreensíveis para todos. Um bloco utilitário descreve os objectivos estratégicos para os decisores, os processos operacionais para os gestores, as questões jurídicas para os juristas, os métodos funcionais para os funcionários encarregados das operações e as especificações técnicas para o pessoal encarregado da TI. É construído e examinado por peritos graças a um modelo de concepção padronizado. Centra-se nas necessidades de uma parte específica do processo operacional das Alfândegas, inclusive os elementos de dados pertinentes, por exemplo operadores económicos autorizados (OEA), fraude comercial, trânsito, etc.

A decomposição dos processos operacionais das Alfândegas em blocos utilitários individuais permite às autoridades aduaneiras serem selectivas quanto aos processos operacionais e às informações conexas que elas escolhem partilhar com os seus parceiros, e concluir mais rapidamente essas alternativas de ligação em rede.

A partilha de informações prévias, o reconhecimento mútuo dos Operadores Económicos Autorizados (OEA), o reconhecimento mútuo dos controles, a coordenação dos controles do trânsito e a partilha transfronteiriça de uma declaração de exportação de mercadorias de um país com vista à sua utilização no país importador são alguns dos exemplos de «Blocos utilitários» em curso de elaboração.

O uso para fins aduaneiros do Número de Referência Único (UCR ou *Unique Consignment Reference*) da OMA poderia ajudar muito a troca de informações a nível internacional (ver apêndice 9). Conforme indica o seu nome, este número de referência seria utilizado durante toda a duração da transacção e constituiria um meio de identificação único da transacção para todos os intervenientes. As Alfândegas deveriam considerar a possibilidade de prever este campo/um campo para este efeito, quando desenvolvem as suas bases de dados de transacções.

As trocas de informações a nível internacional podem suscitar questões legais e de procedimentos que deverão ser examinadas. As Administrações que se empenham nesta via deveriam, desde o lançamento do projecto, recorrer a juristas nacionais para assegurar-se que as modificações eventualmente necessárias no plano legislativo sejam efectuadas em tempo oportuno.

10. Comunicações

(Norma 7.2)

As administrações aduaneiras envolvidas no processo de introdução de um sistema de intercâmbio electrónico de informação devem reconhecer que o êxito dependerá da sua disponibilidade e acessibilidade. Isto só pode ser garantido mediante o uso de padrões internacionais devidamente reconhecidos a todos os níveis apropriados de desenvolvimento do sistema. Existem quatro áreas de interesse relacionadas com os padrões internacionais.

10.1. Soluções em matéria de transferência de dados

Existem três possibilidades no domínio de transferência de dados:

- Entrega física em suporte magnético tais como cassetes e discos através dos serviços postais/correios;
- Transferência de dados de ponto-a-ponto; e
- Redes de comunicação, as quais oferecem condições de armazenamento, envio e outros serviços de valor acrescentado.

Cassete/disco

Este método é lento uma vez que exige que os suportes sejam fisicamente trocados por via postal, ou mediante a entrega directa pelo operador comercial nas Alfândegas. A troca de informação nesses suportes pode ser vista como o primeiro passo para a implementação do Comércio Electrónico (EC). Os padrões de mensagens internacionais, conforme descrito no Modelo de Dados da OMA, podem também ser utilizados. A implementação destes sistemas pode oferecer às Alfândegas e aos operadores comerciais experiência prática valiosa em matéria de comércio electrónico.

Ponto-a-ponto

São usados *modems* para conectar dois computadores a linhas telefónicas ou ligações via satélite para que possam comunicar. As linhas telefónicas tradicionais são destinadas à comunicação por voz, e não às comunicações por computadores. Consequentemente, para a troca da informação são necessários *modems* e *softwares* de telecomunicações.

Se forem usadas linhas telefónicas especializadas em vez de linhas telefónicas genéricas, os computadores de envio e recepção podem usar controladores de comunicação em vez de um *modem*. A principal diferença entre ter uma linha telefónica genérica e uma linha especializada consiste na velocidade. A linha geral possui uma capacidade de transferência muito mais lenta, o que a torna adequada para a transmissão de uma pequena quantidade de dados.

Redes de comunicação

O cenário típico para uma rede de comunicação é que todos operadores comerciais que pretendam trocar informação possuam uma caixa de correio, gerida pela rede de comunicação. As mensagens electrónicas são transmitidas pela rede de comunicação de uma caixa de correio para outra. Isto significa que, ao contrário do ponto-a-ponto, onde ambos os sistemas devem estar disponíveis e abertos a receber dados ao mesmo tempo, a transmissão e armazenagem temporária da informação é separada do sistema de aplicação. Se por qualquer razão o sistema aduaneiro não estiver operacional, os operadores comerciais podem continuar a enviar as mensagens pela caixa de correio das Alfândegas.

Uma Rede de Valor Adicionada (VAN) é uma rede de comunicação de terceiros que pode aceitar uma mensagem proveniente de qualquer configuração de *hardware* e *software* e enviar a mensagem a um receptor que utilize *hardware* e *software* diferentes. Uma VAN pode providenciar não apenas serviços de comunicação mas também serviços de segurança e tradução de EDI. A maioria das VAN pode suportar uma vasta gama de protocolos de comunicações. Uma vez que a tecnologia de comunicações e a conversão de protocolo podem tornar-se extremamente complexas, uma VAN oferece um serviço real de valor acrescentado mediante o manuseamento deste aspecto das comunicações entre dois operadores comerciais, ou nos grupos de operadores comerciais, com configurações informáticas diferentes.

As Alfândegas precisarão de analisar as formas mais eficazes para a recepção de informação. Muitos países não possuem serviços de VAN, mas possuem serviços de *Internet*. Estes, tendem a ser mais baratos do que as VAN mas por enquanto existem implicações de segurança e preocupações de níveis de serviços a serem consideradas. As administrações estão já a considerar a *Internet* e a WWW (Rede Internacional de Comunicação) como um meio de disponibilizar aos operadores comerciais a informação essencial relativa aos requisitos exigidos.

10.2. Telecomunicações

Ao nível das telecomunicações, as Alfândegas devem assegurar que os protocolos utilizados para a conexão física sejam reconhecidos, tal como a Organização de Padrões Internacionais (ISO) X21, X25, X400, etc. Também existem padrões para os protocolos de *Internet* tais como o TCP/IP e o Protocolo de Transferência de Hipertexto (*http*). As companhias nacionais de telecomunicações, as VAN e os provedores de serviços de *Internet* geralmente aplicam estes padrões. Contudo, se as administrações estiverem a empregar provedores privados de rede de telecomunicações, devem certificar que os padrões ISO sejam utilizados.

10.3. Troca de Mensagens

(Normas 3.11 e 7.2)

As Alfândegas puderam efectivamente exercer uma influência mais directa sobre a concepção das normas informáticas. Estes últimos anos, elas participaram no desenvolvimento de mensagens padronizadas sob a égide das Nações Unidas. Essas mensagens EDIFACT/ONU constituem doravante uma norma internacional em matéria de EDI. A OMA elaborou o Modelo de Dados da OMA, que permitiu optimizar a troca de dados por via electrónica. Este Modelo constitui uma linguagem universal para a troca de dados transfronteiriços e representa uma norma mundial de dados exigidos na passagem das fronteiras para o desalfandegamento e a libertação das mercadorias, dos contentores, dos meios de transporte e das pessoas;

As mensagens EDIFACT/ONU e outras mensagens EDI podem ser transmitidas por Internet como anexos a um correio electrónico normal por intermédio do Protocolo SMTP. Essas mensagens electrónicas podem ser tornadas mais seguras por uma assinatura numérica utilizando o Protocolo S/MIME.

O desenvolvimento e a generalização rápida da Internet oferecem às trocas de informações novas perspectivas. Em consequência, novos formatos de trocas de informações passarão de facto a ser normas internacionais porque são utilizados a nível mundial; por exemplo os formulários electrónicos, a linguagem hipertexto HTML, a Linguagem de Marcação Extensível-XML ("*eXtensible Markup Language* - XML"), um repertório mundial, a arquitectura de documentos aberta (ODA), etc. Muitos desses formatos estão sempre em curso de desenvolvimento mas as Administrações Aduaneiras que se interessam pelas trocas de dados informatizados futuros deverão tê-los em conta quando definirem a sua estratégia na matéria.

A Internet oferece às pequenas e médias empresas a possibilidade de conhecer a situação das suas mercadorias e/ou a das suas declarações de mercadorias nas Alfândegas e permitirá no futuro efectuar pagamentos electrónicos e arquivar documentos electrónicos.

A troca de dados electrónicos (EDI) consiste em um conjunto de protocolos de troca de dados por via electrónica que permite assegurar trocas estruturadas entre as organizações. As normas de origem estabelecem o método de condicionamento em um envelope MIME dos jogos de transacções EDIFACT/ONU. No entanto, com o crescimento da Internet e a demanda de serviços neutros e interoperáveis, novas normas chamadas EDIINT (EDI – Internet Integration) foram elaboradas e versam sobre questões de segurança tais como a confidencialidade, a autenticidade, a integridade e a não-repudiação das mensagens. A «*Internet Engineering Task Force*» gerou a evolução dessas normas, que apareceram inicialmente, sob a forma de Pedidos de observações (Request for Comment ou RFC) contendo «Declarações de Aplicabilidade».

AS1 – Declaração de aplicabilidade descrevendo como as mensagens EDI são transmitidas com as normas Internet MIME e SMTP. A transmissão das mensagens EDI é protegida por intermédio de assinaturas numéricas e da codificação/cifragem das informações trocadas. O protocolo AS1 permite trocas seguras na Internet.

AS2 – Declaração de aplicabilidade descrevendo como as mensagens EDI podem ser transmitidas em tempo real através de uma troca de informações com base no protocolo http e na norma MIME. Este método baseia-se na assinatura numérica dos dados trocados, mas a sessão como os ficheiros dos dados trocados estão codificados. O protocolo AS2 assegura uma troca protegida em tempo real entre aplicativos baseados na «Web».

AS3 – Declaração de aplicabilidade descrevendo como os dados EDI ou XML podem ser transmitidos na Internet de maneira protegida graças a um protocolo FTP. A transferência protegida obtém-se graças à encriptação bem como à codificação dos ficheiros de dados trocados.

Recentemente, uma nova norma AS4 surgiu e assenta em serviços Web que fornecem a técnica central de transporte das mensagens, garantindo que os imperativos de segurança exigidos para o transporte de mensagens pela Internet sejam respeitados ao mesmo título que com os protocolos AS2 e AS3.

Anexo A à Secção 10.3. Mensagem

Generalidades

Na Versão 1.1 do Modelo de Dados Aduaneiros (CDM) dá-se atenção na forma de preenchimento das mensagens de EDIFACT correspondentes às declarações de mercadorias e de carga. A partir da versão 2.0 do CDM, deve-se focalizar sobre o significado semântico de alto nível dos dados e como interagir com as outras administrações do Estado, bem como as indústrias. Este anexo à secção 10.3 introduz os três níveis de abstracção sobre um modelo de dados e o porque é que a atenção deve estar direccionada sobre o nível mais alto de abstracção. Os artefactos incluídos no CDM e que correspondem a cada nível de abstracção são referenciados, sempre que possível.

Modelo Externo, Modelo Físico, Modelo Conceptual

Os modelos menos abstractos, chamados Modelos Externos, descrevem implementações específicas de uma Declaração de Mercadorias e de um Manifesto. Os exemplos típicos são a mensagem CUSCAR conforme à Versão 1.1 do CDM, e uma mensagem de WCOCAR conforme à Versão 2.0 do CDM.

Os Modelos Físicos são mais genéricos porque descrevem um conjunto ou uma categoria de exemplos, mas captam ainda a tecnologia em que os exemplos foram implementados. Um exemplo típico é o Guia de Implementação de Mensagens (GIM) para a implementação de uma mensagem CUSCAR, o qual está incluído na Versão 1.1 do Manual do Modelo de Dados Aduaneiros da OMA publicado em Novembro de 2003.

Os Modelos Conceptuais retiram a tecnologia de implementação para enfatizar os conceitos e significados que definem algumas classes de casos documentais. Este nível mais alto de abstracção foi recentemente introduzido na Versão 2.0 do CDM. Os exemplos típicos são os Diagramas de Classe UML para todos os tipos de documentos, os Diagramas de Classe UML para um tipo de documento único, e o inventário de todos os 250 dados colectivamente conhecidos como o Conjunto de Dados do CDM.

Necessidade do Modelo Conceptual

A actividade das Alfândegas tal como a maioria das áreas de actividade, não muda tão rápido quanto a tecnologia. Se o CDM for apenas descrito em qualquer tecnologia específica (por exemplo; através de um Modelo Físico de Dados tal com o EDIFACT), será necessário definir o CDM em todas as tecnologias emergentes. Ainda assim, será muito difícil, se não impossível, garantir que os Modelos Físicos de Dados em tecnologias diferentes sejam equivalentes.

Mediante o estabelecimento de um Modelo Conceptual e captação de todas as regras institucionais no Modelo Conceptual, o comércio estará em condições de implementar os documentos aduaneiros em qualquer que seja a tecnologia utilizada (isto é; Modelo Físico de Dados) que satisfaçam as suas necessidades.

Outros benefícios do estabelecimento de um Modelo Conceptual

Torna-se mais claro porque o significado e as regras de apresentação dos dados são preservados em Modelos Físicos diferentes, os quais são derivados do mesmo Modelo Conceptual. Por exemplo; a classe “Equipamento de Transporte” designa os recursos materiais necessários para acondicionar as remessas para transporte” e inclui os mesmos atributos da classe, quer seja usada nas Declarações de Importação, Exportação, de carga à saída, de carga à entrada, de Transporte ou de Trânsito.

A interoperabilidade dos modelos de dados de outras administrações ou das administrações do Estado participantes e das empresas é facilitada quando cada elemento de informações é dotado de um significado único no conjunto de documentos aduaneiros. Por exemplo, o termo de transporte UN/CEFACT TBG3 “Equipamento de transporte” pode ser directamente inserido na classe da versão 2.0 do CDM “Equipamento de transporte”.

10.4 Códigos

(Normas 3.11 e 7.2)

A OMA recomenda o uso de códigos internacionais, tais como os códigos ISO de países e moedas, os códigos de transporte das Nações Unidas, o Sistema Harmonizado de Designação e de Codificação de Mercadorias da OMA, etc. (Ver Apêndice 9). O uso dos códigos internacionais disponíveis garante a abrangência e o acesso dos sistemas aduaneiros. O uso harmonizado de códigos ao nível das aplicações contribuirá de modo significativo para facilitar o comércio internacional. Ajudará a simplificar o desenvolvimento de sistemas para os operadores comerciais e das outras administrações que pretendam comunicar com as Alfândegas. Tornará também mais vantajosa a troca de informação entre as Alfândegas.

11. Segurança das TIC

As actividades realizadas pelo governo e a as empresas evoluíram consideravelmente no decurso dos últimos 10 anos. O uso da *Internet* e o acesso generalizado às TIC de baixo custo permitem aos sistemas comunicar com um vasto leque de pessoas com um conhecimento crescente sobre como aplicar e manipular as TIC.

Estas mudanças trouxeram muitos benefícios em termos de rapidez e acesso, mas aumentaram também a consciência dos riscos de segurança a que estão expostas as nossas comunicações, os nossos sistemas e as bases de dados.

O desenvolvimento da fraude informática e os riscos de sabotagem e de avaria acidental dos sistemas são alguns dos desafios que as Alfândegas que empreguem as TIC devem enfrentar na gestão das suas actividades e procedimentos associados. A corrupção ou a violação dos sistemas das TIC das Alfândegas pode causar sérios problemas ao comércio e à arrecadação de receitas. Em circunstâncias mais extremas podem comprometer a segurança nacional.

É particularmente importante que as Alfândegas identifiquem os riscos e desenvolvam uma abordagem integrada que trate não apenas das vulnerabilidades físicas e técnicas mas também da questão da governação, isto é; procedimentos e acordos institucionais com as empresas, para garantir um padrão elevado de segurança das TIC.

Os peritos advogam uma abordagem de gestão de riscos para gerir os riscos atinentes à segurança informática. As alfândegas deveriam dispor das informações e das ferramentas que contribuem para gerir e identificar eficazmente os riscos ligados aos seus activos das tecnologias de informação e da comunicação (TIC). A avaliação dos riscos consiste na definição das ameaças que pesam sobre esses activos bem como as suas falhas mas também na estimativa da probabilidade e das consequências de uma violação das regras de segurança. A fim de garantir uma boa gestão da segurança da informação, as competências em matéria de avaliação dos riscos são essenciais. Os riscos que pesam sobre os activos das TI são os incêndios, as inundações, as perdas de acesso, os ataques do ciberespaço, as violações de acesso, as perdas de dados, etc. Uma abordagem de gestão de riscos ajuda a definir esses riscos e prepara a organização a reduzi-los e a responder de maneira apropriada.

A Norma ISO 27001 versa sobre o Sistema de gestão da segurança da informação, cujas exigências ela fixa. Esta Norma prevê a realização de uma avaliação específica dos riscos antes de seleccionar e de aplicar uma medida de controle. Uma iniciativa que tem por base a gestão dos riscos está descrita na Norma ISO/IEC 27005:2011, Tecnologias da Informação – Técnicas de segurança – Gestão dos riscos ligados à segurança da informação. Cada controle deve ser justificado por uma avaliação dos riscos. Quando ela incide sobre cada activo das TIC em causa, a avaliação dos riscos permite orçamentar contra-medidas proporcionais às perdas ou aos danos que poderiam resultar de uma violação das regras de segurança atinentes a esses activos. Este princípio de gestão da segurança das TIC deve ser incorporado na política de segurança evocada na secção 11.2 abaixo.

A gravidade dos riscos ligados à segurança dos activos das TIC requer toda a atenção dos gestores das Alfândegas na medida em que esses riscos dizem respeito a dados importantes que beneficiam de uma protecção jurídica, a informações sobre transacções que tenham consequências financeiras e a ameaças para a saúde e a segurança pública de um país. As Alfândegas não se podem dar ao luxo de perder esses dados ou de os ver expostos. Dadas as consequências de uma violação ou de uma perda das informações (por exemplo, a perda da confiança do público), a gestão estratégica dos riscos ligados à segurança da informação deve ser confiada à direcção executiva.

11.1. Segurança das TIC – Definição e objectivo

A norma ISO 27000:2012 (tecnologia de informação – código de prática para a gestão de segurança da informação) - define a segurança da informação como segue:

"… preservação da confidencialidade, integridade e disponibilidade de informação"

a **confidencialidade** consiste em " garantir o acesso à informação apenas às pessoas autorizadas"; a **integridade** em "salvaguardar a exactidão e a plenitude da informação e dos métodos de processamento"; e a **disponibilidade** em garantir que apenas "os utilizadores autorizados tenham acesso à informação e aos elementos associados".

11.2. Política de segurança das TIC

Uma forma para alcançar este objectivo é publicar uma política de segurança das TIC no sentido de assegurar-se de que todos os funcionários estejam ao corrente das questões que se colocam e das suas responsabilidades pessoais nesta matéria.

A referida política deve demonstrar uma abordagem e o compromisso da gestão superior para com a segurança das TIC e definir o que é que a administração espera do seu pessoal. Os papéis, as responsabilidades e as obrigações dos utilizadores devem também ser definidos de uma maneira geral.

Embora seja possível simplesmente informar os utilizadores sobre as políticas das TIC pode ser mais apropriado desenvolver acordos com os utilizadores que definam claramente as suas obrigações e responsabilidades.

Contudo, a política de segurança das TIC não irá por si só oferecer "confiança, integridade e disponibilidade". Em qualquer instalação das TIC, será necessário desenvolver um conjunto complexo de procedimentos, soluções técnicas, requisitos legais e políticas, processos de gestão e considerações práticas para sustentar a política geral da administração em matéria de segurança das TIC.

11.3. Segurança das TIC - Considerações

A segurança das TIC abrange os seguintes aspectos das actividades de uma Alfândega:

- organização da segurança da informação;
- segurança dos recursos humanos;
- gestão do património;
- controle do acesso;
- criptografia;
- segurança física e ambiental;
- segurança das operações;
- segurança das comunicações e das operações
- aquisição, desenvolvimento e manutenção de sistemas;
- relações com os fornecedores;

- gestão de incidentes de segurança da informação;
- aspectos de segurança da informação da gestão de continuidade de negócios (BCM)
- compliance / conformidade

Estes aspectos são detalhadamente abordados na norma ISO 27002:2013 e recomenda-se que as Alfândegas sigam cuidadosamente as considerações e explicações contidas no referido padrão.

Os títulos seguintes, retirados da norma ISO 27002:2013, contribuem para identificar as áreas abrangentes que devem ser consideradas em qualquer quadro de segurança das TIC.

Organização da segurança da informação

Trata-se do quadro de gestão para implementar e controlar os dispositivos de segurança no seio da administração. Deveria abranger os papéis, responsabilidades e a separação de tarefas.

Envolve o estabelecimento de uma infra-estrutura interna de gestão para atribuir e manter as responsabilidades e as funções em matéria de segurança, e a possibilidade de exercer certos controles no contacto com autoridades, no contacto com grupos de especial interesse e na segurança da informação na gestão de projectos. Abrange também os prestadores de serviços, por exemplo; a prestação por terceiros de serviços das TIC.

A utilização de dispositivos portáteis e o recurso ao teletrabalho devem figurar nesta parte.

Segurança dos recursos humanos

As autorizações de segurança e a formação do pessoal são importantes para assegurar um nível apropriado de confiança e de boa prática. Além disso, os acordos de confidencialidade, os termos e as condições específicas de emprego podem ser tidos em conta, dependendo da natureza da informação e do acesso que os funcionários têm ao sistema.

O cumprimento das obrigações de segurança deve ser avaliado no quadro dos procedimentos permitindo controlar e assinalar as violações de segurança.

Isto inclui controles específicos para a identificação, os termos e condições de emprego, durante o emprego, a gestão de responsabilidades e a consciencialização, educação e formação.

Gestão do património

Para proteger o seu património informático, nomeadamente os bancos de informação, as Alfândegas devem dispor, de um lado, de um meio para contabilizar o seu património e informações e do outro, de um meio para os classificar com vista a estabelecer níveis apropriados de protecção

O património pode incluir tanto as infra-estruturas físicas/materiais como as bases de dados, ficheiros e aplicativos *software* que podem fazer parte do património material. Convém determinar o proprietário, o uso aceitável e a restituição de cada património. Um inventário do património deve ser estabelecido.

As informações devem ser classificadas não apenas em termos de seu tratamento de segurança mas igualmente no que toca ao nível de segurança a prever. Este nível determina a protecção de que deve beneficiar a informação (por exemplo, quem e em que circunstâncias pode consultá-la) e pode até determinar a natureza do património material (material, instalações, etc.) onde ela pode ser armazenada ou através dos quais pode ser transmitida. A informação deve ser etiquetada.

Os suportes que contêm informações devem ser geridos de maneira apropriada. Convém descrever a gestão, a cessão e a transferência material/física dos suportes amovíveis.

Controle de acesso

O controle de acesso à informação é a chave para o estabelecimento de sistemas seguros e confiáveis para os utilizadores.

O acesso deve basear-se em requisitos fixados pela administração para assegurar que apenas os devidamente autorizados possam consultar ou transmitir determinada informação. Estes requisitos são geralmente documentados como parte de uma "política de controle de acesso" que estabelece os termos e os critérios para a determinação do acesso aos sistemas e à informação.

Para além da forma como os controles de acesso devem ser administrados, os respectivos serviços deverão determinar:

- quem é responsável pela autorização do acesso;
- as regras que regem a concessão do acesso;
- os níveis e tipos de acesso que devem ser disponibilizados, e
- os privilégios associados aos vários níveis e tipos de acesso.

Regras de gestão de acesso podem igualmente ser necessárias para decidir questões como, por exemplo, o tempo que pode passar antes do encerramento automático de uma sessão inactiva, as pré-condições de acesso a certas áreas do sistema, bem como as mudanças das autorizações, as quais podem ser automáticas ou sujeitas à decisão da gestão superior.

Os controles de acesso à rede e a monitorização do acesso são também importantes porque as conexões à rede podem representar um risco significativo para a segurança. Os aspectos importantes para o acesso à rede incluem os meios pelos quais:

- os utilizadores são autenticados;
- os terminais e outros pontos de entrada são identificados e consignados, e
- a trajectória dos utilizadores é controlada.

As questões da autenticação dos utilizadores e as mais frequentemente constatadas na matéria são tratadas em detalhe na parte 10.4 – Autenticação.

As responsabilidades do utilizador e o controle do acesso ao sistema e à aplicação deveriam igualmente figurar nesta secção.

Criptografia

A criptografia deve ser utilizada de maneira apropriada e eficaz para proteger a confidencialidade, a autenticidade, a integridade e a não-rejeição da informação.

O uso da criptografia e a gestão das chaves criptográficas deveriam estar descritos em uma política.

Segurança física e ambiental

Ao desenvolver uma política de segurança física e das TIC, é essencial prever potenciais riscos físicos aos quais possam estar expostos os edifícios, o equipamento ou o ambiente de trabalho das TIC.

As contra-medidas podem variar desde o estabelecimento de um perímetro de segurança aos pontos de controle de segurança, políticas de secretárias e ecrãs limpos, fonte alternativa de fornecimento de corrente eléctrica, cabos seguros, procedimentos e medidas de segurança para o equipamento instalado no exterior. A selecção e o uso de qualquer contra-medida dependem dos riscos específicos, dos diferentes equipamentos instalados e do ambiente físico.

Segurança das operações

Para garantir que as instalações de processamento das Alfândegas estejam correctamente protegidas, é essencial estabelecer procedimentos apropriados.

Este aspecto abrange diversas questões, nomeadamente:

- documentação e aplicação de procedimentos operacionais
- gestão da mudança
- medidas procedimentais necessárias para separar diferentes ambientes de TIC tais como ambientes de teste e produção
- separação das obrigações
- planificação a longo prazo de capacitação, aceitação de sistemas novos ou actualizações
- protecção contra *softwares* hostis
- contrôle e gestão da rede
- gestão dos suportes, incluindo armazenamento dos suportes segurança da documentação do sistema
- proteção de informações ou software durante a transmissão.

Segurança das comunicações

- controles e gestão de redes,
- segregação de redes
- transferência de informações e acordos sobre as transferências de informações
- mensagens electrónicas

Os detalhes adicionais relativos à troca de informação e de *software* constam na parte 11.4 – Autenticação, a qual abrange muitos dos factores que os serviços precisam de analisar no sentido de assegurar a integridade da informação e estabelecer a identidade dos comunicadores.

11.3.1. Aquisição, desenvolvimento e manutenção dos sistemas

A segurança deve fazer parte integrante da concepção dos sistemas e compreender. a infra-estrutura, as aplicações e os procedimentos de apoio.

Quando se efectua a mudança, selecção ou aceitação do *software*, convém tomar precauções a fim de evitar canais dissimulados (uma "porta de acesso oculta" que permitiria o acesso não autorizado) e cavalos de Tróia. O controle de acesso para as mudanças de códigos, o uso de fornecedores confiáveis, a inspecção de código e o teste de produto são apenas algumas das possíveis estratégias. Convém proteger de maneira apropriada os dados destinados a testes.

Relação com os fornecedores

As relações com os fornecedores devem ter em conta os aspectos seguintes:

- ❖ política de segurança ligada às relações com os fornecedores;
- ❖ questão da segurança prevista nos acordos;
- ❖ cadeia logística da tecnologia;
- ❖ controle e exame dos serviços dos fornecedores;
- ❖ gestão das mudanças nos serviços dos fornecedores.

Gestão dos incidentes das actividades ligadas à segurança da informação

É indispensável gerir os incidentes ligados à segurança. Convém descrever as responsabilidades e os procedimentos. Os eventos e as fraquezas devem ser notificados o mais rapidamente possível aos gestores superiores. Quando surgir um incidente ligado à informação, convém avalia-lo, responder e recolher as evidências.

As lições tiradas de cada evento devem reduzir a probabilidade ou incidência dos eventos futuros.

Aspectos da gestão da continuidade das actividades ligados à segurança da informação

As consequências de uma falha, quer por lapso de segurança, quer por desastre, devem ser consideradas antes que um plano de continuidade das actividades seja desenvolvido e testado.

Tal como acontece com qualquer aspecto da planificação de segurança, as medidas de continuidade das actividades adoptadas dependerão dos riscos identificados, da probabilidade destes riscos se materializarem e das consequências para as actividades da administração. Para muitas Alfândegas, uma falha na prestação dos serviços poderia não apenas perturbar o comércio, mas prejudicaria a segurança nacional através do enfraquecimento da selectividade, do escrutínio, da criação de perfis e das instalações de comunicação.

Para garantir a disponibilidade das instalações de tratamento da informação, as mesmas devem ser implementadas com redundância suficiente.

Cumprimento da lei

Devem ser consideradas as medidas que permitam assegurar que a administração cumpra com quaisquer exigências legais ou contratuais a que possa estar sujeita, bem como o cumprimento das suas normas e princípios de segurança interna.

As considerações relevantes incluem os direitos de autor, protecção dos arquivos administrativos, gestão dos arquivos admissíveis como elementos de prova e monitoramento dos relatórios de auditoria (ou de mais informação requerida).

11.4. Autenticação

11.4.1. Porque é que a autenticação é necessária?

Num ambiente baseado em papel, há muito que foram aceites os procedimentos e convenções que dizem respeito à autenticação de identidade e de documentos. Por exemplo; as assinaturas escritas, as assinaturas de testemunhas e os selos são métodos usados para autenticar a identidade., O desenvolvimento de métodos legais e forenses que visam "provar" a autenticidade da identidade de uma entidade e a ligação com as suas transacções levou muito tempo e, embora não infalíveis, estes meios foram devidamente testados no quadro dos sistemas judiciários de diferentes países.

Nem sempre é possível transferir estes métodos para um ambiente electrónico e os novos métodos de autenticação precisam ainda de ser avaliados e adoptados.

O desafio da autenticação é ainda mais importante no ambiente electrónico por causa:

- da amplitude de acesso providenciado pelas TIC;
- do volume crescente das transacções; e
- da "distância" do utilizador (quer geograficamente, quer em termos de relações) que a transacção electrónica encoraja.

Isto é particularmente significativo para as Alfândegas nas suas funções de cumprimento de aplicação da lei e de luta contra a fraude. Qualquer falha em ligar um indivíduo firmemente à sua identidade electrónica, documentos ou declarações, prejudicaria a importância das provas nos processos legais. Poderia também expor os sistemas aduaneiros ao risco de fraude ou utilização abusiva da identidade, pondo em causa, deste modo a confiança dos utilizadores nos sistemas e a reputação de uma administração.

11.4.2. As alternativas electrónicas

Existe um vasto leque de opções disponíveis para fins de autenticação. Estas opções variam consideravelmente com respeito ao grau de garantia da identidade oferecida e ao grau de fiabilidade com o qual uma parte pode estar ligada à sua mensagem.

Os métodos de autenticação variam de um simples sistema de palavra-chave aos sistemas complexos providenciados pela criptografia de chave pública. Cada método ou tecnologia tem os seus pontos fortes e fracos. Os vários métodos disponíveis estão sucintamente descritos a seguir.

Palavra-chave, PIN e Identificações de Utilizadores

Actualmente, o método mais comum de autenticação para sistemas informáticos é a palavra-chave. Estima-se que em 2002 mais de 90% dos sistemas de TI utilizavam ainda as palavra-chave ou números de identificação pessoal (PIN) como principal meio de autenticação. Uma percentagem aproximadamente similar de sítios de comércio electrónico usa palavra-chave como o principal meio de autenticação dos utilizadores.

O princípio da palavra-chave é ela ser conhecida apenas pelo seu detentor e pelo administrador, sendo o acesso apenas permitido nos casos em que a palavra-chave do utilizador corresponde aos arquivos do administrador. Tal como em muitos sistemas de autenticação, ela obriga o utilizador a preservar a segurança da sua identidade *on-line* – sua palavra-chave.

Numa perspectiva técnica, o modelo de palavra-chave é susceptível de ataques por "força bruta" por exemplo, por "dicionário". Estes ataques consistem geralmente em tentativas informáticas repetidas que visam obter um acesso não autorizado por experimentação e erro. Por esta razão, os sistemas de palavra-chave baseiam-se na segurança dos canais através dos quais a palavra-chave é comunicada e das práticas de segurança e disposições tomadas em matéria de segurança pelo administrador.

Normalmente, a palavra-chave autentica a identidade do utilizador. Não permite autenticar os documentos comunicados nem verificar a integridade do conteúdo da mensagem.

Os sistemas de palavra-chave apresentam certamente a vantagem de implementação a baixo custo, mas adaptam-se melhor a uma utilização única ou em casos em que os dados ou o sistema a ser protegido possuam um baixo nível de segurança.

Os sistemas de palavra-chave podem-se tornar mais seguros através da sua combinação com outros métodos de segurança e autenticação tais como a codificação, Identificações de Utilizadores ou confrontação e resposta.

As boas práticas de gestão de palavra-chave são essenciais. As decisões de políticas de gestão determinarão a eficácia de qualquer sistema de palavra-chave e o grau de apoio necessário para manter os utilizadores. Estas decisões podem incluir simples políticas de segurança em questões como:

- a extensão, composição e o tempo de vida da palavra-chave;
- o número de tentativas falhadas de início de sessão permitidas;
- os procedimentos e processos para a emissão, reemissão e suspensão de palavras-chave; e
- velar que os utilizadores se mantenham conscientes sobre a necessidade de proteger devidamente a sua palavra-chave.

Palavra-chave de uso único

As palavras-chave de uso único superam a principal desvantagem de sistemas convencionais de palavra-chave, nomeadamente, o facto da palavra-chave poder ser perdida, roubada ou por vezes violada e posteriormente usada várias vezes sem autorização.

O sistema de palavra-chave de uso único gera uma única palavra-chave para cada sessão. Isto é geralmente alcançado através de um dispositivo de *hardware* conectado que gera automaticamente uma palavra-chave O sistema das Alfândegas sabe que as palavras-chave ou

sequências estão associadas a cada utilizador e permitirá apenas o acesso caso haja compatibilidade.

Este método tem a desvantagem de exigir que todos os utilizadores adquiram, ou beneficiem, do *hardware* e *software* necessários. Uma implementação abrangente poderia ser onerosa, porém mais adequada para grupos de utilizadores heterogéneos. Uma debilidade que este sistema partilha com outros sistemas de autenticação consiste no facto deste depender também das práticas de segurança empregues pelos utilizadores para manter controle sobre os seus dispositivos de palavra-chave e os meios de o aceder.

Sistemas de confrontação e resposta

A confrontação e resposta são comummente usadas em combinação com outros métodos tais como as palavras-chave.

O princípio é o seguinte: o utilizador fornece as respostas a uma pergunta ao qual ele é o único que pode responder. Em algumas versões, o utilizador pode mesmo ser solicitado a sugerir a questão. As questões servem depois para "testar" a identidade da pessoa quando, por exemplo; os registos do utilizador precisarem de ser emendados ou haver a necessidade de emitir uma nova palavra-chave. A confrontação e resposta podem também ser usadas como uma verificação adicional de autenticação durante o início de sessão

Segundo a abordagem e as necessidades da administração, o sistema de confrontação pelo dispositivo de resposta pode revelar-se de funcionamento complicado. O processo de gestão do sistema pode envolver custos elevados e ter implicações financeiras contínuas para a administração.

Cookies

Cookies são símbolos instalados nos computadores dos utilizadores que podem ser usados para reconhecer a máquina do utilizador.

Como meio de autenticação do utilizador, os *cookies* trabalham assentes no pressuposto de que cada máquina é apenas usada por uma única entidade. Por conseguinte, não podem ser vistos como um meio fiável de autenticação para uma entidade particular.

Visto que os *cookies* podem ser usados para rastrear os hábitos de pesquisa de um indivíduo, pode também existir sérias questões de privacidade que emergem nos casos em que são mal utilizados. Os *cookies* podem também ser roubados e usados para aceder fraudulentamente ao sistema de uma administração. Além disso, o seu nível de aceitação pelos utilizadores é relativamente fraco.

Biometria

A maioria dos métodos de autenticação não associa uma identidade física ao utilizador quando este acede ao sistema da administração. A biometria procura ultrapassar esta questão mediante o oferecimento de uma ligação directa entre as conhecidas características fisiológicas e comportamentais de um indivíduo e do utilizador.

As características da voz, as impressões digitais ou a palma da mão, a retina ou a face, que são únicas, por exemplo, são codificadas numericamente e comparadas por um dispositivo de reconhecimento cada vez que o utilizador pretenda aceder ao sistema.

A biometria depende da possibilidade do utilizador ter acesso ao *hardware* de leitura sempre que este acede aos sistemas da administração. Depende também da segurança do código digital que representa a identidade do indivíduo.

Para além de ser caro, a aplicação abrangente da biometria pode encontrar dificuldades quanto à aceitação pelos utilizadores de alguns métodos de leitura biométrica empregues - por exemplo, em muitas culturas, o reconhecimento da íris pode ser considerado como uma invasão à vida privada.

Codificação Convencional

A codificação convencional é comummente conhecida como "criptografia simétrica". Relativamente aos algoritmos simétricos o emissor e o receptor devem usar a mesma chave (um arquivo informático com um único código de identificação também conhecido como chave secreta). Num exemplo muito simples, se a mensagem a ser enviada fosse a número 20, o emissor e o receptor poderiam concordar que o algoritmo a usar seria subtrair a chave da mensagem. Ambas as partes podem então concordar que a chave seja o número 2. O emissor codifica a mensagem ao número 18, envia, e o receptor descodifica acrescentando a chave para obter novamente o 20. Desde que seja usado um algoritmo complexo e ambas as partes mantenham as suas chaves seguras, podem ser obtidos bons níveis de confidencialidade. Os algoritmos simétricos oferecem também tempos rápidos de processamento.

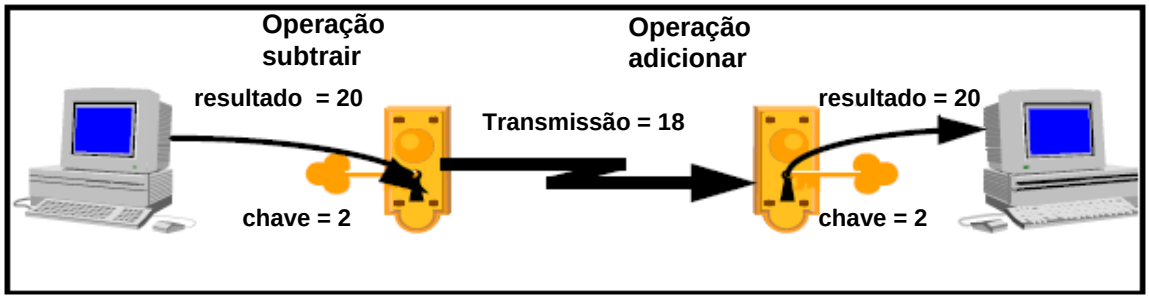


Figura 2: *Elementos de um sistema que usa chaves simétricas*

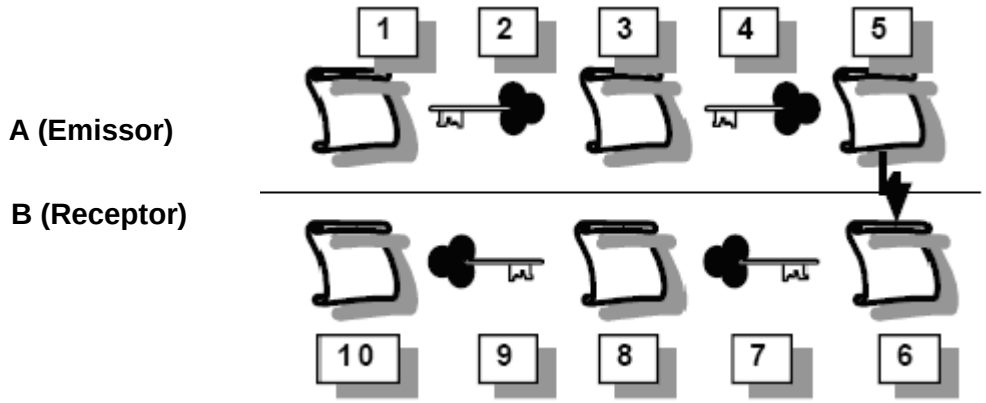
Contudo, a principal debilidade deste sistema consiste na emissão e distribuição das chaves que permitem o utilizador e o emissor identificarem-se mutuamente. Não basta apenas ser acordado um conjunto separado de chaves com cada utilizador, mas as chaves precisam de ser fisicamente fornecidas ao cliente de modo a manter alguma certeza de identidade. Nos casos em que são usados serviços de correio e terceiros para a entrega da chave, a segurança da identidade pode estar comprometida. Enquanto os algoritmos simétricos providenciam tempos rápidos de processamento para a codificação e descodificação, a gestão de chave necessária para garantir a autenticação pode revelar-se onerosa e inconveniente para o uso abrangente.

Criptografia de chave pública (certificados digitais)

Os problemas de distribuição de chaves associados à codificação convencional são resolvidos pela criptografia de chave pública. A criptografia de chave pública usa pares distintos de chaves para fins de autenticação (ou assinatura) e codificação (ou confidencialidade). Os pares de chave são referidos como chaves públicas e particulares. A criptografia de chave pública é frequentemente referida como "assimétrica", visto que as chaves públicas e particulares são diferentes.

A chave privada é apenas conhecida pelo seu proprietário, ao passo que a chave pública pode ser publicada e conhecida por todos. Uma mensagem codificada mediante o uso da chave

pública do receptor só pode ser descodificada com a chave privada correspondente. No quadro da norma RSA (atribuído o nome dos inventores), as chaves são construídas através da manipulação de dois números primos de grande extensão, mas as noções matemáticas respeitantes aos algoritmos são muito complexas para serem abordadas no presente documento. Portanto, qualquer pessoa pode codificar uma mensagem ao receptor pretendido, desde que conheça a sua chave pública. A desvantagem do uso de chaves assimétricas em vez de simétricas consiste no facto dos cálculos levarem mais tempo.



1 = Documento em texto claro sem assinatura electrónica;

2.= Chave privada do A para codificar o valor de controlo de dados + carimbo de data (=assinatura digital) (Integridade);

3 = Documento em texto claro com assinatura electrónica;

4 = Algoritmo simétrico para codificar o conteúdo (confidencialidade);

5 = Documento codificado e assinado electronicamente;

6 = Documento igual a 5;

7 = Algoritmo simétrico para descodificar o conteúdo (verificação de confidencialidade)

8 = Documento igual a 3

9 = Cálculo do valor de controlo de dados + carimbo de data; chave pública de A para descodificar o controlo de valor recebido; conferir ambos os valores (Verificação de Integridade)

10 =Documento igual a 1

Figura 3: *Fluxo de funcionamento do sistema de codificação de uma chave pública*

Embora a criptografia assimétrica resolva alguns dos problemas que possam ser encontrados com a distribuição de chaves, obriga o utilizador a manter sempre a segurança apropriada das suas chaves. A criptografia levanta também questões relativas à maneira como a identidade do utilizador é validada no momento da emissão da chave.

Infra-estrutura da chave pública

A Infra-estrutura da Chave Pública (PKI) procura ultrapassar problemas não resolvidos na criptografia assimétrica convencional. Usando a criptografia assimétrica como a sua base técnica, a PKI oferece um quadro para assegurar o conteúdo da mensagem, autenticando o emissor, bem como validar a sua identidade.

Estes objectivos são alcançados mediante a introdução de um certificado digital. Um

certificado digital é um documento electrónico assinado por uma Autoridade de Certificação reconhecida, que identifica o proprietário da chave e a entidade empresarial (onde for apropriado) que este representa. Vincula o proprietário da chave a um par de chaves mediante especificação da chave pública do referido par de chave.

A PKI envolve uma complexidade de elementos legais e organizacionais que permitem operar com eficácia. Estes elementos, juntamente com o trabalho da PKI são analisados detalhadamente na secção 11.9.

A PKI apresenta pontos fortes nas áreas de autenticação, integridade de mensagem, confidencialidade e não-rejeição dentro de uma solução única.

Contudo, um dos seus pontos fracos consiste na dependência dos processos de terceiros para a verificação de identidades e emissão de certificados com base nestas verificações. Isto pode ser remediado através da restrição das especificações ou realização da função na administração, mas apenas a custo extra.

Um outro ponto fraco é a própria segurança e práticas de gestão do detentor do certificado. Se o proprietário perder (ou permitir aos outros usar) o seu certificado, torna-se impossível confiar na sua autenticação.

Transport Layer Security (TLS)

O protocolo *Secure Sockets Layer* (SSL) é um conjunto de regras que regem a autenticação dos servidores (tais como servidores de *Internet*) e as comunicações codificadas entre os clientes e servidores. Este protocolo foi desenvolvido para garantir a transmissão de dados via *Internet*. O processo de autenticação ao abrigo do SSL usa a Codificação de chave pública e assinaturas digitais para confirmar se o servidor é realmente o que reinvindica ser. Não autentica o utilizador. Uma vez autenticado o servidor, o cliente e o servidor usam técnicas de codificação de chave simétrica para codificar a informação que estiverem a trocar. Para cada transacção usa-se uma chave de sessão diferente. Isto impede a capacidade de um *hacker* descodificar as mensagens. Subsequentemente, o protocolo "*Transport Layer Security*" foi desenvolvido como actualização da versão 3.0 do SSL.

Deve-se realçar que o SSL e o *Transport Layer Security* (TLS) asseguram apenas a confidencialidade e integridade do servidor. Estes, não asseguram a não-rejeição e salvo se apoiados por uma combinação de protecção apropriada da chave privada associada à vontade e capacidade do utilizador de validar certificados digitais, não asseguram uma autenticação eficaz. O SSL é bem conhecido devido ao seu uso no *Netscape Navigator e Internet Explorer* ou Pesquisador de *Internet*.

Em Maio de 1996, o desenvolvimento do SSL tornou-se da responsabilidade de uma organização internacional de normalização, o Grupo de Trabalho de Engenharia de *Internet* (IETF), o qual desenvolve muitas das normas de protocolo para a *Internet*. O TLS, a versão aperfeiçoada do SSL, foi lançado no princípio de 1999 e foi actualizado para TLS 1.2. O protocolo *Transport Layer Security* é uma tecnologia amplamente usada e as versões deste produto podem ser adequadas para uso das Alfândegas.

11.4.3. Que método utilizar?

"Qual é a solução de autenticação requerida?" é uma pergunta importante, mas não existe uma única resposta certa. A medida adoptada deve ser determinada pelo resultado de uma avaliação de riscos e sujeita à preparação de um plano de necessidades associado. A escolha de qualquer método ou combinação de métodos dependerá dos riscos e consequências que uma

administração pode enfrentar se uma identidade se provar falsa ou se as transacções e a informação forem rejeitadas. Dependerá também dos custos relativos e do ambiente de trabalho em que a administração opera.

11.4.4. Risco Aceitável

Já existem vários processos bem desenvolvidos para a identificação, avaliação e gestão de riscos. Um dos primeiros destes processos foi a norma AS/NZ4360.1999 (www.standards.com.au) da Austrália e Nova Zelândia. Esta norma figura igualmente na norma ISO/IEC27005:2011, Tecnologias de Informação – Técnicas de segurança – Gestão dos riscos ligados à segurança da informação, cuja secção 3.14 relativa à avaliação dos riscos define esta última como sendo um processo de comparação entre os resultados da análise dos riscos e os critérios de risco com vista a determinar se o risco e/ou a sua amplitude é aceitável ou tolerável [FONTE: ISO Guide 73:2009]. Podem existir outras normas nacionais disponíveis e recomenda-se que as administrações consultem estes documentos durante a avaliação dos seus riscos.

Para identificar e avaliar os riscos em contexto, as administrações devem considerar:

- o ambiente em que operam – incluindo quaisquer aspectos políticos, económicos, técnicos, institucionais e legais que afectem as suas operações;
- os seus utilizadores e seu relacionamento com estes;
- os tipos de transacções efectuadas, e
- os seus requisitos de actividades e operações.

Desta forma a administração ganhará uma visão ampla das áreas onde existem riscos. Por exemplo; a situação política pode exigir que a administração providencie ao público acesso abrangente à transacções *on-line*. Por conseguinte, a administração precisará de lidar com grupos diferentes de utilizadores, incluindo alguns com os quais já possui há muito tempo acordos de cumprimento e outros que podem vir a efectuar apenas uma transacção. Um ambiente legal de uma administração pode obrigá-la a depender das suas transacções como provas legais para efeitos de processos crimes, impondo desta forma uma obrigação de não-rejeição. As debilidades e ameaças identificadas à luz destas considerações são efectivamente os riscos que a administração precisará de avaliar.

A avaliação dos riscos identificados consiste, geralmente, na análise das consequências de cada risco e as probabilidades deste se concretizar – quanto mais graves forem as consequências maior será a probabilidade de concretização e menos aceitável será o risco. Depois disto, os riscos podem ser priorizados, as contra-medidas existentes podem ser avaliadas e outras medidas podem ser identificadas, caso necessário. A eliminação completa dos riscos é improvável e proibitivamente onerosa. A avaliação deve reconhecer que nem todas as soluções de autenticação são totalmente confiáveis e seguras. Todos os métodos de autenticação podem estar comprometidos devido aos recursos e habilidades suficientes, ou devido aos fracos procedimentos de segurança, práticas ou implementação.

O estabelecimento de um sistema informatizado altamente seguro, mas oneroso, pode de facto oferecer apenas uma vantagem marginal sobre outras soluções alternativas em termos de impedimento ou redução dos riscos e pode não justificar o custo adicional.

O objectivo é garantir que os riscos sejam reduzidos a níveis aceitáveis e que as medidas adoptadas tenham um efeito dissuasor sobre ameaças a que o sistema está exposto.. Por exemplo; uma administração pode ter constatado que as suas transacções electrónicas estão potencialmente expostas ao risco de rejeição porque não é capaz de garantir por si a identidade da entidade com a qual se comunica. Acredita que as consequências seriam graves – fraude de identidade, perda da receita e comércio ilícito. Decidindo que precisa do mais alto nível de

autenticação e segurança disponíveis, a administração pode ponderar uma solução de PKI, mas com provas fortes dos requisitos de identidade e controles estritos sobre a revogação de certificados. Contudo, actualmente os certificados digitais são quatro vezes mais onerosos, alguns provedores irão ponderar a hipótese de apoio às necessidades da administração, o esforço e o custo, no plano administrativo aumentarão significativamente.

Ao analisar de modo mais detalhado a probabilidade dos riscos se concretizarem, a administração constata que os seus grupos de utilizadores apresentam características e aspectos diferentes das suas actividades. Constata que a maioria das suas transacções são feitas com utilizadores de confiança com os quais tem fortes acordos de cumprimento e de procedimentos transparentes. Para estes utilizadores, pelo menos, a administração pode fazer face aos seus riscos através da tomada de uma medida menos onerosa e elaborada.

11.4.5 Comparação de métodos de autenticação

Ao identificar soluções apropriadas para a gestão de riscos, as administrações devem avaliar e comparar os métodos de autenticação. Muitos destes métodos são identificados no parágrafo 11.4.2, onde são também indicados os seus pontos fracos e fortes.

Ao comparar estes e outros métodos é importante ter em mente que não existe solução única e que é possível usar um combinação de métodos para alcançar altos níveis de autenticação e segurança. Por exemplo, ao efectuar transacções financeiras simples de baixo valor é comum usar PIN e palavra-chave em combinação com alguma forma de criptografia. De igual modo, o sistema de confrontação e resposta é frequentemente usado não como o principal meio de autenticação, mas sim como uma verificação secundária para actualizar a informação do utilizador nas transacções que apresentam riscos baixos ou moderados.

Cada método deve ser avaliado em relação às necessidades da administração e aos riscos identificados. Em seguida, pode ser seleccionado um método apropriado baseado na forma correcta com que este pode satisfazer as necessidades da administração à medida em que reduz os riscos da administração a um nível aceitável. Para além disso, vários métodos podem ser usados ao mesmo tempo, no qual será também necessário determinar como operam em conjunto.

11.5. Não-Rejeição

A não-rejeição é uma questão de particular preocupação para as Alfândegas, que desempenham normalmente funções em matéria de regulamentação, de arrecadação de receitas e gestão de fronteiras. Os relatórios, as declarações e a apresentação de documentos são frequentemente necessários por força da lei e as penalidades resultantes da violação das disposições da lei são normalmente encaminhadas ao tribunal.

Portanto, as Alfândegas devem considerar seriamente a amplitude na qual sejam capazes de associar correctamente as transacções e o conteúdo de mensagens com um determinado expedidor. Precisam também de considerar como devem assegurar-se de que uma vez sob o seu controle a informação não seja corrompida ou transformada de maneira que se torne inadmissível como prova.

11.5.1.Definição de não-rejeição

Há um problema inerente e muitas vezes desarticulado da noção de "não-rejeição". Em sentido técnico, a palavra é entendida como o uso de procedimentos criptográficos por uma parte de confiança para apresentar provas de que uma mensagem só podia ter sido enviada pelo signatário e mais ninguém. Isto geralmente significa que devem ser usados os procedimentos técnicos para identificar o signatário, assegurar a integridade da mensagem e estabelecer uma ligação entre o signatário e a mensagem. Este processo pode também ser alargado de modo a incluir a ligação da mensagem ao receptor. Contudo, do ponto de vista legal, o conceito de não-rejeição não existe. Em certas circunstâncias, independentemente da prova reunida pelos referidos procedimentos criptográficos, é ainda possível que uma pessoa negue as consequências legais desta transacção. Com efeito, é apenas possível limitar as oportunidades de rejeição.

Apesar destas anomalias, a não-rejeição pode normalmente ser definida como: "a garantia razoável de que uma entidade pode estar claramente ligada a uma transacção para efeitos de a vincular às consequências legais desta transacção".

A não-rejeição tem por finalidade garantir a certeza técnica e legal. Embora os requisitos técnicos e de actividades possam conduzir ao desenvolvimento de políticas de não-rejeição, é também uma questão legal. A não-rejeição deve ser considerada à luz das possíveis consequências legais futuras.

11.5.2. A não-rejeição não é uma questão autónoma

A não-rejeição é apenas uma das questões que uma administração precisará de considerar no desenvolvimento de um sistema de transacção ou realização de transacções electrónicas. As políticas e os processos de não-rejeição devem ser encarados como parte da abordagem de gestão de riscos, a qual trata de uma série de outras questões igualmente importantes incluindo (mas não limitadas a estas):

- privacidade;
- custo (para as Alfândegas e seus utilizadores);
- usabilidade;
- segurança;
- requisitos legais nacionais aplicáveis aos serviços públicos em geral (por exemplo, qualquer legislação geral que abrange a privacidade, liberdade de informação, manutenção de registos, etc.);

- requisitos legais aplicáveis especialmente às Alfândegas (por exemplo; legislação relacionada com as Alfândegas e Impostos ou, em alguns casos, a segurança nacional).

A política específica de não-rejeição e a solução legal/técnica adoptada por uma administração dependem das necessidades desta administração em relação a estas questões.

11.5.3. Consequências legais da rejeição

Não existe uma política única em matéria de não-rejeição, nem uma solução legal, comercial ou técnica única que permite limitar a rejeição que se aplica a todas as administrações. As arquitecturas, as políticas e os processos cujas administrações adoptam para evitar a rejeição variam em função das suas necessidades e do tipo de consequências legais que se pretende alcançar com as suas transacções.

De modo geral, as consequências legais das transacções enquadram-se em quatro categorias as quais são aplicáveis às Alfândegas:

Infracções Penais

Aplicáveis às transacções oficiais ou conforme a lei. As Alfândegas devem ter em conta a prova exigida no âmbito penal (além da dúvida razoável), o requisito de julgamento pelo júri, e os requisitos forenses específicos dos processos-crime.

Processos Civis

Aplicáveis às transacções comerciais (isto é, a administração compra ou vende bens e serviços). Normalmente são processos regulados pelo direito privado, embora outras soluções possam ser igualmente aplicáveis, por exemplo, alguns países podem ter disposições legislativas comerciais específicas. Em casos desta natureza, as instituições podem estar em condições de especificar formas alternativas de resolução de litígios tais como a arbitragem ou a mediação.

Contencioso Administrativo

Aplicável nos casos em que a transacção conduz a uma tomada de decisão em relação ao utilizador. Alguns países possuem tribunais de recurso que revêem tais decisões. Questões como a necessidade de garantir a justiça natural para o utilizador são relevantes aqui.

Acção Executiva

Por vezes, a solução mais eficaz das Alfândegas consiste em negar ao utilizador a oportunidade de lidar com esta electronicamente no futuro. Isto não exclui a rejeição de uma determinada transacção. Contudo, em alguns casos, a probabilidade de perder o acesso pode impedir o utilizador de tentar rejeitar uma transacção. O utilizador pode não ter qualquer direito de recurso contra a administração, mas nos casos em que existem os tribunais de recurso, um mediador ou outras vias de recurso, as administrações devem estar em condições de justificar as suas acções.

Uma administração deve ter em consideração o nível de risco aceitável de rejeição das transacções que esta gere. Ao avaliar estes riscos, deve igualmente ter em consideração equilíbrio entre o custo e a efectivação dos objectivos fixados.

A solução varia consideravelmente dependendo dos tipos de transacção envolvida e dos riscos associados. Com simples pagamentos financeiros, pode haver pouca necessidade de não-rejeição, sendo os dois principais riscos a demonstração da remessa e a recepção. A necessidade da não-rejeição será muito maior aquando da aceitação da garantia ou das declarações nas quais a entidade deve estar especificamente vinculada.

De igual modo, as soluções variam sensivelmente em função da tecnologia adoptada pelas Alfândegas. Uma administração que faça o uso de PIN e palavras-chave, por exemplo, pode precisar de realizar a sua própria autenticação envolvendo procedimentos internos e basear-se num simples acordo com os utilizadores. Por outro lado, uma administração que usa a PKI tem maior probabilidade de depender de terceiros e usará uma série complexa de acordos que se estendem além do utilizador.

11.5.4. Garantia

A não-rejeição é, essencialmente, um exercício de gestão de riscos. O nível de garantia que uma administração requer relativamente à identidade, conteúdo ou processo é o reflexo do risco de um utilizador rejeitar uma transacção e as eventuais consequências dessa rejeição.

Para que uma transacção electrónica seja bem sucedida convém recolher os elementos de prova (de uma maneira aceitável pelo tribunal, caso necessário) em relação a muitos aspectos da transacção, nomeadamente:

- o processo que permite provar a identificação (EOI);
- como é que a identidade do emissor de uma transacção electrónica é confirmada (por exemplo; controles de acesso, *PIN*, chave privada, etc.);
- se a administração impôs ou não quaisquer condições de uso;
- a informação fornecida aos utilizadores relacionada com os controles de acesso e possivelmente com a formação e outras representações ou instruções;
- a tecnologia de autenticação particular usada (arquivo, sistemas legais podem ser necessários);
- a versão de *software* de aplicação usado pelo utilizador;
- a forma como o *software* foi implementado naquela altura; e
- a prova do momento em que a transacção foi realizada.

11.5.5. Razões da rejeição

As razões pelas quais um utilizador rejeita uma transacção podem ser classificadas como se segue:

- **Razões específicas da transacção electrónica:** O utilizador alega que a transacção, ou uma parte da mesma, ocorreu sem o seu conhecimento ou aprovação (por exemplo, falsificação). Isto, usualmente envolve um desafio à integridade ou adequação dos procedimentos ou infra-estrutura técnica dentro da qual a transacção foi conduzida;
- **Razões legais gerais:** O utilizador admite que a transacção ocorreu, mas alega não estar legalmente vinculado à mesma.

As razões específicas da transacção electrónica podem incluir alegações, segundo as quais:

- a transacção foi falsificada ou alterada em trânsito por terceiros – por ofensa cripto-analítica ou por perda ou comprometimento da chave do utilizador, do símbolo, etc;
- a transacção foi falsificada ou alterada depois da recepção pela administração ou por um funcionário de má-fé ou infractor externo que conseguiu aceder ao sistema da administração;
- a identidade do utilizador é falsa devido a falhas do registo/EOI.

As razões gerais, em termos legais, pelas quais um utilizador pode tentar rejeitar uma transacção dependem do tipo de efeitos legais que a administração pretende que a mesma transacção tenha. O Anexo A fornece alguns exemplos deste capítulo.

Deve ser sublinhado que a não-rejeição de transacções feitas electronicamente requer, apenas, soluções técnicas. Por exemplo, pode ser apropriado que uma transacção seja considerada através de procedimentos *off-line*, para minimizar os riscos de rejeição. Por conseguinte, um utilizador pode ter de imprimir um formulário obtido no *website*, preenchê-lo e enviá-lo por correio, por fax ou entregar o formulário preenchido à administração interessada.

Uma provável razão legal para a rejeição é o facto do utilizador não estar totalmente informado sobre o conteúdo da transacção que alegadamente aprovou. Em larga medida, a solução no plano técnico para este tipo de fraudes é permitir que o conteúdo seja totalmente revelado no sistema e, se necessário, passar na tela do computador, antes do utilizador pressionar a tecla “concordo” ou “enviar”.

11.6. Garantia de Identidade

11.6.1. *Prova de Identidade*

Enquanto que a questão é essencialmente o da autenticação, a prova usada no estabelecimento de uma Identidade Electrónica (EOI), bem como os procedimentos usados na verificação da prova, formam a base indispensável para estabelecer uma ligação entre uma entidade e as suas transacções. Uma falha a este nível aumenta o risco de rejeição das transacções baseadas na identidade.

A administração deve comparar as exigências EOI em relação às suas próprias necessidades, para autenticar a identidade e evitar rejeições de transacções. Como as consequências da rejeição tornam-se muito sérias, são necessários níveis mais elevados de validação e de prova.

Uma outra complicação surge quando os métodos de autenticação envolvendo terceiros (como por exemplo uma Infra-estrutura Chave Pública “PKI”) requerem acordos específicos para estabelecer as obrigações de terceiros, bem como para assegurar a identidade. Todavia, estas questões são resolvidas no âmbito do “*Gatekeeper Framework*”, relativas ao funcionamento das Autoridades de Certificação.

11.6.2. *Prova de Autorização*

A prova de autorização para executar transacções é particularmente importante quando são os agentes ou empregados de uma instituição a executarem as transacções. É fácil rejeitar uma transacção quando não há ligação clara entre a identidade electrónica e a autorização para o seu uso.

A este respeito, é importante o uso de acordos legais para a criação de identidades

electrónicas. O momento em que são estabelecidos, as pessoas a quem vinculam e a forma que tomam são influenciados pelo tipo de transacção, pelo sistema e pelos procedimentos específicos escolhidos pela administração envolvida.

11.6.3. *O quadro*

A garantia da identidade depende da posse por parte dos utilizadores, de ferramentas apropriadas de controles de verificação (tais como os Números de Identificação Pessoal "PIN" ou chaves particulares), sendo o acesso restrito à pessoa adequada. Neste contexto, a questão relacionada com o uso da identidade necessita de ser considerada quer em termos da responsabilidade do utilizador, para segurança da sua identidade, quer em termos de protecção que os sistemas e os procedimentos de uma administração proporcionam, para salvaguarda da identidade. Tais responsabilidades são normalmente estabelecidas mediante acordos entre as partes.

Como são armazenadas as identidades – (por exemplo, em senhas especiais: tais como cartões electrónicos ou directamente em *disk drives* de computadores, onde aplicável). O utilizador deve estar ciente da necessidade de armazenamento dos registos de forma segura, bem como de outras questões que devem ser consideradas pelas administrações.

11.7. Garantia do Conteúdo

11.7.1. *Garantia da Integridade*

Durante o ciclo de vida de uma transacção o seu conteúdo é acedido, manipulado, accionado e armazenado. Durante todo este período o conteúdo do autor necessita de ser identificável e reproduzível, assim como o da transmissão original. Se uma administração estiver incapaz de reproduzir o conteúdo e de demonstrar a sua integridade, através do processo que a mesma utilizou para conduzir a transacção, as suas acções podem, talvez, ser contestadas e o conteúdo sujeito à rejeição.

A ligação entre a identidade electrónica e o conteúdo de uma transacção é de importância primordial. Sem isso, pode falhar qualquer tentativa para restringir a rejeição de uma transacção. A gestão deste assunto depende da solução técnica adoptada pela administração. Um certificado electrónico que faça parte de um correio electrónico com um conteúdo anexo, pode facilmente ser separado e os procedimentos administrativos podem se tornar necessários para preservar a comunicação original e completa. Um processo de transacção completamente automatizado pode, simplesmente, requerer a manutenção dos *logs* de transmissão electrónica detalhados, bem como acessos e alterações autorizadas.

11.7.2. *Combinar as diferentes partes*

As transacções podem sempre envolver um número de componentes de comunicação electrónica e de decisões. É importante que todas as componentes de uma transacção sejam rastreadas e mantidas ligadas a uma transacção específica. Onde nem todas as componentes podem ser recuperadas para o fornecimento de provas de toda a transacção, a integridade da mesma pode ser questionada, e parte dela ou o seu todo pode ser rejeitada.

Procedimentos apropriados, como "*registo"* e "*anotação"* necessitam de ser considerados.

11.7.3. *Armazenamento e Reprodução*

Existem várias questões ligadas ao armazenamento e reprodução do material da

transacção que afecta a rejeição.

A integridade do local de armazenamento, a forma como um documento é armazenado, a gestão e actualização dos mecanismos de criptografia, nos casos em que são usados, bem como as ligações mantidas entre os dados a serem processados, estão todos relacionados com a consistência das provas que limitam a rejeição.

11.8. Integridade dos Processos

11.8.1. *Sistema de Gestão*

A concepção de qualquer procedimento da actividade, inclui elementos que garantem a qualidade e, por conseguinte, a integridade quer do procedimento quer do material a ser processado. Isto corresponde aos pontos mais relevantes do processo para limitação da rejeição. De uma maneira geral, envolvem assuntos de governação, tais como a identificação das responsabilidades de tomada de decisão e os procedimentos para autorização e revisão do acesso.

Como estes procedimentos dizem respeito a integridade de uma transacção, os mesmos são essenciais às garantias necessárias para evitar rejeições, e constituem uma importante fonte de elementos de prova, se for necessário que a administração se defenda contra as acusações de fraude ou negligência interna.

11.8.2. *Arquitectura e Regulamentos do Sistema*

Ao considerar a fiabilidade dos documentos, os tribunais podem examinar a integridade e a capacidade dos sistemas electrónicos utilizados. Neste contexto, diversas questões importantes para limitar a rejeição incluem os regulamentos do sistema, do *software* e da arquitectura.

Os sistemas electrónicos operam no âmbito de um quadro de normas - decisões predeterminadas que afectam as medidas tomadas relacionadas com cada transacção. Estas normas podem abordar questões que variam desde os termos e alcance do acesso ao que é registado ou arquivado, quando e em que forma. Necessitam de ser revistos, do ponto de vista das garantias que os mesmos oferecem.

11.9. Infra-estrutura de Chave Pública (PKI)

A PKI é um dos métodos mais complexos de autenticação. Como o nome implica, a PKI não é uma “solução isolada” mas sim uma “infra-estrutura” centrada na criptografia de chave pública, envolvendo tanto uma estrutura organizacional como um sistema legal. Deste modo, ao contrário de muitas outras soluções, a PKI tem como objectivo oferecer um pacote “completo” de tecnologias e procedimentos de integração, de maneira a garantir a autenticação e a integridade, bem como reduzir a possibilidade de rejeição.

Este método, embora ainda não seja de uso comum, surge como uma das soluções mais eficazes para organizações que exigem altos níveis de garantia. Como as Alfândegas muito provavelmente estão requerendo tal exigência, foi decidido tratar a PKI separadamente e de maneira detalhada.

11.9.1. Antecedentes

A decisão das Alfândegas para permitir aos operadores económicos, despachantes, transportadores e outras entidades habilitadas a declarar as suas mercadorias, na importação e exportação de forma segura, via Internet ou com a ajuda de fornecedores de serviços de Redes Adicionadas (VAN), envolve questões de segurança da Tecnologia de Informação (TI), abordadas nas secções anteriores.

A *Internet* é por natureza um sistema aberto. Os seus pontos fortes decorrem desta abertura, do seu baixo custo e do seu fácil acesso, que a torna num meio pouco oneroso de efectuar transacções aduaneiras e comerciais. Todavia, o seu carácter aberto pode também ser uma principal ameaça para os utilizadores.

A natureza aberta do sistema torna-o relativamente fácil para as comunicações via *websites* e *Internet* serem comprometidas, bem como os bens/activos de TI de uma Alfândega usados na comunicação EDI estão expostos a tais ameaças. Ao considerar as estratégias para atenuação é necessário fazer referência aos padrões que os vários órgãos estão desenvolvendo. As transacções via *Internet* implicam quatro tipos genéricos de riscos, estando estes relacionados com: a) a privacidade da mensagem; b) a sua autenticidade; c) a sua integridade e d) a sua não rejeição. A PKI baseada na tecnologia de criptografia de chave pública, proporciona um meio para limitar estes riscos.

As normas EDIINT foram desenvolvidas por um Grupo de Estudo Técnico encarregado da *Internet* (*Internet Engineering Task Force* - IETF), para abordar as questões relacionadas com a protecção das técnicas de comunicação EDI, através da *Internet*. Estas normas definem as PKI como uma das técnicas de facilitação que permitem resolver esses problemas de segurança.

11.9.2. Definição de uma PKI

Uma PKI pode ser definida como a arquitectura, a organização, as técnicas, as praticas e os procedimentos que colectivamente suportam a implementação e a operação de um certificado baseado num sistema de criptografia de chave pública. Isto inclui um conjunto de políticas, procedimentos, servidores, softwares e estações de trabalho para o propósito de administração de chaves e de certificados digitais. Um sistema de criptografia de chave pública funciona por meio de algoritmos de sistemas de criptografia assimétrica.

11.9.3. Comparação de assinaturas digitais e convencionais

O desafio para a PKI é a tradução das convenções credíveis no mundo físico e fazê-las funcionar nas transacções *on-line*. As assinaturas não são a substância das transacções. As mesmas representam apenas um evento nas transacções, e transmitem certas características aos objectos envolvidos na transacção. Mais precisamente, uma assinatura no papel autentica o signatário e o documento assinado. Por conseguinte, o signatário deixa uma marca distintiva, e a sua caligrafia converte-se em assinatura, que depois se torna numa prova, estabelecendo uma ligação entre o signatário e o documento assinado. O signatário de um documento em papel conhece a importância de que se reveste o acto de assinar e a finalidade associada à assinatura. Em direito comum, o acto de assinar implica que o signatário na altura devida aprova o conteúdo do documento a ser assinado. Os documentos assinados representam “etapas” distintas ou etapas finais numa transacção.

As assinaturas convencionais são baseadas no papel e, por conseguinte, na ausência

deste as características da assinatura devem ser configuradas em assinatura digital. A tecnologia PKI permite a produção, a verificação de assinaturas e o arquivo/registo dos documentos verificados, como também o fornecimento de provas sempre que necessário. Uma real implementação da PKI deve, por conseguinte, abordar estes aspectos.

11.9.4. O ciclo de vida operacional de um certificado digital

De acordo com a PKI, uma pessoa pode solicitar um certificado digital, criando primeiro um par de chaves constituído por uma chave pública e uma chave particular. O requerente deve, seguidamente, preencher um formulário de solicitação de um certificado digital para assinatura e/ou de autenticação, e enviá-lo para uma Autoridade de Certificação.

A Autoridade de Certificação recebe a solicitação, verifica se o par de chaves submetido pelo requerente forma um par de chaves criptográfico válido, bem como verifica a exactidão da informação fornecida pelo mesmo, e, de seguida emite um certificado digital, que é assinado pela própria Autoridade de Certificação.

A chave pública é publicada num directório, que usualmente cumpre com a norma X.5000 da União Internacional de Telecomunicações (ITU). O requerente mantém segura a chave particular correspondente, para uso em conexão com a codificação e/ou assinatura e/ou operações de verificação.

O certificado é valido apenas para um certo período de tempo devendo, por conseguinte, ser renovado periodicamente. Por certas razões específicas – principalmente o uso impróprio do relatório ou o comprometimento de uma chave particular – a Autoridade de Certificação deve suspender ou revogar um certificado digital. O ciclo de vida operacional está descrito na forma RFC 2527 do Grupo de Estudo Técnico encarregado da *Internet* (*Internet Engineering Task Force* - IETF),

11.9.5. Considerações importantes na implementação de soluções baseadas na PKI

Na óptica das vantagens oferecidas pela tecnologia PKI, as Alfândegas podem querer considerar o uso de sistemas baseados na PKI ao projectarem e implementarem as soluções para as mensagens EDI. Isto requer uma capacidade para gerir os certificados e as assinaturas digitais nos procedimentos da actividade das Alfândegas e dos sistemas informáticos.

A implementação da PKI permite reforçar as capacidades em relação ao armazenamento seguro dos dados electrónicos, como também da transmissão electrónica dos dados, através da utilização de certificados (assinaturas) digitais. Contudo, antes de iniciar a implementação, as administrações devem primeiramente considerar o âmbito dos seus PKI. Isto, normalmente requer a preparação de um Documento de Expansão, que descrimine os objectivos, as pretensões e metas, bem como quaisquer limitações que necessitam de ser colocadas no projecto.

É importante ponderar as limitações para evitar a expansão do projecto desnecessariamente às áreas onde a administração já tenha expandido a implementação. O documento de expansão pode incluir cenários ilustrativos indicando como a administração deve utilizar os certificados de autenticação digitais, para proteger as mensagens e a assinatura. Ver a figura 6, como ilustração.

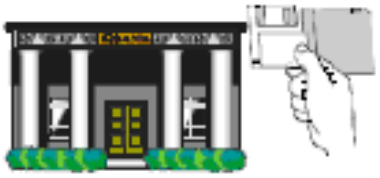
Particularmente, devem ser dados passos para assegurar que todas as soluções de comércio electrónico e EDI implementadas pela administração sejam conformes e compatíveis com a PKI.

Efectuar as transacções com as Alfândegas

PRONTO – Obtenção do Certificado

Sistema de Registo do Utilizador

- Visitar o Website das Alfândegas para informação sobre como lidar electronicamente com as Alfândegas.
- Fornecer detalhes sobre a identidade à Autoridade de Registo (RA) aprovada.
- Obter um certificado digital da Autoridade de Certificação (CA) aprovada.



Autoridade de Certificação (AC)

Sistema de Registo do Cliente

GRUPO – Registar como Utilizador das Alfândegas

Reggie (Agente de Carga) | Alice (Importadora) | Eddie (Exportador)

- Preencher o Formulário de Registo do Utilizador das Alfândegas.
- Certificado e o formulário de registo validados pelas Alfândegas, e o utilizador é notificado de que o registo está concluído.

SAÍDA – Inserir Transacções Aduaneiras

Completar a Transacção Online.

Assinar a Transacção com a Chave Particular, anexar o certificado.

Codificar a Transacção com a Chave Pública obtida das

- Transmitir a Transacção às Alfândegas.
- Assinatura Digital/Certificado validado pelas Alfândegas.
- Transacção do Utilizador

Fonte: Administração das Alfândegas Australianas, 1999

Figura 6: "*Alice e Eddie*"

11.9.6. Uso de assinaturas digitais no EDI e nas mensagens de Linguagem de Marcas Extensível (XML)

O Consórcio WWW (W3C) e o Grupo de Estudo Técnico encarregado da *Internet* (*Internet Engineering Task Force* - IETF),estão a trabalhar sobre uma norma para assinatura digital por XML. A UN/CEFACT e a OASIS estão a trabalhar sobre a integração SOAP (Protocolo de Acesso de Objecto Simples) com especificações anexas em especificações *ebXML (www.ebxml.org)*. Isto resultará em uma norma aberta e global para o transporte credível de mensagens electrónicas comerciais através da Internet.

As especificações de mensagens *ebXML* em si, englobam um conjunto de serviços e protocolos que permitem ao Utilizador solicitar serviços a partir dos servidores sobre o protocolo de transporte a nível dos aplicativos comummente usados, tais como o SMTP (Protocolo de Transferência de Mail Simples), http (Protocolo de Transferência de Hiper texto) e outros. O *ebXML* permite mensagens de propósito gerais envolvendo um cabeçalho de mensagem que suporta *payloads* múltiplos, enquanto proporcionam assinaturas digitais dentro e entre as mensagens digitais relacionadas com quaisquer especificações.

As mensagens UN/EDIFACT proporcionam o uso de assinaturas digitais juntamente com as mensagens electrónicas. Para além disso, as mensagens UN/EDIFACT proporcionam a importação e a exportação de chaves públicas (fornecidas via formato de mensagem UN/EDIFACT KEYMAN). À semelhança de outras formas de mensagens, as administrações necessitam de ponderar as questões envolvidas com o *registo* e arquivo de tais mensagens, por conseguinte, manter a segurança dos dados, de maneira a gerir as consequências da rejeição.

11.9.7. Autoridade de Certificação e Quadro Legal

Depois de decidir sobre uma solução baseada na PKI, as Alfândegas têm de considerar várias questões técnicas e legais que surgem no decorrer da implementação da PKI. Conforme acima indicado, a PKI requer um sistema para a produção e manutenção dos certificados digitais. Isto é normalmente alcançado através do estabelecimento de uma Autoridade de Certificação.

A Autoridade de Certificação é uma entidade que atesta a identidade de uma pessoa ou de uma organização. A principal função da Autoridade de Certificação é verificar a identidade das partes e emitir certificados para confirmar a identidade. Os certificados digitais são uma forma de verificar a identidade de uma pessoa ou (de uma empresa). Os equivalentes digitais de cartões de identidades, auxiliam a estabelecer as características de segurança desejáveis para as transacções através da *Internet*.

O quadro nacional legal respeitante à PKI, que especifica as exigências técnicas, bem como as legais, tem uma importante relação com o seguinte:

- a forma como são emitidos os certificados digitais por uma Autoridade de Certificação;
- como a Autoridade de Certificação gere o ciclo de vida de um certificado;
- que normas técnicas devem ser aplicadas.

Para um quadro legal modelo, as administrações podem provavelmente considerar as orientações apresentadas no modelo legal da UNCITRAL sobre o assunto (*http:/www.uncitral.org/en-index.htm* - Modelo Legal da UNCITRAL sobre Assinaturas Electrónicas e o Guia 2001 para promulgação).

Entre outras coisas, o quadro legal deve cobrir:

- a maneira como a informação digital deve ser autenticada por meio de uma assinatura digital e a admissibilidade de tal assinatura como prova nos tribunais;
- o processo de criação de uma assinatura digital;
- o processo de verificação das assinaturas digitais;
- as normas técnicas aplicáveis a estes processos;
- o licenciamento de Autoridades de Certificação; e
- as directivas aplicáveis em matéria de segurança ao funcionamento de uma Autoridade de Certificação.

Na ausência de um quadro legal geral, as administrações podem ponderar a celebração de acordos bilaterais e multilaterais com os utilizadores e os fornecedores de serviços, similares aos acordos VAN, mas tendo em conta a tecnologia PKI permitida.

11.9.8. PKI e Alfândegas: Principais questões a analisar

As Administrações podem aferir se estão em condições de preencher as funções de uma autoridade de certificação ou se outra instituição pública/do Estado ou privada oferece serviços de certificação com qualidade aceitável. Existem, a este respeito, em função dos países, modelos diferentes no âmbito dos quais as autoridades de certificação podem funcionar, conforme o quadro legal em vigor, enquanto cadeias (ou hierarquias) de confiança. Independentemente do modelo escolhido, e da autoridade de certificação escolhida, vários pontos deverão provavelmente ser objecto de uma decisão, juntamente com a aceitação dos certificados numéricos emitidos pela Autoridade de Certificação.

Apêndice A da Parte 11. Segurança das TIC

Exemplos de razões jurídicas de rejeição nos processos civil e criminal australiano

1. Procedimentos Penais

1.1 Falhas de natureza judicial (é provavelmente a causa mais comum de falhas em procedimentos criminais): a ausência de elementos de prova suficientemente persuasivos (falta de registo, arquivo, etc.); ou a inadmissibilidade de elementos de prova (problemas com actividades de investigação ou recolha de prova, ou problemas jurídicos ligados à admissibilidade dos registos informáticos).

1.2 Falta de elemento subjectivo:

De natureza individual (aplicável a ofensas gerais tais como fraude – pode não ser aplicável quando há violação à legislação de certas administrações, por exemplo ao Código Aduaneiro); ou de natureza colectiva – se aplicável, a intenção colectiva deve ser inferida a partir da intenção/conduta dos funcionários e agentes.

1.3 Meios de defesa tais como a insanidade mental ou o automatismo (improvável neste contexto).

1.4 O acusado é menor em matéria de responsabilidade criminal (10 anos de idade em Nova Gales do Sul) (improvável – indica sérias falhas EOI).

1.5 Pretensão de furto de identidade (que tem ocorrido mesmo se um processo apropriado de prova de identidade/registo tenha sido implementado).

2. Procedimentos Cíveis

(Nota: os exemplos seguintes estão relacionados com o cenário de um contracto entre uma administração e um utilizador. Existem outras possíveis acções cíveis, por exemplo um *e-mail* dando um mau conselho conduz a uma acção por delito de natureza civil por falsa declaração por negligência, mas isto parece improvável no contexto das transacções com as Alfândegas).

2.1 Defeito na celebração do contrato vinculativo (ausência de processos *click-wrap*) ou elementos de prova insuficientes no processo. Inclui:

- Aprovação do utilizador não claramente demonstrada no processo; ou

- Termos e condições não adequadamente indicados.

2.2 Defeito na celebração do contrato vinculativo por razões não relacionadas com o processo, incluindo a falta de consideração ou de intenção para estabelecer relações legais. Pode também incluir soluções que permitam o cancelamento sem falha: por exemplo erro mútuo (mas pouco provável).

2.3 Acção errada cometida pelo destinatário (ou em alguns casos por um terceiro). Várias soluções permitem a um tribunal colocar de parte uma transacção, incluindo a coação (física ou económica), conduta inaceitável, prática dolosa ou comportamento enganoso (TPA s. 52), Yerkey v. Jones, etc.

2.4 (Utilizador individual apenas) soluções de protecção do consumidor tais como a Lei de Revisão de Contratos da Nova Gales do Sul (NGS).

2.5 (Quando o utilizador é uma organização) o representante/agente individual tem agido sem autorização

2.6 Furto de identidade (o mesmo que em 1.5).

2.7 O utilizador é menor de idade ou não possui capacidade contratual.

11.10. Gestão da identidade

[Proposta de inserção no Capítulo 11, como nova Secção 11.10)

A gestão da identidade consiste na verificação da identidade de uma entidade que tenta obter um acesso à distância a um sistema informático, reivindica a paternidade de uma comunicação electrónica ou assina um documento electrónico. Nos sistemas informáticos, as identidades em linha são «electrónicas». Por altura da interacção "*face-à-face*", a identidade é verificada assegurando-se visualmente dos atributos correspondentes. Da mesma forma, as identidades electrónicas em linha devem ser verificadas com cuidado antes de autorizar uma pessoa ou uma identidade a participar em transacções por via electrónica. A Secção 11.6 evoca as questões relativas às garantias da identidade. É no entanto necessário tratar os problemas colocados em matéria de segurança e de comércio através da utilização operacional de identidades electrónicas e a presente secção evoca os problemas de gestão de identidades electrónicas do ponto de vista do seu ciclo de vida.

O uso generalizado das TIC conduziu a uma multiplicação dos aplicativos e das redes internas. Para aceder a um aplicativo ou a uma rede, um sistema específico de identificação e autenticação deve ser utilizado. Com o andar do tempo, muitos sistemas de identidade, muitas vezes compatíveis entre si, tendem a aparecer. Os utilizadores das TIC não são capazes de gerir uma multidão/multiplicidade de identidades electrónicas e podem não conseguir preservar palavras-chave de qualidade, conforme descrito acima no presente Capítulo. Vão assim acumular muitas palavras-chave, o que tornará ainda mais difícil a gestão das contas e das palavras-chave, complicará o processo de autenticação e levará a um número excessivo de contas de utilizadores inactivos e órfãos. Este cenário produzirá infalivelmente carências em termos de segurança e de controlo, os sistemas informáticos ficando assim expostos ao roubo de palavras-chave e à sua exploração para fins criminais. Os princípios e as práticas da Gestão de identidade visam trazer soluções com vista a uma gestão corrente das identidades electrónicas em um ambiente onde os utilizadores devem poder aceder a muitos aplicativos.

A OCDE define como se segue a Gestão da Identidade:

«A Gestão da identidade numérica designa o conjunto das regras, procedimentos e elementos técnicos necessários para implementar a política de uma organização no que concerne à criação, à utilização e à troca de informações de identidade numérica para o acesso a serviços ou recursos. Para serem eficazes, as políticas de Gestão da identidade numérica ao longo do seu ciclo de vida - desde o seu registo até à sua revogação – maximizando os ganhos potenciais ligados à sua utilização, nomeadamente entre diferentes domínios para a prestação de serviços integrados na Internet.

«O papel da gestão numérica na economia internet: guia introdutório à atenção dos decisores» (Junho de 2009), Grupo de trabalho da OCDE sobre a segurança da informação e da vida privada

A gestão da identidade é um elemento importante da segurança informática. Contribui para a resolução dos problemas seguintes:

Oferece um controlo do acesso material e lógico aos sistemas informáticos. É graças a esses controlos que é possível garantir que apenas as pessoas autorizadas acedam aos dados pertinentes e executem nesses dados as operações autorizadas.

Protege as pessoas de qualquer acesso não autorizado a informações pessoais e do roubo de identidade durante o uso em linha das identidades electrónicas. Essas pessoas querem ter a certeza que as suas identidades electrónicas não serão utilizadas de maneira imprópria ou

comprometidas quando elas são utilizadas nas transacções electrónicas. A Gestão da identidade contribui portanto para proteger a sua vida privada em linha.

Num contexto de crescimento rápido dos serviços em linha, as pessoas têm dificuldades em gerir os procedimentos de acesso definidos em separado para cada serviço. Por exemplo, a necessidade de memorizar e utilizar identificadores e palavras-chave distintos para cada serviço em linha, as suas informações pessoais multiplicam-se sobre cada um dos diferentes serviços informáticos, o que abre o caminho para eventuais violações dos dados e das responsabilidades correspondentes.

A Gestão da identidade compreende dois processos principais, a saber a identificação (identificar a pessoa) e a autenticação (verificar que a pessoa é efectivamente quem pretende ser). A identificação consiste em associar a pessoa a atributos que a caracterizam. Estes atributos apresentam-se sob a forma de informações de base sobre a pessoa. Podem ser de ordem física (características biológicas) ou documental (documentos atribuídos ou associados à pessoa, por exemplo um passaporte ou um bilhete de identidade). Os atributos que ajudam a distinguir as pessoas entre si contribuem para identificá-las eficazmente e os atributos correspondem a uma única pessoa são «identificadores únicos". O processo de registo das informações sobre a identidade é designado "inscrição". A inscrição é um processo em uma etapa que permite verificar ou provar a identidade de uma pessoa. O objectivo da inscrição é poder utilizar posteriormente as informações para efeitos da autenticação. O nível de garantia que oferece o processo de identificação aumenta com o número e a variedade dos atributos recolhidos. No entanto, neste caso, o risco de uma utilização imprópria dos dados pessoais e provados recolhidos durante a inscrição é maior. Quanto menos atributos forem recolhidos durante a inscrição, mais o risco de violação da vida privada é fraco.

A verificação dos atributos recolhidos pode efectuar-se em linha (por intermédio de uma confirmação visual que os atributos correspondem à pessoa a identificar) ou fora de linha/*offline* não (enviando um número pessoal de identificação por correio registado. A exactidão das informações pessoais recolhidas depende da fiabilidade dos dados e da pessoa ou do sistema encarregado(a) de avaliar a validade do atributo. Informações pessoais como a altura podem ser avaliadas de maneira fiável e não se espera que variem. Em contrapartida, a verificação das impressões digitais depende da precisão do sistema de registo do atributo e da verificação posterior. A verificação varia em função do tipo de informação sobre a identidade por verificar, a sua origem, dos processos de verificação implementados e da precisão do sistema de verificação.

O processo de identificação conclui-se com a entrega de identificadores (palavra-chave do utilizador, fichas de autenticação, etc.). Alguns identificadores baseiam-se nos atributos biológicos das pessoas.

Os serviços de lista/directório servem para armazenar e gerar as contas, as informações sobre a identidade e os identificadores de acesso. Na ausência de sistemas de «identidade federada», as informações sobre os identificadores são conservadas em listas/directórios distintos e destinados a aplicativos distintos. A federação das identidades permitiria manter actualizadas mais facilmente as políticas de gestão dos direitos associados aos identificadores electrónicos. As actividades ligadas à gestão da conta-utilizador, do ciclo de vida da identidade e do acesso tornam-se consideravelmente mais simples.

A gestão da identidade federada implica «terceiros» encarregados da gestão das contas, da autenticação e da gestão do acesso. Graças às soluções de identidade federada, os utilizadores já não ficam submersos com uma multiplicidade de identificadores e de palavras-chave. A solução de gestão da identidade por um terceiro equivale/corresponde a uma "janela única" para o utilizador e para o sistema ao qual acede. O terceiro é o "fornecedor de identidade", o utilizador é o "sujeito" que deseja aceder ao sistema informático de uma empresa ou de um governo designado "terceiro de confiança". Não é necessário que o terceiro seja uma entidade

comercial diferente mas o seu papel é claramente distinto. As soluções de gestão da identidade federada compreendem riscos jurídicos, como a perda de dados de carácter privado implicando um acesso não autorizado aos atributos da identidade do utilizador. O comprometimento das informações que figuram no bilhete de identidade do utilizador pode resultar em riscos de autenticação errónea ou de acesso não autorizado e expor a sanções incorridas por ter forçado o acesso a um sistema. Convém reduzir esses riscos tomando as contra-medidas que se impõem.

Em conclusão, as presentes Directivas convidam as Administrações Aduaneiras a aplicar soluções e princípios seguros para a Gestão da identidade, a fim de melhorar a segurança e reduzir o tempo perdido em actividades improdutivas ligadas à gestão dos utilizadores.

12. Questões legais

(Norma 7.4)

12.1. Introdução

Não é possível dar orientação específica sobre questões legais que sejam igualmente válidas para todas as Alfândegas, porque cada administração opera sob um sistema legal diferente e em diferentes bases legais. A orientação dada neste documento tem como intenção proporcionar ao leitor uma compreensão inicial das questões legais mais comuns. Orientação sobre as implicações legais dos procedimentos aduaneiros automatizados deve ser obtida de peritos relevantes nas primeiras etapas de um projecto.

Tratando-se de questões legais, importa lembrar que as leis possuem diferentes áreas de aplicabilidade, por exemplo:

- Convenções Internacionais (por exemplo a Convenção de Quioto Revista);
- Leis supranacionais (por exemplo a Legislação Comunitária, com implicações tais como a aplicabilidade directa e primazia);
- Leis nacionais com aplicabilidade geral que podem afectar entidades dentro e fora do domínio das Alfândegas (por exemplo, leis da privacidade, leis do comércio electrónico leis da assinatura digital, leis da protecção de dados);
- Leis nacionais com âmbito específico, tais como as leis nacionais aduaneiras que afectam apenas aqueles dentro do domínio das Alfândegas; e
- Leis sobre os procedimentos aduaneiros, que estão limitadas a um procedimento aduaneiro (por exemplo deve existir uma lei de trânsito aduaneiro).

As questões legais são ocasionalmente citadas como obstáculos intransponíveis para a implementação de algumas opções dos sistemas propostos. Um vasto número de administrações membros constatou que para mudar as obrigações legais não é necessário um processo difícil e moroso.

12.2. Adaptabilidade da legislação existente

Quando um procedimento aduaneiro está para ser informatizado é improvável que a vasta maioria da legislação existente requeira emendas. Contudo, a informatização pode ter efeito de simplificação dos procedimentos, que precisam de ser reflectidos nas disposições legais. As definições de responsabilidades podem necessitar de ser alteradas, incluindo o ponto no qual o pagamento é devido, quando uma declaração é considerada ter sido feita, etc.

12.3. Tipos de questões legais

Num ambiente electrónico, as questões legais que necessitam de ser tomadas em consideração quando um novo sistema é introduzido pode ser dividido em grupos, conforme abaixo descriminado. Deve-se notar que grupos deste tipo são sempre artificiais e criados apenas para propósitos de apresentação. Na prática, o grupo não tem qualquer valor legal e as questões sobrepõem-se de um grupo para o outro.

- Questões legais relacionadas com o Intercâmbio Electrónico de Dados (EDI) (requisitos formais, por exemplo provisões que requerem o uso de papel, um documento, um documento assinado, etc., e exigências relacionadas com o uso e aceitação de dados electrónicos como prova);
- Questões legais associadas à segurança (formato e media para o armazenamento de dados, autenticação, integridade, não rejeição, agradecimentos, etc. e também questões relativas à prova);
- Questões legais relacionadas com a protecção de dados (restrições de acesso aos dados, restrições na transferência dos dados entre administrações, etc.);
- Outras questões, tais como, confidencialidade, obrigações e responsabilidades operacionais devido à utilização do sistema de intercâmbio electrónico de dados, disposições em matéria de recurso, disposições legais que interditam o uso de códigos, etc.;
- Como introduzir o novo sistema: por meio de acordo (por exemplo: um Acordo de Intercâmbio de Dados, o que levanta outras questões contratuais) ou na base de um estatuto de administração tendo em conta a autoridade de que a administração é investida.

12.4. Assinatura

Apesar da existência de sofisticados sistemas de intercâmbio de dados, o processo de importação/exportação mantêm-se, algumas vezes, embora parcialmente, baseado em papel, devido às exigências legais e operacionais das autoridades aduaneiras nacionais. Em certos sistemas informáticos aduaneiros existentes, as exigências com relação às assinaturas requerem a apresentação às Alfândegas de declarações em cópia impressa juntamente com a informação transmitida electronicamente bloqueando, por conseguinte, o avanço em direcção a um ambiente "sem papel". Tais barreiras legais devem ser ultrapassadas se se pretende beneficiar completamente das vantagens que uma Alfândega informatizada disponibiliza.

Estão disponíveis técnicas eficazes para substituir a assinatura manuscrita num ambiente de informatização das Alfândegas. As palavras-chave, números pessoais de identificação, cartões de identificação, etc. e assinaturas digitais podem ser usadas para autenticar uma mensagem electrónica e identificar a sua origem. Já estão a ser usadas em outros sectores tais como bancário, bem como por um grande número de Alfândegas.

A legislação em matéria de assinatura electrónica pode obedecer a duas lógicas:

- Especificar os meios técnicos a serem utilizados (por exemplo, que algoritmo, como será aplicado, etc.); ou
- Especificar que a escolha de um mecanismo adequado é da responsabilidade das Alfândegas.

A segunda solução tem a vantagem de não requerer nenhuma modificação na legislação se as Alfândegas decidem mudar de um mecanismo para o outro.

12.5. Admissibilidade

Os obstáculos legais ainda existem no que concerne à admissibilidade de dados informatizados legíveis como provas de procedimentos nos tribunais. A Organização Mundial das Alfândegas (OMA) numa resolução aprovada em 1986, apelou às suas administrações membros

para pressionarem as autoridades nacionais competentes de maneira a produzirem as necessárias mudanças legais. Isto não proporcionará apenas a admissibilidade de dados informatizados legíveis como provas nos tribunais, mas também proporcionará a autenticação de tais dados por meios informatizados ao contrário de assinaturas manuscritas (ver parágrafo 12.4 acima). Estas reformas legais são necessárias não apenas a partir do ponto de vista das Alfândegas, mas também do ponto vista dos parceiros comerciais no geral.

Quando uma tal legislação é introduzida ou está em vias de o ser, importa ponderar determinadas etapas para que o sistema informatizado seja capaz de proporcionar material de provas conforme prescrito na matéria.

12.6 Protecção dos dados e protecção da vida privada

À exclusão, em geral, dos sistemas de luta contra a fraude, a legislação em matéria de protecção dos dados e de protecção da vida privada aplica-se habitualmente aos sistemas de TI das Alfândegas. O seu campo de aplicação pode limitar-se aos particulares ou englobar tanto os particulares como as entidades públicas.

Durante a elaboração da legislação sobre a protecção da vida privada ou a protecção dos dados, as Alfândegas devem, na medida do possível, certificar-se que as disposições da referida legislação não hipotequem a capacidade de proteger os interesses do Estado em matéria de receitas, de comércio ou outro, limitando as disposições que permitam conservar informações e trocar informações com outras partes interessadas (a nível nacional ou internacional). A protecção da vida privada torna-se uma questão importante quando as Alfândegas utilizam as redes de comunicação pública, como a Internet e partilham informações sobre os utilizadores com terceiros.

È igualmente do interesse do país em causa que as Alfândegas sejam habilitadas a consultar os sistemas informáticos dos operadores comerciais para proceder às verificações/auditorias necessárias. As Alfândegas devem garantir que a nova legislação não proíba esta prática.

No momento da implementação de uma nova tecnologia de IC, deve-se examinar a legislação em matéria de protecção da vida privada e de protecção dos dados para assegurar que o novo sistema respeite todas as disposições.

Os documentos seguintes contêm dados suplementares relativos às bases jurídicas sobre as quais baseiam-se as trocas sem suporte papel.

(I) Lei-tipo da CNUDCI sobre as assinaturas electrónicas e do Guia para a sua incorporação 2001 [Nações Unidas, 2002]

(II) Convenção das Nações Unidas referente à utilização das comunicações electrónicas nos contratos internacionais [Nações Unidas, 2007]

(III) «Promover a confiança no comércio electrónico: questões jurídicas relativas à utilização internacional dos métodos de autenticação e de assinatura electrónicos" [Nações Unidas, 2007]

13. Auditorias dos controles internos dos sistemas informáticos

(Norme transitoire 6.9)

13.1 Generalidades

A auditoria de um sistema informático garante o bom desenrolar de uma actividade ou de um procedimento determinado. Conforme indica a própria expressão, a auditoria de sistemas consiste no exame do ciclo de tratamento na sua totalidade e não simplesmente as transacções propriamente ditas. Uma auditoria de sistemas não se baseia nem na verificação retrospectiva de um procedimento tangível nem no exame aprofundado da totalidade ou de um número significativo de transacções, ao contrário do que é feito em um sistema manual, para assegurar o bom funcionamento de um aplicativo ou de uma instalação particular. Em contrapartida, uma auditoria visa reforçar a confiança dos utilizadores baseando-se nas características próprias do tratamento informático.

Se puder ficar estabelecido que o procedimento em si é fiável e preciso, e que os dispositivos de controle aos quais responde são eficazes e respeitados, justifica-se concluir que o resultado apresenta a qualidade almejada. A grande vantagem dos sistemas informáticos, que é também, paradoxalmente, o seu ponto fraco, é que uma vez programados, desempenham sistematicamente a mesma tarefa da mesma maneira, até que uma modificação seja introduzida. Assim, se foram programados correctamente, o resultado será sempre exacto, mas no caso contrário, será sempre erróneo!

As Alfândegas podem aplicar as técnicas de auditorias de sistemas ou aos sistemas dos operadores comerciais ou aos seus próprios aplicativos internos. O recurso a essas técnicas permite verificar a integridade dos sistemas e, assim, identificar os pontos fracos que devem ser remediados para restabelecer a confiança.

13.2 Auditorias de concepção

As auditorias dos sistemas informáticos são particularmente úteis no momento da concepção de um aplicativo novo. Tratando-se das Alfândegas, será sempre necessário implementar novos aplicativos o mais rapidamente possível, em virtude da introdução de legislação nova. No entanto, quando a rapidez da implementação foi privilegiada, foi em detrimento da possibilidade de proceder facilmente a auditorias, que foi negligenciada ou considerada somente parcialmente. Uma má adaptação do sistema às auditorias traduz-se em controles inadequados, ou até mesmo inexistentes; o que é prejudicial para a fiabilidade dos dados.

É por isso que a equipa encarregada de planificar a implementação de um aplicativo novo deveria igualmente ter um auditor informático. Este estará em medida de garantir que a questão dos controles e das verificações retrospectivas não seja negligenciada. Poderá igualmente fornecer dados de teste que permitam proceder a testes realistas do sistema. Estará assim depois em medida de confirmar que o tratamento dos dados, desde a sua introdução até ao seu registo definitivo, realiza-se correctamente, e de proceder igualmente a uma verificação retrospectiva das transacções. Assim, se os imperativos em matéria de auditoria são tidos em consideração desde a concepção do sistema, as auditorias e os controles posteriores serão mais eficazes e fiáveis. Igualmente, é mais rentável ordenar o sistema para este efeito desde o início, em vez de tentar fazê-lo posteriormente.

As partes principais de uma auditoria de sistema estão descritas abaixo.

13.3 Planificação

A planificação é determinante para a eficácia e a credibilidade de uma auditoria. Define orientações e especifica o âmbito da auditoria ou objectivo final em função do qual a sua eficácia será apreciada. Tratando-se dos novos sistemas, a planificação é geralmente precedida de um estudo de viabilidade. A questão fundamental à qual a planificação deve permitir responder é a seguinte: é possível?

A planificação permitirá nomeadamente determinar:

- Os objectivos da auditoria; o auditor deve ter uma ideia precisa do objectivo da sua missão. Este objectivo deve igualmente ser do perfeito conhecimento dos funcionários interessados ou dos colaboradores que fazem parte da equipa de concepção.

- o âmbito; define os limites da auditoria especificando as áreas e os sistemas que deverá abranger;

- a existência de riscos; trata-se de definir as áreas onde uma falha teria consequências graves, talvez até, catastróficas, e nas quais o auditor deve concentrar os seus esforços;

- a condução da auditoria e a organização das entrevistas de início e fim de auditoria com os funcionários interessados; estas reuniões permitem fixar antes as regras de base da auditoria e de afastar assim qualquer risco eventual de mal-entendido ou problema durante a própria auditoria; permitem igualmente aos funcionários interessados saber o que podem esperar das conclusões da auditoria;

- a duração da auditoria; o período que levará a auditoria deve ser definido para permitir aos funcionários interessados organizar os seus trabalhos em consequência;

- os recursos necessários para realizar a auditoria; é indispensável definir o número de auditores em função do tamanho do ou dos sistemas a analisar, a sua localização, bem como a disponibilidade dos funcionários directamente interessados;

- o período durante o qual os funcionários directamente interessados estarão disponíveis para as entrevistas; é ainda mais essencial assegurar que os funcionários directamente interessados saibam perfeitamente quando é que auditoria deve realizar-se e quando é que os auditores desejarão encontrar-se com eles. Deve-se portanto, na medida do possível, definir datas com antecedência suficiente.

Enfim, convém os auditores avaliarem a incidência das modificações eventualmente efectuadas ao sistema ou à Administração que o explora, nos conhecimentos adquiridos, após as auditorias anteriores. No que toca aos sistemas existentes, muitas informações recolhidas no decorrer de auditorias anteriores podem provavelmente ajudar a auditor o compreender o sistema e a maneira como funcionou no passado. No entanto, se muitas modificações foram introduzidas, a utilidade dessas informações fica fortemente reduzida.

13.4 Inquérito ou recolha de informações

Existe nessa área um conjunto de métodos, que são essencialmente os seguintes:

13.4.1 Entrevistas

Deve-se, se possível, realizar encontros com os gestores seniores de todos os níveis, tanto os utilizadores dos aplicativos como os informáticos e os que desenvolveram o sistema. Graças a essas entrevistas o auditor poderá determinar:

- A maneira como o funcionamento do sistema é percebida (geralmente pela direcção)
- a maneira como o sistema funciona efectivamente (ponto de vista dos utilizadores)
- a maneira como o sistema é suposto funcionar (caderno de encargos estabelecido pelos desenvolvedores/os utilizadores)

13.4.2 Exame da documentação

Os auditores podem examinar:

- O caderno de encargos dos utilizadores que detalha as tarefas que os utilizadores querem que o sistema desempenhe;
- o descritivo do sistema que especifica a solução proposta pela equipa de desenvolvimento;
- os relatórios de testes, que contêm, entre outras coisas, o leque e o âmbito dos testes a fim de garantir a eficácia de um sistema em qualquer circunstâncias, a sua precisão, a sua solidez e de assegurar que ele disponha da capacidade necessária para fazer face a sobrecargas inesperadas, e enfim, que esteja dotado de dispositivos necessários para detectar e assinalar os erros;
- as conclusões dos testes e das explorações em paralelo: esses relatórios contêm os resultados das explorações em tempo real de um sítio piloto ou em paralelo com um sistema existente;
- os manuais do utilizador: esses manuais devem ser exaustivos e de compreensão fácil ;
- as medidas de socorro/de segurança: essas medidas devem especificar como corrigir as deficiências e a maneira de proteger o sistema tanto a nível dos aplicativos como do material;
- a política de arquivo: esta política deve definir a frequência das cópias de segurança bem como a duração da conservação e o local de armazenagem dessas cópias; neste caso, devem ser armazenadas distante do sítio e num cofre à prova de fogo.

Estes elementos, que não são exaustivos, permitem determinar controles internos ou operacionais, que foram implementados ou que fazem falta. Os auditores podem igualmente tirar muitas conclusões a respeito do estado da documentação (até da sua ausência) relativa ao sistema que pode, por exemplo, estar ultrapassada ou incompleta. O exame da gestão da configuração e dos documentos fornecerá aos auditores outros indícios sobre o bom funcionamento do sistema e sobre a confiança que ele inspira.

13.5 Consignação dos resultados de uma auditoria

Os auditores consignarão as suas conclusões ou em um relatório escrito ou sob a forma de diagramas. Existem numerosas convenções e normas em matéria de estabelecimento dos organigramas, cada uma delas destinando-se geralmente a relatar um aspecto particular. A este respeito, nomeadamente:

- o organigrama de programação
- o organigrama de análise
- os esquemas funcionais
- os esquemas de bases de dados.

Os auditores compararão frequentemente os seus próprios organigramas com o do sistema analisado para detectar qualquer omissão ou anomalia. Os apêndices 5 e 6 contêm exemplos correntes de diagramas desse tipo. Nesta fase da auditoria, e antes de passar para a fase seguinte, a pessoa ou organização objecto da auditoria confirma que o auditor apreendeu correctamente o sistema.

13.6 Avaliação

Ao avaliar os dados recolhidos, o auditor pode começar a determinar os supostos ou reais pontos fracos dos controles internos. Esta parte da sua missão permitirá ao auditor elaborar os testes e determinar as áreas onde estes podem ser aplicados, a fim de apreciar a eficácia dos controles e a fiabilidade do resultado.

13.7 Confirmação das conclusões de uma auditoria

Este procedimento vem concluir cada etapa de uma auditoria. A confirmação pode intervir, por meio de observação, na fase de recolha das informações, ou da avaliação. Podemos proceder por inspecção dos processos, dos relatórios de resultados, etc. até executando novamente o procedimento de tratamento.

O exame da documentação, seja ela gerada por computador ou que se trate de *arquivos* concernentes às transacções realizadas manualmente, deverá confirmar em que medida ela é exaustiva, exacta e fiável. Quando uma verificação retrospectiva for possível, será realizada para assegurar que a cadeia não sofre qualquer interrupção.

Quando for impossível proceder a uma verificação retrospectiva, ou devido à falta de elementos, ou por causa do volume de transacções, as TIC podem trazer soluções, por exemplo a elaboração de programas especiais para examinar os dados registados em suporte magnético. Tais programas podem estar escritos de maneira *ad hoc* na mesma linguagem que a do *software* do aplicativo, podemos igualmente utilizar *softwares* de interrogação de ficheiros de proprietário.

Estes métodos permitem de maneira simples verificar e confirmar que o cômputo das transacções, a liquidação dos direitos, as isenções, etc. podem igualmente servir para testar combinações de dados inabituais, o que seria praticamente impossível com a ajuda de técnicas manuais. Frequentemente, os auditores instalam no sistema um conjunto de programas de teste e de *softwares* de auditoria que podem ser implementados em cada auditoria. Estes *softwares* podem ser modificados, por exemplo alterando alguns parâmetros, mas são apenas realmente úteis quando o sistema permanecer inalterado.

Estes meios aperfeiçoados são essencialmente utilizados quando eventuais erros poderiam ter consequências importantes, por exemplo, comprometer gravemente a arrecadação dos direitos e demais imposições aduaneiras devidos ou alterar as estatísticas, levando assim a problemas na balança dos pagamentos, etc.

13.8 Relatório

No final da auditoria, os auditores endereçarão geralmente à Gestão, um relatório contendo recomendações sobre a maneira como as lacunas podem ser eliminadas e os controles adaptados para torná-los mais eficazes. Controles podem até ser rejeitados se parecerem inadequados em uma situação particular.

As recomendações não são vinculativas mas a sua rejeição eventual é geralmente precedida por um exame aprofundado, porquanto pode, em determinadas circunstâncias, ter consequências desastrosas.

13.9 Verificação após auditoria

Quando um sistema novo foi instalado ou que um sistema existente foi substancialmente alterado, é habitual verificar o seu funcionamento. Esta verificação, realizada após um determinado prazo, visa determinar se o sistema funciona conforme previsto, se apresenta pontos fracos ou se informações podem ser aproveitadas para projectos futuros. De igual modo, quando após a auditoria de um sistema informático, recomendações concretas foram formuladas relativamente ao seu funcionamento, uma verificação pós-auditoria permitirá determinar se essas recomendações foram executadas e de apreciar as repercussões; quando as recomendações não foram implementadas, deve-se determinar a razão.

13.10 Conclusão

Quando um sistema foi registado e avaliado e que as modificações recomendadas para melhorar o controle foram implementadas, podemos legitimamente esperar que esse sistema funcione de maneira fiável até à próxima alteração importante. Convirá proceder a auditorias periódicas que deverão confirmar que a situação permanece inalterada e que os controles que foram incorporados no sistema continuam a ser implementados e respeitados.

14. Problemas Correntes

14.1. Introdução

Antes de implementar um sistema informático seja lá qual for, convém examinar as áreas susceptíveis de causar problemas durante a execução do projecto e definir estratégias que garantam que os problemas eventuais, sejam eles específicos da organização administrativa, dos procedimentos ou dos recursos, não levem ao fracasso do projecto.

Deve-se prever um apoio quando um sistema informático é instalado em uma Administração Aduaneira. As Administrações que pretendam informatizar-se desejarão igualmente implementar um serviço para apoiar as medidas que tomam. Todas as actividades e os custos atinentes imputáveis à gestão das actividades ligadas às tecnologias da informação, a concepção, o desenvolvimento e a utilização de sistemas informáticos novos ou melhorados e a exploração, a manutenção e o apoio a esses sistemas são de grande importância e devem ser tidos em conta (ver o Apêndice 8: Quadro recapitulativo dos trabalhos sucessivos a empreender).

14.2. Resistência cultural

Os funcionários aduaneiros podem recear que a informática ameace os seus empregos e oferecer resistência à sua introdução. As Administrações Aduaneiras podem eliminar essas resistências e tornar os seus funcionários mais produtivos organizando programas de formação e de incitação. Podem igualmente combater os boatos e acalmar as incertezas assegurando que as informações necessárias concernentes aos planos, ao âmbito, etc. do projecto estejam acessíveis a todos, e desde o início do projecto. A este propósito, uma solução consiste na publicação, em intervalos regulares, de relatórios relativos ao projecto e na organização de reuniões com as pessoas afectadas directamente.

14.3. Informatização dos dados de base

Se os dados de base não forem informatizados, o interesse que apresenta a informatização para alguns parceiros das Alfândegas fica reduzido. Por exemplo, quando os documentos comerciais não são comunicados por via electrónica, as empresas não podem utilizá-los para elaborar as suas declarações aduaneiras. Uma solução consiste em encarregar gabinetes especializados de introduzir os dados. Esses gabinetes especializados podem ser geridos, ou pelas Alfândegas, ou por empresas privadas. Neste último caso, o gabinete especializado deve ser supervisionado pelas Alfândegas para garantir que as normas em matéria de introdução de dados satisfazem os critérios na matéria. Outra solução consiste em adquirir material que as empresas e as Alfândegas precisam por intermédio de programas de crédito aos fornecedores, o que permitiria eventualmente obter reduções substanciais.

14.4. Ausência de infra-estrutura adequada

Outro problema que pode hipotecar a informatização é a ausência de infra-estruturas de telecomunicação adequadas. Neste caso, os dados podem ser trocados por meio de disquetes em vez de redes públicas. Deve-se igualmente examinar a possibilidade de utilizar a comunicação por satélite. Pode igualmente ser difícil para algumas Administrações ter acesso a uma fonte ininterrupta de abastecimento de electricidade. Quando os sistemas informáticos devem estar disponíveis em permanência, deve-se inscrever a compra de um gerador de electricidade no orçamento do projecto.

14.5. Legislação aduaneira

As alterações muito frequentes da legislação aduaneira podem igualmente impedir a informatização global das Alfândegas no âmbito de um único projecto. Em vez de informatizar a totalidade de um sistema que se tornará rapidamente obsoleto, é preferível adoptar uma abordagem modular informatizando as diversas actividades e inserindo-as em um sistema central, segundo as necessidades ou a permanência da legislação. Podemos citar por exemplo o sistema de pagamento e de arrecadação dos direitos, ao qual outros sistemas poderiam ser acrescidos posteriormente. Recursos podem igualmente ser dedicadas à racionalização dos procedimentos manuais em vigor a fim de eliminar qualquer sobreposição no sistema.

14.6. Limitação dos recursos e das competências

Quando os recursos estão limitados, importa definir as prioridades do projecto em função dos ganhos de produtividade e de eficácia, de maneira a fazer o melhor aproveitamento possível dos valores investidos. Por exemplo, uma Administração pode pensar em informatizar em primeiro lugar o procedimento mais oneroso do ponto de vista da mão-de-obra a fim de melhorar a sua produtividade. Uma Administração Aduaneira não pode possuir as competências necessárias para implementar um projecto. Quando a solução que consiste na contratação de especialistas externos é ponderada, importa planificar correctamente os custos e, talvez sobretudo, definir expressamente o papel do ou dos consultores.

_____vvv_____

Apêndice 1 - Estruturas de Informação e de Telecomunicações para o Comércio Eletrónico

Sobre o comércio eletrónico (E-commerce)

O que é o comércio eletrónico? Para os fins desta parte, o comércio electrónico é definido como o “processo que consiste na troca de informações por via electrónica para facilitar o comércio de bens e serviços. Um componente essencial deste processo é a integração de procedimentos do comércio com tecnologias apropriadas".

O termo "comércio electrónico" começou a ser usado há relativamente pouco tempo e, segundo muitos, é uma nova maneira de efectuar transacções. No entanto, muitas administrações, incluindo as Alfândegas, já usam aspectos do "comércio electrónico" nos seus métodos de trabalho actuais. Os parceiros comerciais trocam geralmente informações por via electrónica por meio de EDI, correio electrónico, fax etc. O "comércio electrónico" consiste essencialmente para efectuar transacções por via electrónica. Poderia ser definido formalmente como "um meio de efectuar as transacções usando as técnicas das telecomunicações e da informática para a troca de dados entre os sistemas de informação automatizados independentes".

O comércio eletrónico abarca certos EDI, mas também vai mais além, pois inclui todas as outras tecnologias existentes que podem ser usadas para transmitir as informações de um parceiro comercial para outro. É importante lembrar que as informações consistem em dados estruturados (usando formatos padronizados de mensagens, transferência directa de registos de uma base de dados, dos códigos de barras), de imagens (imagem e textos não estruturados) e de sons (correio de voz, etc.). As administrações aduaneiras devem agora considerar o impacto que podem ter essas outras técnicas nas suas operações. Em particular, precisam determinar se o uso dessas técnicas pode fornecer soluções mais rentáveis, que lhes permita oferecer serviços mais flexíveis às empresas e outras administrações públicas com as quais elas podem precisar trocar informações.

O comércio electrónico já está bem implementado na Alfândega. As administrações utilizam amplamente as técnicas de EDI para fins de desembaraço aduaneiro de mercadorias para importação e exportação. A comunicação em larga escala de informações de natureza comercial e de dados constam nas declarações de mercadorias entre empresas e Alfândegas, também se prestam à aplicação de técnicas de EDI. Esta aplicação do comércio electrónico aumentará, sem dúvida, na próxima década. No entanto, à medida que o papel da Alfândega se expande e surgem novas maneiras de realizar tarefas tradicionais, será cada vez mais necessário explorar outras possibilidades oferecidas pelo uso do comércio electrónico no sentido mais amplo.

O termo "comércio electrónico" é usado como uma expressão genérica que descreve várias relações electrónicas, que apresentam todas as suas regras e características próprias. Entre as muitas configurações possíveis, importa mencionar as relações empresas-consumidores (B2C), relações empresas-empresas (B2B) e os três tipos de relacionamento envolvendo o governo, a saber, governo-empresas (G2B), governo-cidadãos (G2C). e governo-governo (G2G).

Canais de acesso electrónico

O diagrama abaixo (Apêndice 1- Estruturas de Telecomunicações e de Informação para o Comércio Electrónico) fornece um resumo das diferentes rotas de acesso que podem ser fornecidas ao usuário dos serviços oferecidos pela alfândega no contexto do comércio electrónico.2

Normas de troca de informações

Normas de troca de informações no Modelo de Dados da OMA – foca-se no significado semântico de alto nível dos dados e sobre o modo de proceder à interacção entre o governo e as empresas. Existem três níveis de abstracção no que concerne um modelo de dados, que pode ser externo, físico e conceptual. O Modelo de Dados da OMA concentra-se no nível mais alto de abstracção, o nível conceptual do modelo de dados.

O Modelo de Dados da OMA como um Modelo de Dados Conceptual

Os modelos menos abstractos, chamados modelos externos, descrevem as operações específicas de uma declaração de mercadorias, bem como o relatório de um manifesto. Os exemplos mais representativos são a mensagem CUSCAR em conformidade com a versão 3 do MD da OMA e a mensagem GOVCBR em conformidade com a versão 3.0 do Modelo de Dados da OMA.

Os modelos físicos são mais gerais porque descrevem um conjunto ou categoria de exemplos, mas ainda apreende ainda a tecnologia na qual os exemplos foram implementados. O Guia de Implementação de Mensagens (GIM) é um exemplo representativo da implementação de uma mensagem CUSCAR incluída na versão 1.1 do Modelo de Dados da OMA, publicada em novembro de 2003.

Os modelos conceptuais suprimem a tecnologia de implementação para enfatizar os conceitos e significados que definem determinadas categorias de documentos. O nível mais alto de abstracção foi recentemente integrado na versão 2.0 do Modelo de Dados da OMA. Os exemplos mais representativos são os diagramas de categoria UML para todos os tipos de documentos, os diagramas da categoria UML para uma única categoria de documentos e o inventário de 450 elementos de dados colectivamente chamados de conjuntos de dados MDD.

Necessidade do modelo conceptual

Como a maioria dos círculos comerciais, os círculos aduaneiros não evoluem ao mesmo ritmo que a tecnologia. Se o Modelo de Dados da OMA for unicamente descrito como uma tecnologia específica (ou seja, através de um modelo de dados físicos como o EDIFACT), será necessário definir o Modelo de Dados em cada tecnologia futura. De qualquer forma, será difícil, se não impossível, garantir que todos os modelos de dados físicos sejam análogos em diferentes tecnologias.

Ao estabelecer um modelo conceptual e ao inserir todas as regras comerciais no modelo conceptual, a comunidade comercial poderá implementar os documentos aduaneiros, independentemente da tecnologia usada (ou seja, modelos de dados físicos) que atenda às suas necessidades.

Outros benefícios do estabelecimento de um modelo conceptual

Poderia ganhar em clareza porque o significado e as regras de apresentação de um elemento de dados são preservados em diferentes modelos físicos que são derivados de um único modelo conceptual. Por exemplo, a categoria “TransportEquipment” designa os “recursos materiais necessários para conter ou reter a(s) remessa(s) a serem transportada(s)” e possui os mesmos atributos de categoria, independentemente da categoria usada ser uma declaração de entrada, uma declaração de saída, uma declaração de frete à saída, uma declaração de frete à entrada, uma declaração de transporte ou uma declaração de trânsito.

A interoperabilidade com os modelos de dados de outras administrações ou de administrações nacionais participantes e de empresas é facilitada quando cada elemento das informações tem um significado único em todos os documentos aduaneiros. Por exemplo, o termo "Equipamento de transporte", da ONU / CEFACT que aparece no campo do transporte, pode ser directamente associado à categoria "Equipamento de transporte" do Modelo de Dados da OMA.

Na versão 3.0, os benefícios do desenvolvimento de um modelo conceptual são visíveis. Desde a publicação da versão 3.3, o Modelo de Dados da OMA, divide-se em duas partes:

1) Os componentes padronizados (o conjunto de dados, os modelos de informações, os modelos de procedimentos operacionais e as listas de códigos) e

2) Os arquivos de informação (Directivas de implementação de mensagens e Esquemas XML que traduzem os modelos de troca electrónica de dados adaptados às necessidades das actividades).

Um “Arquivo de Informação” indica como os componentes padronizados do Modelo de Dados da OMA foram reagrupados e são usados para responder às necessidades de uma determinada actividade. Os arquivos de informação contêm principalmente os modelos para a troca de dados electrónicos, mas também podem ser usados para explicar o significado operacional das informações estruturadas usadas na troca de informações. Os arquivos de informação foram anteriormente designados por "Mensagens Electrónicas". Esses modelos são de tipos diferentes e referem-se, em particular, a declarações específicas de regulamentos transfronteiriços (importação, exportação, relatório de carregamento de importação, relatório de carregamento de exportação, declaração de trânsito, etc.), de respostas governo-empresas e de trocas governo-governo.

Além disso, as licenças, as autorizações, os certificados e outros tipos de "janela única" foram incorporados na Versão 3.3.

Podemos considerar que os arquivos de Informação do Modelo de Dados possuem uma estrutura hierárquica. Os arquivos de Informação de base da OMA compreendem os principais padrões transaccionais num ambiente de janela única, e em particular:

- As mensagens empresa-governo tais como IM (declaração de importação de mercadorias), EX (declaração de exportação de mercadorias), CRI (relatório de carregamento de importação), CRE (relatório de carregamento de exportação), CONV (Relatório sobre o meio de transporte), informações prévias sobre TRT (Trânsito), etc;

- As mensagens governo-empresas tais como as mensagens de notificação de desalfandegamento ou do estado da Declaração;

- ❖ As mensagens entre todas as partes relativas às licenças, os certificados, as permissões e outros tipos de autorização;

- ❖ As mensagens governo-governo relativas à gestão da garantia para os fins das admissões temporárias e de outros tipos de trocas.

Os arquivos de informações básicas contêm o máximo de dados necessários num determinado contexto de utilização. A partir desses arquivos, o EPMD trabalhou no contexto do seu trabalho de suporte à implementação, para desenvolver formatos comummente usados, formatos que denominou "Arquivos derivados de informações da OMA" Normalmente, essas " Arquivos derivados de informações" são baseados em modelos electrónicos padronizados aplicados internacionalmente como, por exemplo, os formulários electrónicos FAL da Organização Marítima Internacional (OMI), o Documento Administrativo Único da EU (DAU), as Licenças electrónicas CITES, a Declaração de Valor da OMC, a Gestão da Garantia no contexto da Caderneta TIR, etc.

Os Membros e as outras organizações que já estão usando o Modelo de Dados para troca real de dados ou que estão em processo de implementação podem ir ainda mais longe na "personalização" local e desenvolver um arquivo chamado "Meu Arquivo de Informação ". Este arquivo, que contém informações muito específicas, tem como objetivo descrever como cada componente do Modelo de Dados da OMA foi adotado e usado nos contextos operacionais específicos de uma determinada implementação. Pode ser mais facilmente elaborado a partir de um “arquivo derivado de informação” semelhante. Por exemplo, um Membro que utiliza um formulário de declaração aduaneira baseado no “Documento administrativo único” pode elaborar o documento intitulado “Meu arquivo de informação” a partir do arquivo derivado de informações publicado pela OMA. Da mesma forma, um Membro pode elaborar um "Meu arquivo de informação" cobrindo os requisitos nacionais aplicáveis ao relatório de carregamento.

Esse arquivo permite explicar como os requisitos nacionais estão vinculados aos formulários FAL da OMI, bem como ao modelo de dados da OMA.

O desenvolvimento de um pacote chamado "Meu Arquivo de Informação" seria da responsabilidade dos Membros e das organizações que usam o Modelo de Dados da OMA. O EPMD está trabalhando para determinar como um uso nacional da OMA pode ser representado num modelo XML padrão da OMA, que pode ser "lido por uma máquina". Um tal modelo possibilitaria, não apenas, elaborar uma tabela comparativa do uso nacional dos vários elementos do conjunto de dados da OMA mas, também, copiar automaticamente os dados de um arquivo "Meu arquivo de informação" para as ferramentas de um fornecedor de soluções, facilitando, assim, uma introdução mais rápida de soluções concretas para troca de dados.

Troca de informações: um cenário em mudança

Nos cenários anteriores de EDI, essas informações são fornecidas à Alfândega por meio de normas internacionais de mensagens, tais como:

- ❖ CUSDEC: mensagem aduaneira EDIFACT/ONU relativa à declaração aduaneira;

- ❖ CUSCAR: mensagem aduaneira EDIFACT/ONU relativa à carga;

- ❖ CUSREP: mensagem aduaneira EDIFACT/ONU relativa ao meio de transporte;

- ❖ CUSRES: mensagem aduaneira EDIFACT/ONU relativa à resposta da Alfândega; e

- ❖ CUSEXP: Mensagem alfandegária EDIFACT/ONU relativa às remessas expresso.

Atualmente, existem em matéria de EDI, várias outras mensagens internacionais EDIFACT/ONU que podem ser usadas para os fins acima. A título de exemplo, pode-se citar o CUSDEC e o GESMES (estatísticas), o PAXLST (lista dos membros da tripulação/dos viajantes) e o SANCRT (diversos requisitos para as licenças e os certificados).

Até a presente data, o Modelo de Dados da OMA inclui uma mensagem EDIFACT GOVCBR, cobrindo a maioria dos dados exigidos pelos órgãos responsáveis pela regulamentação dos fluxos transfronteiriços. Uma administração poderia, assim, usar a mensagem GOVCBR para responder a todos os requisitos associados às mensagens, em vez de manter actualizadas várias mensagens EDIFACT.

Modelos de transacção:

A troca de informações com os operadores comerciais passa pelo recurso a diferentes modelos de transacção (com base na taxinomia ebXML). Estes modelos são os seguintes:

i) Fazer uma oferta - Aceitar uma oferta:

[Exemplo: a Alfândega aceita um operador comercial na sua aplicação da Internet, oferecendo-lhe um caderno de encargos. O operador comercial aceita esse caderno de encargos.

ii) Solicitar uma informação – Fornecer uma informação. [Exemplo: o operador comercial solicita informações sobre os impostos e taxas associados a um artigo que deseja importar. A Alfândega fornece as informações solicitadas.]

iii) Solicitar uma confirmação - Receber uma resposta de confirmação (ou uma recusa). [Exemplo 1: o operador comercial envia uma declaração para o desalfandegamento das mercadorias. A Alfândega confirma ou invalida o desalfandegamento das mercadorias. Exemplo 2: A empresa envia uma caução e solicita a confirmação do registo da referida caução. A Alfândega regista a caução e transmite a confirmação.]

iv) Formular um pedido - Receber uma resposta. [Exemplo: a Alfândega formula ao operador comercial um pedido de precisão relativo à natureza do produto importado e recebe uma resposta.]

v) Entregar uma notificação a um operador comercial. [A Alfândega envia ao operador comercial uma notificação sobre o estado de sua conta fiscal.]

vi) Fornecer informações personalizadas aos operadores comerciais [A Alfândega informa todos os operadores comerciais sobre o estado das suas respectivas mercadorias.]

Graças à Internet e às técnicas do comércio electrónico, e seguindo os modelos de transacção descritos acima, é fácil permitir às empresas que tenham acesso apenas ao seu domínio nas bases de dados da Alfândega. Estas informações podem ser fornecidas graças à técnica de publicação das bases de dados. Em geral, informações as seguintes podem ser consultadas:

- Base de dados em que nas empresas estão inseridas (saldo das garantias em curso, nome e detalhes de contacto da parte interessada)

- Mensagens administrativas (informações relativas a alterações do sistema, às actualizações, etc.);

- ❖ Situação das mercadorias que são objecto da declaração do parceiro comercial (desalfandegamento acordado, mercadorias retidas para verificação, solicitação de informações complementares);

- ❖ Taxa de direitos anti-dumping / direitos compensatórios;

- ❖ Estatísticas em matéria de erro;

- ❖ Taxa de câmbio;

- ❖ Base de dados sobre tarifas (nomenclatura e informações relativas às listas de tarifas harmonizadas);

- ❖ Contingentes;

- ❖ Códigos de região / distrito / departamento de Alfândega;

- ❖ Códigos de país;

- ❖ Códigos das estâncias aduaneiras no estrangeiro

- ❖ Montante e situação no que respeita ao reembolso

- ❖ Multas e sanções impostas pela Alfândega (pagas por um determinado período)

- ❖ Informações tarifárias vinculativas (para mercadorias importadas ou exportadas).

Contudo, antes que essas informações sejam disponibilizadas, várias questões precisam ser resolvidas, por exemplo, no que respeita aos direitos de autor, à confidencialidade, à protecção de dados e ao eventual pagamento de taxas.

No que diz respeito às informações disponibilizadas aos usuários, a questão dos direitos de autor é particularmente importante, principalmente no que diz respeito a documentos como as listas tarifárias harmonizadas. Cada administração membro terá que examinar se tem o direito de publicar listas tarifárias actualizadas. As Alfândegas também devem garantir que estejam autorizadas a publicar as informações fornecidas por outras administrações. A Internet permitirá estabelecer uma ligação entre o site da Alfândega e o de outros sectores públicos.

A questão da cobrança ou a cobrança de taxas pela disponibilização de determinadas informações também deverá ser examinada. Por exemplo, a maioria das administrações nacionais solicita à comunidade empresarial uma contribuição financeira para dispor suas listas tarifárias e actualizações relacionadas. Num universo informatizado, as administrações terão que determinar se uma determinada taxa deve ser solicitada. Antes de distribuir gratuitamente as informações, a Alfândega deve ter em conta a sua origem e determinar se o seu proprietário as distribui, habitualmente, mediante pagamento.

A questão da confidencialidade e proteção de dados deve ser tratada adequadamente, permitindo o acesso às bases de dados da Alfândega. Os dados pessoais e os dados comerciais enviados à Alfândega a título confidencial estão sujeitos às disposições da legislação nacional sobre a confidencialidade e a protecção de dados.

A eficiência do controle das mercadorias e dos viajantes também pode, igualmente, ser melhorada, autorizando as Alfândegas a acederem às bases de dados dos operadores comerciais. Por exemplo, quando a Alfândega pode consultar a base de dados dos viajantes de uma companhia aérea, é mais capaz de determinar quais são os viajantes que devem ser submetidos a controle de triagem na sua chegada. Da mesma forma, consultando a base de dados de um transportador, a Alfândega pode determinar as remessas de alto risco.

Códigos

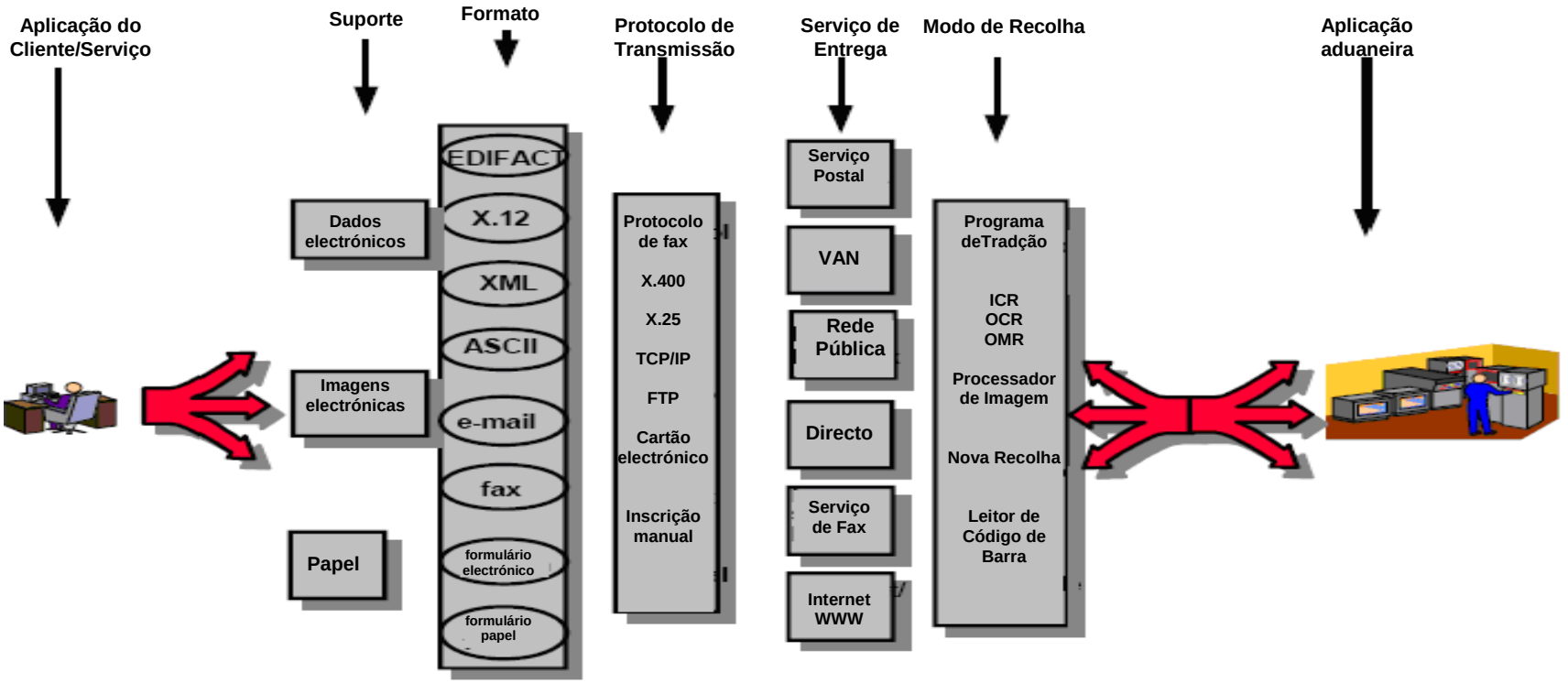
(Padrões 3.11 e 7.2)

Ao trocar informações, os códigos e os identificadores desempenham um papel muito importante. A OMA recomenda o uso de códigos internacionais, como códigos de países e de moeda ISO, os códigos de transporte da ONU, o Sistema Harmonizado de Designação e Codificação de Mercadorias da OMA, etc. (ver apêndice 9). O uso de códigos internacionais existentes garante a abertura e acessibilidade dos sistemas aduaneiros. O uso harmonizado de códigos ao nível das aplicações contribuirá significativamente para facilitar o comércio internacional. Isso contribuirá para simplificar o desenvolvimento dos sistemas das empresas e das outras administrações que desejem comunicar-se com a Alfândega. Também tornará mais vantajosa a troca de informações entre administrações aduaneiras.

Recomendações

As Alfândegas precisarão estabelecer os mecanismos necessários em matéria de consulta com a comunidade empresarial, bem como as capacidades indispensáveis de infra-estrutura operacional, de recursos humanos e de infra-estrutura dos sistemas de informação necessária para usar eficazmente o comércio electrónico. Em primeiro lugar, a administração aduaneira precisará conhecer com precisão as suas capacidades internas, bem como as expectativas das partes externas, o que exige uma consulta nos vários serviços da administração e com as partes externas que participarão, eventualmente, do comércio electrónico com a administração. Em segundo lugar, depois de considerar as repercussões sobre o plano jurídico e político, a administração aduaneira deverá definir a sua estratégia em matéria de comércio electrónico e elaborar um plano de implementação que será aprovado pelos quadros superiores e pelas partes externas envolvidas. Por fim, as Alfândegas devem esforçar-se por alinhar os seus requisitos com o Modelo de Dados da OMA e desenvolver a nível nacional os arquivos intitulados "Meu Arquivo de Informação", fornecendo a transparência necessária para reduzir os custos das actividades comerciais.

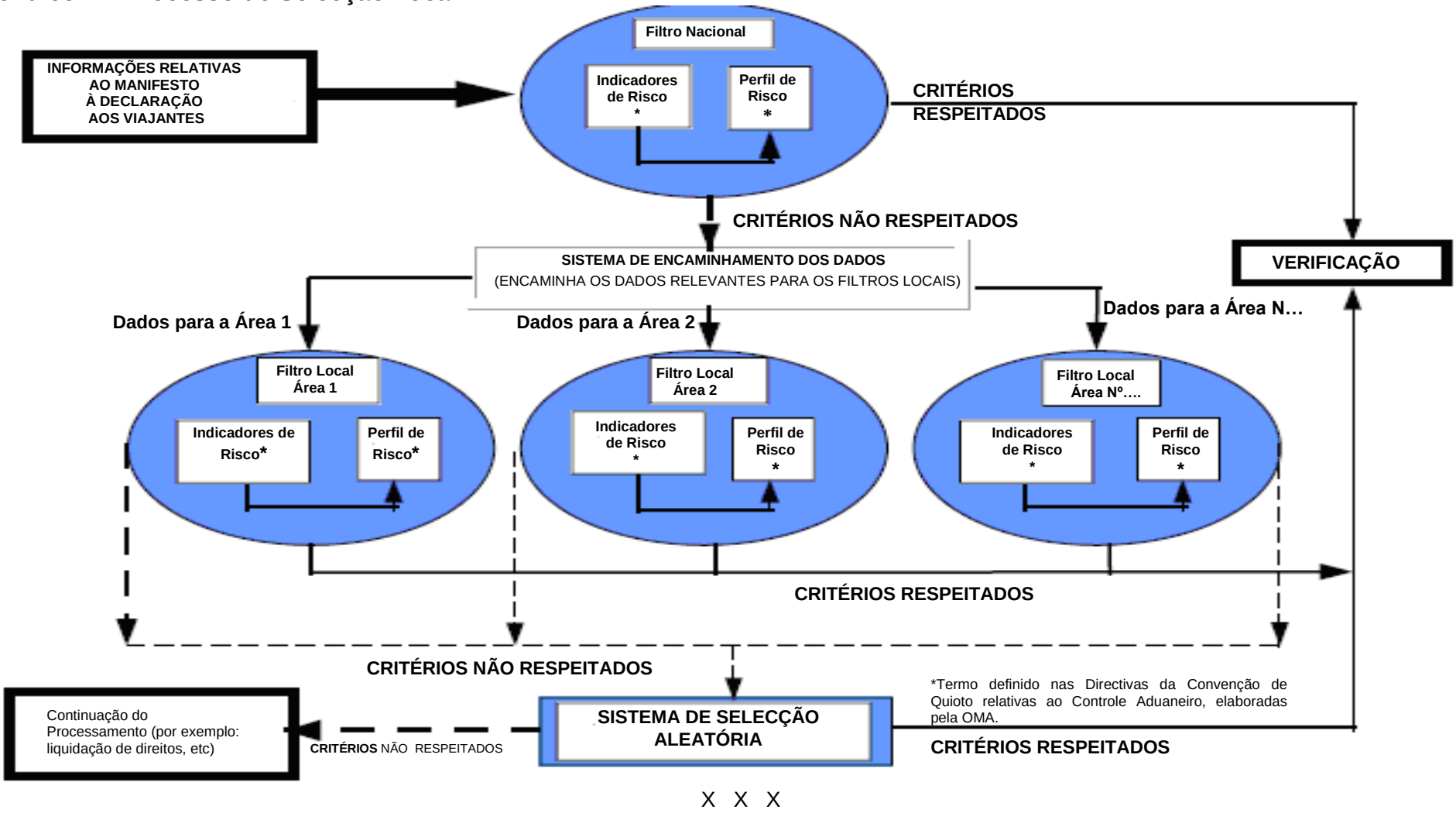
Apêndice 1 – Estruturas de Telecomunicações e de Informação para o Comércio Electrónico



Baseado no livro da Receita do Canadá intitulado: "Operações de Comércio Electrónico nas Alfândegas - Análise Preliminar" (Dezembro 1994)

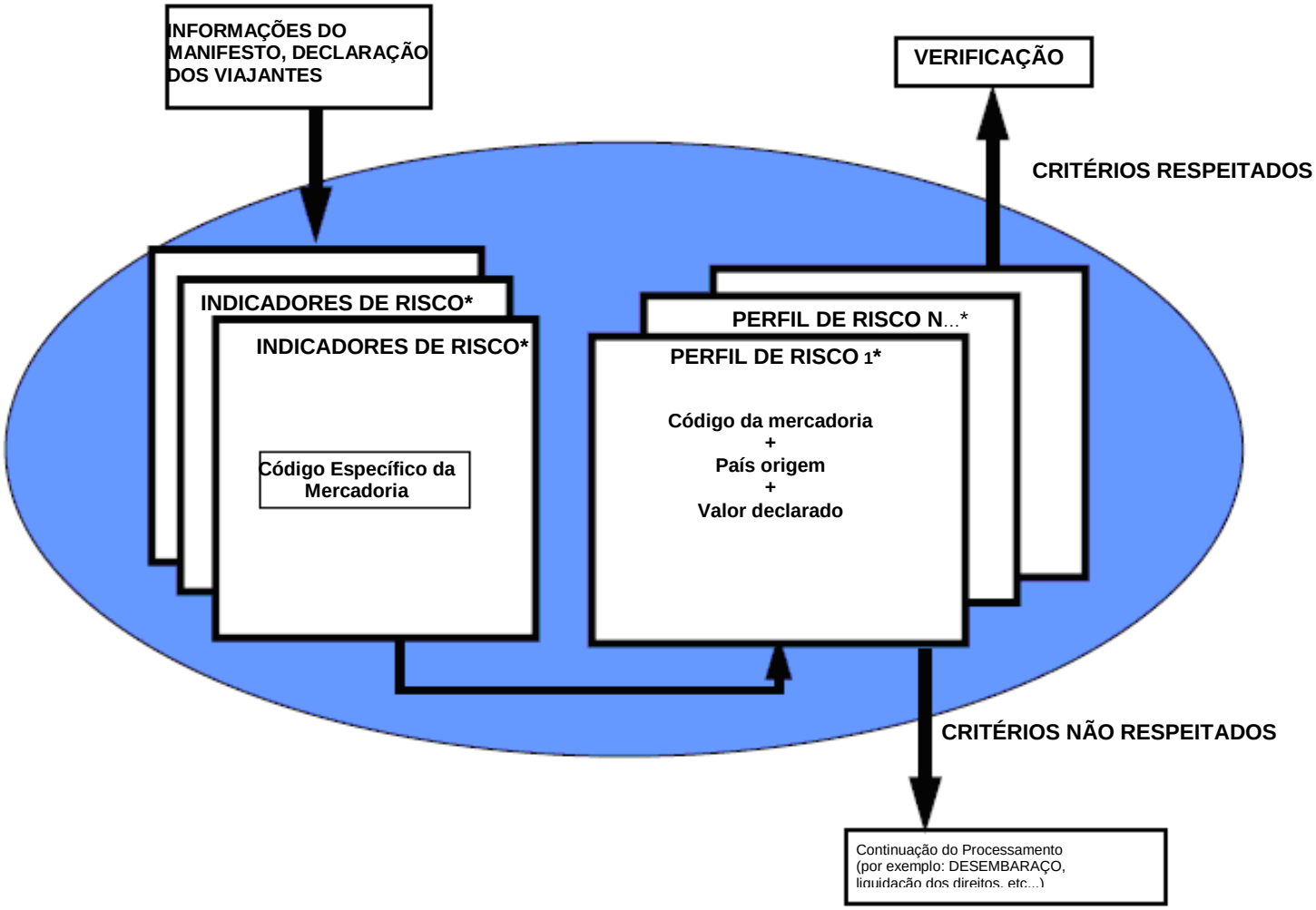
X X X

Apêndice 2 – Processo de Selecção Local



X X X

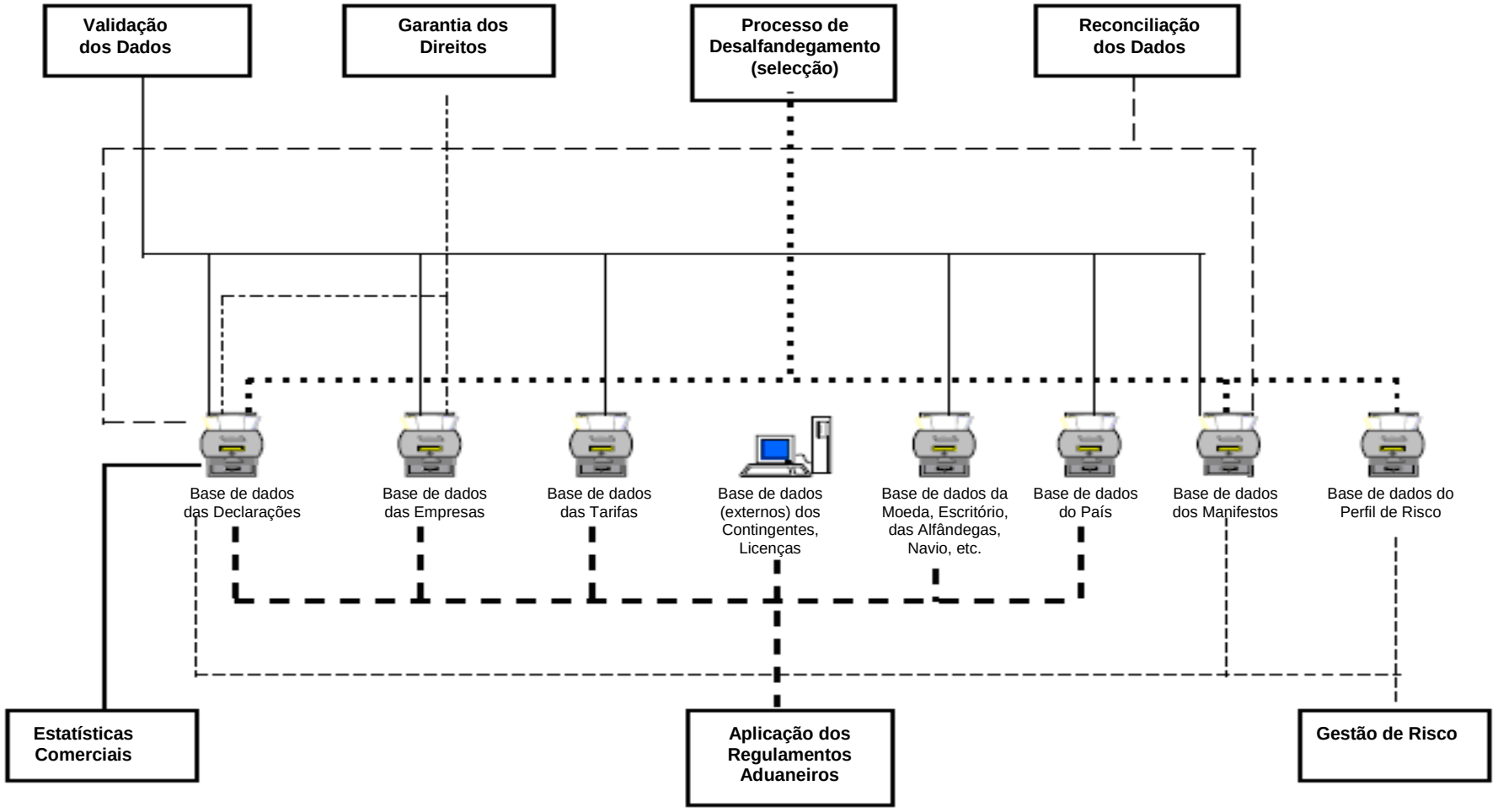
Apêndice 3 – Sistema de Filtro do Perfil de Selecção



* Termo definido nas Directivas da Convenção de Quioto relativas ao Controle Aduaneiro, elaboradas pela OMA.

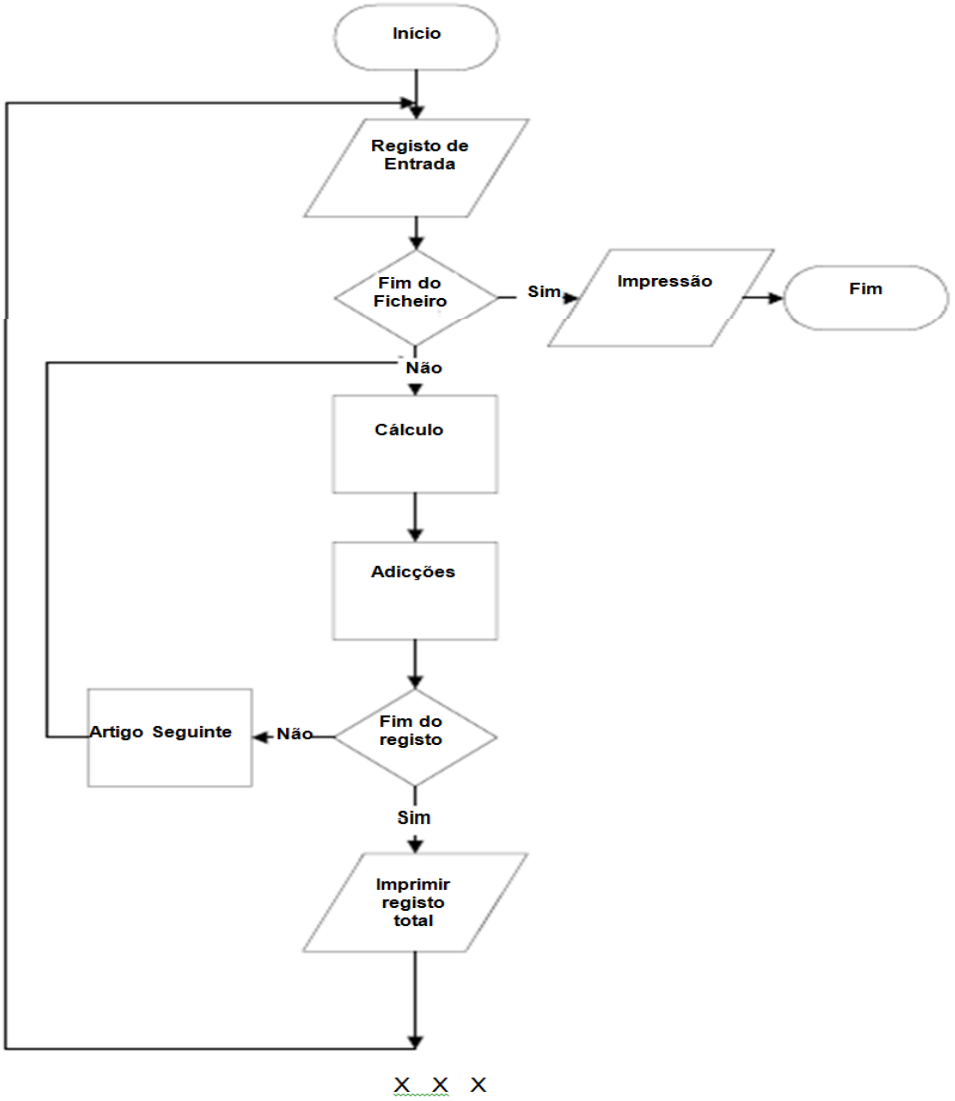
X X X

Apêndice 4 – Modelo de Procedimentos Aduaneiros e de Acesso aos Arquivos



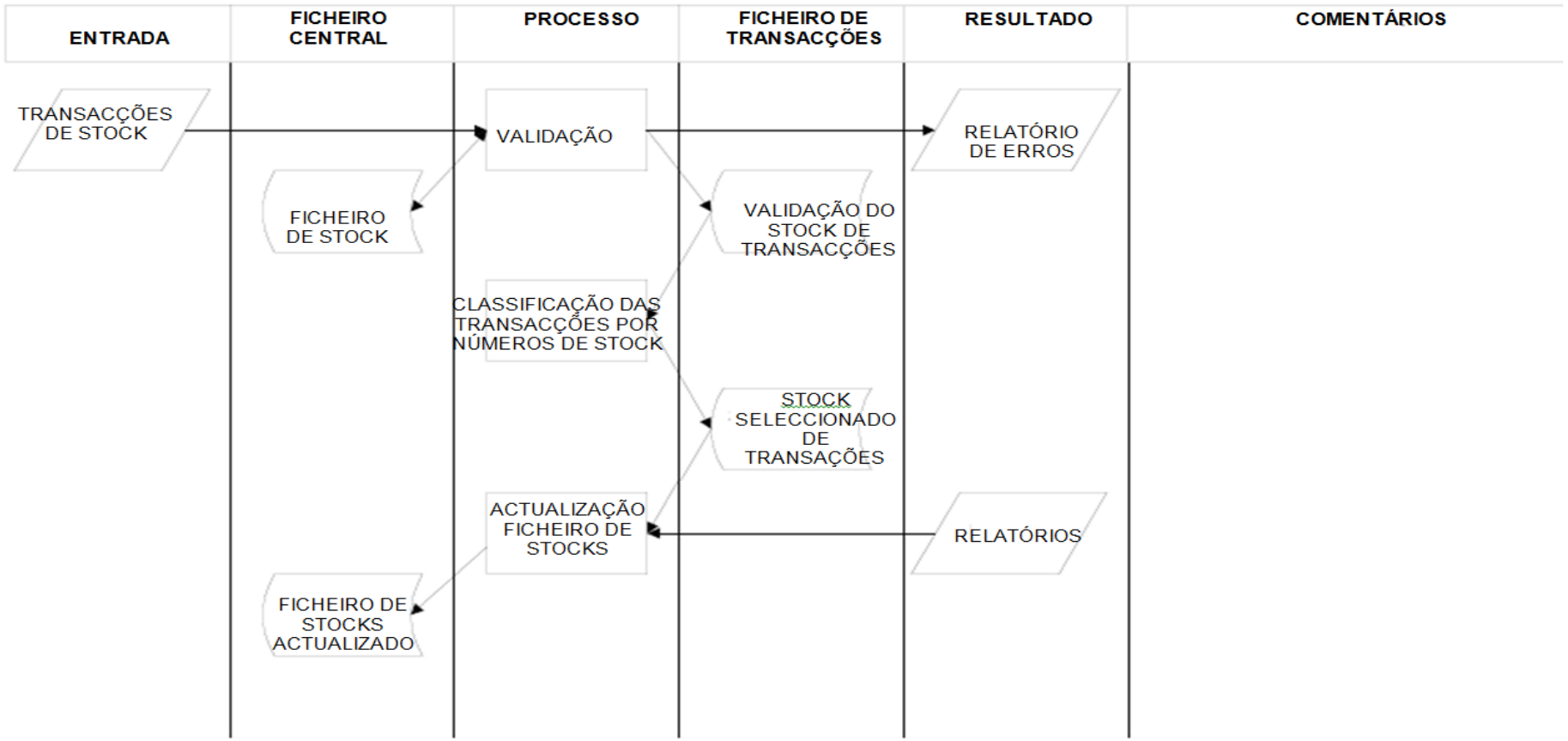
X X X

Apêndice 5 – Fluxograma do Programa



X X X

Apêndice 6 – Diagrama de Processamento por Computador



X X X

Apêndice 7 – Glossário dos Termos e Abreviaturas

ADO	Ver “Arquitectura de documentos abertos”
Aplicação	Programa ou conjunto de programas elaborados para uma actividade específica do utilizador.
Arquitectura de Documentos Abertos	Arquitectura tem como objectivo proceder a “trocas cegas” de informação. Isto significa que dois sistemas podem intercambiar documentos, manter a sua estrutura e revisibilidade sem qualquer prévio conhecimento, desde que ambos sistemas suportem um específico perfil padronizado do padrão ODA internacional. A ODA oferece uma arquitectura que pode lidar com a maioria dos documentos que provavelmente podem ser encontrados no ambiente de escritório.
Assinatura digital	Propriedade particular de um utilizador ou processo que é usado para assinatura de mensagens através de uma ligação de comunicação.
Autenticação	Para a segurança de dados, controlos que previnem ou detectam a alteração e/ou destruição acidental de dados, incluindo a identidade do remetente e do receptor de mensagens.
Base de dados	Conjunto de dados interrelacionados armazenados para que possam ser acedidos por utilizadores autorizados através de procedimentos de diálogo simples e amigáveis
Biometria	Biometrias são métodos automatizados de reconhecimento de uma pessoa baseada nas características fisiológicas (www.biometrics.org)
Caixa de correio electrónico (Electronic mailbox)	Local para armazenar pacotes de mensagens em pontos intermediários antes da transmissão. As mensagens recebidas são armazenadas na caixa de correio do destinatário e recuperados mais tarde pelo mesmo.
Captura de dados	Acto de inserir dados por meio de dispositivos periféricos, por exemplo: um teclado.
Codificação	Transformação reversível de dados (chamado “plaintext”) em uma forma (chamada “cipher text”) que cancela o significado original dos dados para prevenir que vos mesmos sejam conhecidos ou usados. (www.techweb.com/encyclopedia) (http://www.sans.org/resources/glossary.php)

Comércio Electrónico (*e-commerce*)	Meio de efectuar transacções através das tecnologias de telecomunicações para a troca de dados entre sistemas computorizados de informação autónomos.
Contra-medidas	Acção tomada para contrapor um perigo, uma ameaça, etc.
Controlador de comunicações	Unidade electrónica que proporciona funções de interface orientadas em linhas, por exemplo: detecção de erros, sincronização, entre um grupo de modems e um computador ou processador de rede de comunicação.
Cookie	Símbolos colocados no computador do utilizador que podem ser usados para reconhecer a máquina do utilizador. (www.techweb.com/encyclopedia)
CPS	Certificado Prático de Declaração
Criptografia	Conversão de dados em um código secreto para transmissão através de uma rede pública. (www.techweb.com/encyclopedia)
Diagrama Bloco	Diagrama de um sistema no qual as partes principais são representadas por figuras geométricas anotadas adequadamente para indicar a função de componentes e as suas inter-relacções.
Documento	Qualquer meio (incluindo fitas magnéticas e discos, microfilmes e mensagens de comércio electrónico) destinado a transportar um registo dos dados das declarações.
DTI	Ver **Introdução directa de dados pelas empresas**
EC	Ver Comércio Electrónico
EDI	Ver Intercâmbio Electrónico de Dados
EFT	Ver Transferência Electrónica de Fundos
Especificações do Utilizador	Informação formal identificando, em detalhes, toadas as necessidades especificadas pelo utilizador de sistema informático sob desenvolvimento.
Esquema de base de dados	Mapa de toda a estrutura lógica de uma base de dados.

Estudo de viabilidade	Fase de implementação de um sistema na qual o sistema proposto é avaliado em função de considerações de ordem técnica e financeira. É usado como base para decidir se prossegue-se para a fase seguinte.
Fluxograma	Representação gráfica de um processo (lógica ou física).
Fonte dos Dados	Factura, formulário, recibo ou uma outra forma escrita de evidências de uma transação da qual a informação básica é extraída para processamento.
Formulários electrónicos	Documento no qual certos itens são pré-codificados e no qual são inseridas várias informações.
GUI	Ver Interface Gráfico do Utilizador
Hardware	Equipamento físico, como por exemplo disk-drive, PC ou impressora.
HTML	Ver HyperText Markup Language ou Linguagem de Programação Baseada em marcas.
Hyper Text Markup Language	A linguagem usada para criar páginas na Web. As páginas são escritas em texto normal e depois são aplicadas as marcas HTML ao formato do texto para mostrá-lo com o software browser WWW. AS marcas incluem opções de formatação, ligações às páginas, gráficos. HTML é independente da máquina.
ICP	ICP (Infra-estrutura de Chave Pública) é um sistema automatizado que gere a produção, manutenção, codificação e de chaves de assinaturas digitais. Ambos tipos de chaves, a codificação e a assinatura digital, possuem duas componentes relacionadas: uma componente chave pública que é acessível a todos os utilizadores e uma componente chave privada cujo acesso por outros deve ser protegido. A chave pública e a outra informação de identificação são armazenadas em um certificado digital que é digitalmente assinado pela Autoridade de Certificação (AC). A assinatura digital da AC no certificado digital confirma a identidade da entidade final, bem como a sua chave pública. Isto também garante que a chave pública não foi falsificada.
IETF	Internet Engineering Task Force (http:/www.ietf.org/)
Integridade	Protecção de programas contra a perda ou corrupção, a fim de conservar a sua integridade para poderem entrar em fase de exploração.
Intercâmbio de Informação	No contexto da presente directiva é o intercâmbio electrónico de informação entre sistemas

	informáticos.
Intercâmbio Electrónico de Dados	Transmissão de dados estruturados de acordo com os padrões de mensagens acordados, entre um sistema informático e um outro, por meio electrónico.
Interface Gráfico do Utilizador (GUI)	Interface do programa que utiliza as capacidades gráficas do computador para tornar o programa mais fácil. As interfaces gráficas bem desenhadas podem liberar o utilizador de conhecer comandos de linguagens complexas. Por outro lado, muitos utilizadores acham que trabalham de forma mais efectiva com interface de comandos dirigidos, particularmente se já conhecem a linguagem do comando. A Microsoft Windows é um interface gráfico (GUI).
Interface informática	Partilha de limites entre duas unidades relacionadas entre si.
Internet	Rede internacional de computadores que conecta os computadores de estabelecimentos de ensino, administrações públicas, empresas, etc.
Introdução directa de dados pelas empresas	Sistema no qual os dados das declarações são introduzidos no sistema informático das Alfândegas pelos próprios declarantes, a partir dos terminais normalmente situados nos seus próprios escritórios ou via redes comerciais de terceiras partes.
ISO	International Organization for Standardization ou Organização Internacional de Padronização. (www.iso.org)
Linha comutada	Linha de telecomunicações para comunicação de computador para computador que requer ao remetente digitar fisicamente o número de telefone antes de poder ser iniciada a comunicação entre dois sistemas.
Linha especializada (alugada-dedicada)	Linha alugada por um subscritor para o seu uso permanente ou exclusivo.
Modem	MOdulador/DEModulador – dispositivo que modula o sinal transmitido e desmodula o sinal recebido, por exemplo, um modulo é usado para converter um sinal digital de computador num sinal analógico, normalmente através de uma rede telefónica.
Não rejeição	Possibilidade de impedir o expedidor ou o destinatário de uma mensagem de negar tê-la enviado ou recebido.
Norma Internacional	Norma reconhecida oficialmente em todo o mundo por um organismo internacional de padronização

	reconhecido (ISO, UNECE etc.).
ODA	Ver Arquitectura Aberta de Documentos
On-line	Sistema no qual os dados ou instruções são inseridas directamente a partir do ponto de origem e o resultado dos dados é transmitido directamente para o beneficiário apropriado.
Organigrama	Representação gráfica de um processo (lógico ou físico).
PIN	Número de Identificação Pessoal.
Processador central	Unidade contendo os circuitos que controlam e realizam a execução de instruções.
Processadores de dados	Alguém que executa operações sobre os dados para alcançar um objectivo desejado.
Protocolo	Um conjunto de convenções formalmente especificado que regem o formato e o controlo de *inputs* e *outputs* entre dois sistemas de comunicação.
Rede de comunicação	Instalações interligadas de comunicação de sistemas.
Rede de Telecomunicações	Ver Rede de Comunicação.
Rede de valor ajustado	Serviço de comunicação que transmite dados através das redes de empresas de telecomunicações e oferece serviços adicionais de processamento de dados fornecidos por equipamento próprio. Esses serviços incluem armazenamento temporário e comunicação de mensagens, o estabelecimento de interfaces entre terminais e centros de servidores.
Secure Sockets Layer	Secure Sockets Layer é um protocolo desenvolvido para a transmissão de documentos particulares via Internet.
SIG	Ver **Sistema de Informação da Gestão**
Sistema de Gestão da Informação	Sistema concebido para fornecer algumas vezes em tempo real, ao pessoal da supervisão e da gestão os dados relevantes e necessários, de forma correcta e tempestiva.
SMIME	Secure Multipurpose Internet Mail Extension ou Extensão de Mail Seguro de Multiuso via Internet. (www.ietf.org/html.charters/smime-charter.html)
SMTP	Simple Mail Transport Protocol ou Protocolo de Transporte de Mail Simples

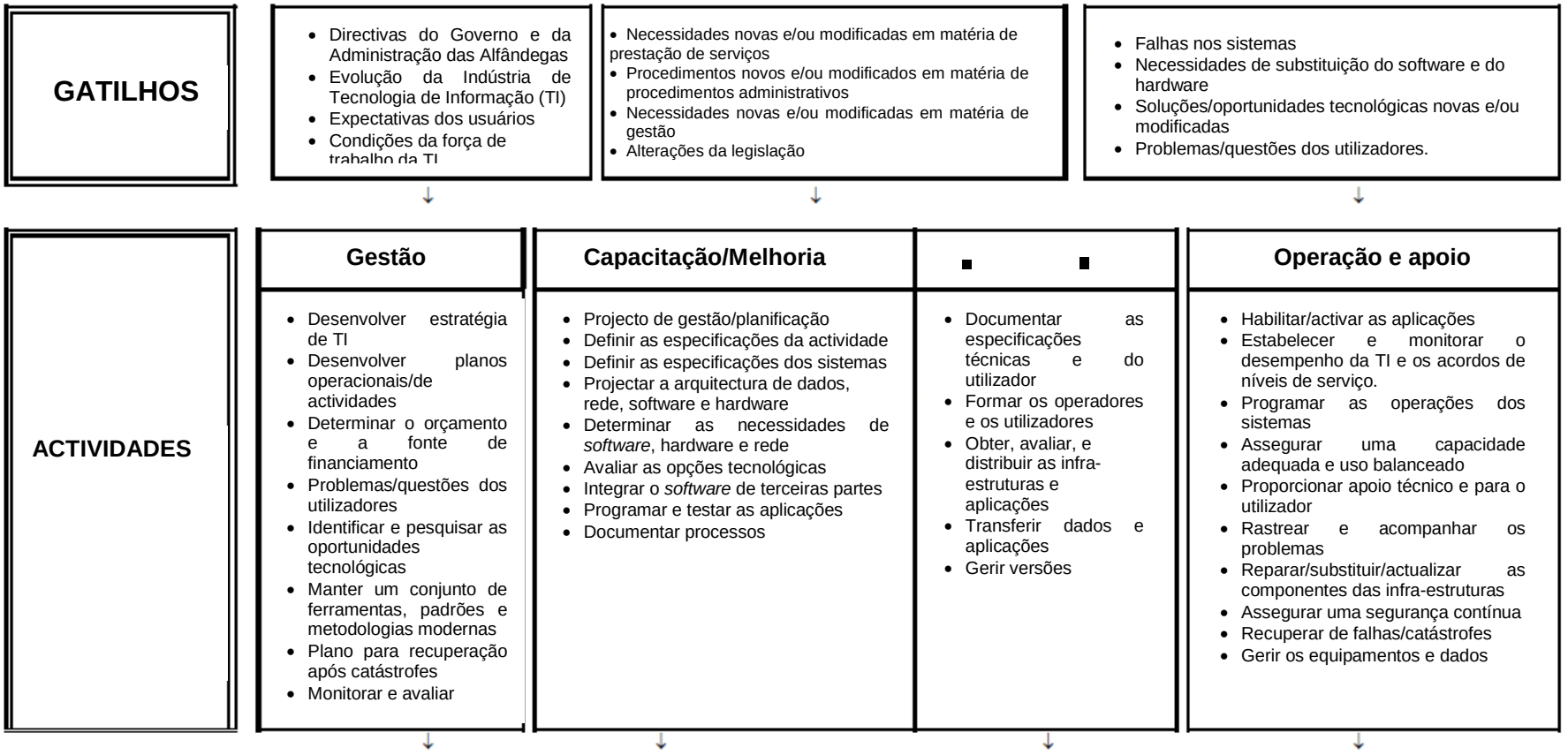
	(http://www.techweb.com/encyclopedia)
Software	Programas, procedimentos, rotinas e possivelmente documentos associados com a operação de um sistema de processamento de dados.
SSL	Secure Socket Layer. Protocolo desenvolvido para transmitir documentos particulares via Internet
Tecnologia de Comunicação e de Informação	Combinação de informatização e telecomunicação baseada em micro-electrónica que permite gerir, recolher, tratar, armazenar e difundir informação sob a forma de voz, número ou texto.
TI	Ver **Tecnologia de Comunicação e de Informação**
TIC	Ver **Tecnologia de Comunicação e de Informação.**
TLS	Protocolo que garante a privacidade entre aplicações de comunicação e seus utilizadores na Internet. (http://www.sans.org/resources/glossary.php)
Tradutor EDI	Dispositivo que converte Informação do formato EDI acordado, a fim de permitir enviar e receber informação num formato de uma aplicação
Transferência Electrónica de Fundos	Sistema automatizado para transferência de fundos de uma conta bancária para uma outra usando equipamento electrónico e comunicação de dados. Exemplos: dinheiro electrónico, cartão de débito, cartão de crédito, pagamento de contas electronicamente (EBPV) (www.ebilling.org).
Transferência Electrónica de Fundos **Segurança/protocolos/sistemas**	Protocolo Seguro –Socket Layer (http://home.netscape.com/eng/ssl3/ssl-toc.html) Transacção Electrónica Segura (www.setco.com) ou (www.setco.org) Pagamento Electrónico (www.I-Pay.com) Micro pagamento (www.w3.org/Ecommerce/Micropayments/#About) Sistema de portefólio eletrónico aberto (www.PCSCworkgroup.com)
Transport Layer Security	Ver TLS
Trojan Codes	Código malicioso escondido no interior de uma peça legítima de software.

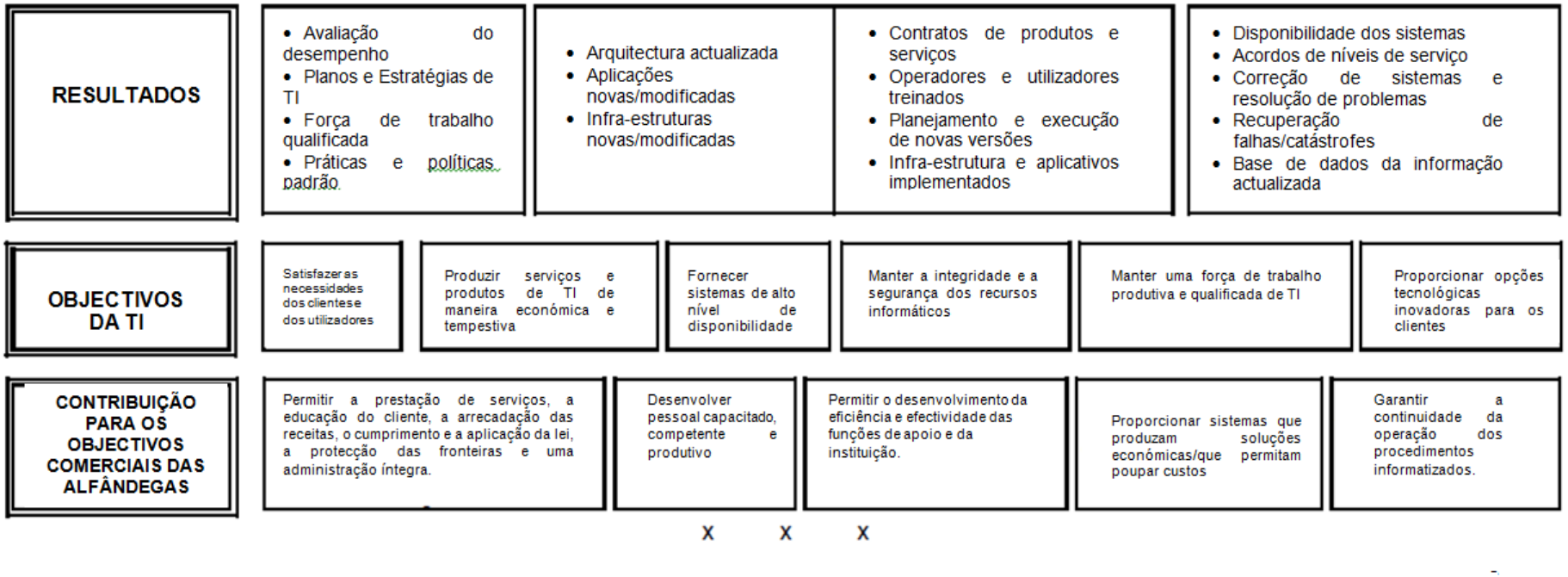
Turn-Key System	Sistema completo de hardware e software distribuído ao consumidor pronto para operar. Isto normalmente inclui a instalação, o ajuste e o teste (técnico) do sistema pelo fornecedor. Apenas “gire a chave” e siga.
UN/EDIFACT	Intercâmbio Electrónico de Dados para a Administração, Comércio e Transporte/Nações Unidas
UNCITRAL	Comissão das Nações Unidas sobre a Legislação do Comércio Internacional
Value-Added Network ou Rede Adicionada	Serviço de comunicação usando redes comuns de transporte de comunicação, para transmissão e fornecimento de serviços de dados adicionados com equipamento adicional separado. Os serviços adicionados podem incluir a transferência e o armazenamento de mensagens.
VAN	Ver Rede Adicionada
VDU	Ver Unidade de Apresentação Visual
Virtual Shop	Loja que pode não existir na realidade mas criada por software para parecer que existe
Visual Display Unit	Dispositivo que permite ao utilizador digitar informação num computador através do teclado, caneta óptica, *touch-screen* (tela transparente sensível ao toque) e visualizar, na tela de tubos de raios catódicos, a informação produzida, o texto ou os gráficos.
World Wide Web	Camada gráfica aplicada acima da Internet. Enquanto o padrão da Internet é unicamente texto, a Web é gráfica por natureza. Os Textos e os gráficos, armazenados nos servidores, são transmitidos através da rede de computadores para os browsers do cliente onde são mostrados.
WWW	Ver “World Wide Web” ou Web/W3/Teia de Alcance Mundial
X.21	Protocolo de interface de uso geral entre o equipamento do terminal de dados e o equipamento do circuito de dados para operação sincrónica em redes públicas de computadores.
X.25	Protocolo de interface entre o terminal de dados e o circuito de dados, para os terminais que operam em modo de pacotes de redes públicas de dados.
X.400	Normas para gestão de mensagens.

X.509	Certificado (ver ICP) usado para verificar a informação intercambiada através de uma rede informática (por exemplo, a Internet). Contem a chave pública do titular da chave e alguma informação de identificação que confirma que o titular da chave e o emissor do certificado são quem ambos dizem ser. Os certificados são armazenados em directórios acessíveis publicamente, como os directórios X500.
XML	Extensible Markup Language ou Linguagem de Marcas Extensivel

X X X

Apêndice 8 – Diagrama lógico de função de tecnologia de informação




RESULTADOS
• Avaliação do desempenho
• Planos e Estratégias de TI
• Força de trabalho qualificada
• Práticas e políticas padrão
• Arquitectura actualizada
• Aplicações novas/modificadas
• Infra-estruturas novas/modificadas
• Contratos de produtos e serviços
• Operadores e utilizadores treinados
• Planejamento e execução de novas versões
• Infra-estrutura e aplicativos implementados
• Disponibilidade dos sistemas
• Acordos de níveis de serviço
• Correção de sistemas e resolução de problemas
• Recuperação de falhas/catástrofes
• Base de dados da informação actualizada
OBJECTIVOS DA TI
Satisfazer as necessidades dos clientes e dos utilizadores
Produzir serviços e produtos de TI de maneira económica e tempestiva
Fornecer sistemas de alto nível de disponibilidade
Manter a integridade e a segurança dos recursos informáticos
Manter uma força de trabalho produtiva e qualificada de TI
Proporcionar opções tecnológicas inovadoras para os clientes
CONTRIBUIÇÃO PARA OS OBJECTIVOS COMERCIAIS DAS ALFÂNDEGAS
Permitir a prestação de serviços, a educação do cliente, a arrecadação das receitas, o cumprimento e a aplicação da lei, a protecção das fronteiras e uma administração íntegra.
Desenvolver pessoal capacitado, competente e produtivo
Permitir o desenvolvimento da eficiência e efectividade das funções de apoio e da instituição.
Proporcionar sistemas que produzam soluções económicas/que permitam poupar custos
Garantir a continuidade da operação dos procedimentos informatizados.
X
X
X

Apêndice 9 – Recomendações da OMA sobre Tecnologia de Informação

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA[3] CONCERNENTE À REFERÊNCIA ÚNICA DA CONSIGNAÇÃO (UCR) PARA FINS ADUANEIROS

(30 de Junho de 2001)

O CONSELHO DE COOPERAÇÃO ADUANEIRA,

CONSIDERANDO a globalização do comércio internacional.

DESEJANDO contribuir para a facilitação da circulação internacional de mercadorias através das Alfândegas.

DESEJANDO aumentar a eficácia e eficiência das Administrações aduaneiras no tratamento das transacções comerciais internacionais.

RECONHECENDO a importância crescente para a cooperação aduaneira internacional em garantir o melhor cumprimento dos regulamentos aduaneiros e a facilitação do comércio legítimo.

RECOMENDA que os membros do Conselho e das Organizações das Nações Unidas ou as suas agências especializadas, e as Uniões Aduaneiras ou Económicas, devem adoptar e implementar um Número de Referência Única da Consignação (UCR) em estreita colaboração com os seus órgãos de comércio, o qual deve ser:

- usado para todas as transacções comerciais internacionais;
- usado apenas como uma chave de acesso para auditoria, rastreio da consignação, propósitos de reconciliação e informação, e não deve ser fonte de qualquer informação sobre a própria consignação;
- capaz de unicamente identificar uma consignação a nível nacional e internacional;
- aplicado ao nível da consignação, com a consignação sendo definida como “o número total de itens especificados no contracto de venda entre o vendedor e o comprador;
- emitido o mais cedo possível no processo de transacção internacional pelo “vendedor”;
- um número de referência para uso das Alfândegas e pode ser exigido para ser reportado às Alfândegas a qualquer momento durante um procedimento aduaneiro.

RECOMENDA TAMBÉM que a Referência Única da consignação seja estruturado como se segue:

- ter um máximo de 35 caracteres alfanuméricos em extensão longitudinal;

- o primeiro carácter é reservado para identificar o ano dentro de um período de dez anos, e ter valores de 0 a 9 (é considerado que isto dará singularidade à

[3] Estabelecido em 1952 como Conselho de Cooperação Aduaneira (CCA), doravante denominado Conselho

referência da consignação durante tempo suficiente para ir ao encontro de exigências legais para armazenamento de dados para auditoria);

- os próximos dois caracteres são reservados para o código do país ISO 2-alfa e ser o identificador do local do vendedor (é considerado que isto dará singularidade à referência da consignação geograficamente a nível do país);

- deve usar os remanescentes 32 caracteres para conter um identificador nacional da empresa reconhecido oficialmente e uma referência da empresa aplicada internamente.

SOLICITA aos membros do Conselho e das Organizações das nações Unidas ou das agências especializadas, e as Uniões Aduaneiras e Económicas que aceitam esta Recomendação, que notifiquem o Secretário Geral do Conselho a data a partir da qual aplicarão a Recomendação e as condições da sua aplicação. O Secretário-Geral transmitirá esta informação às Administrações aduaneiras de todos os membros do Conselho. Ele transmitirá também às Administrações aduaneiras dos membros da Organização das Nações Unidas ou suas agências especializadas e às Uniões Aduaneiras ou Económicas que aceitaram esta Recomendação.

SOLICITA AINDA ao Secretário-Geral que trabalhe com as organizações internacionais relevantes, como a Comissão Económica das Nações Unidas para a Europa, para garantir que esta Recomendação seja reflectida nos seus respectivos instrumentos e recomendações.

X X X

Apêndice 10 – Recomendações da OMA sobre o uso de websites pelas Alfândegas

CONSELHO DE
COOPERAÇÃO ADUANEIRA TC2-3855

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA CONCERNENTE AO USO DA WORLD WIDE WEBSITES (REDE DE ALCANCE MUNDIAL) POR PARTE DAS ALFÂNDEGAS

(26 de Junho de 1999)

O CONSELHO DE COOPERAÇÃO DAS ALFÂNDEGAS,

DESEJANDO facilitar a movimentação internacional de mercadorias e pessoas através das Alfândegas,

DESEJANDO facilitar o acesso a, bem como a disseminação de, informação reguladora das Alfândegas de domínio público, particularmente, para os viajantes e participantes no comércio internacional,

CONSIDERANDO a importância de tornar disponível para o público informação reguladora relevante das Alfândegas, de forma facilmente acessível e económica,

RECONHECENDO, a aceitação comum da Internet e da World Wide Web (WWW) como meios de comunicação e de disseminação da informação,

RECONHECENDO, o uso crescente da Internet e da WWW pelas Alfândegas,

RECOMENDA que os membros do Conselho e membros da Organização das Nações Unidas ou as suas agências especializadas, e as Uniões Aduaneiras ou Económicas, criem um website para as suas Alfândegas,

RECOMENDA AINDA que os membros do Conselho e os membros da Organização das Nações Unidas ou as suas agências especializadas, e as Uniões Aduaneiras ou Económicas disponibilizem nos websites das Alfândegas, os dados conforme o conteúdo especificado no Anexo a esta Recomendação,

CONVIDA os membros do Conselho e aos da Organização das Nações Unidas ou as suas agências especializadas, e às Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação que notifiquem o Secretariado Geral do Conselho a data a partir da qual irão aplicar a Recomendação, bem como as condições da sua aplicação. O Secretário-geral transmitirá esta informação às alfândegas dos membros da Organização das Nações Unidas ou às suas agências especializadas, como também às Uniões Aduaneiras ou Económicas que aceitaram esta Recomendação.

* *

Anexo à Recomendação sobre os Websites das Alfândegas
Informações fundamentais a ser disponibilizada nos Websites das Alfândegas

Informações destinadas aos viajantes

- Resumo geral sobre as Alfândegas.
- Informações detalhadas sobre franquias de bagagem.
- Informações detalhadas sobre mercadorias proibidas para importação e exportação.
- Informação sobre os Canais das Alfândegas (sistema de canal duplo).
- Penalizações por transgressões aduaneiras.
- Contactos (incluindo endereço de e-mail) para outras informações.
- Ligações com outros sites relevantes, particularmente da Imigração e da Agricultura.
- Versões da informação em várias línguas.
- Acesso às publicações oficiais.

Informações detalhadas sobre franquias de bagagem

Os detalhes sobre franquias de bagagem devem cobrir todos os produtos, incluindo as quantidades e os valores máximos. As condições nas quais são dadas isenções de impostos devem ser cobertas, como por exemplo, a origem da viajem, o período da estadia, a idade do viajante, etc. Em alguns casos, particularmente onde dizem respeito as zonas económicas, estão disponíveis diferentes permissões dependendo de onde a viagem teve origem, devendo as referidas diferenças estar devidamente indicadas.

Informações detalhadas sobre mercadorias proibidas para importação e exportação

As mercadorias que são proibidas ou restritas devem ser devidamente identificadas, por exemplo: armas e munições, animais vivos, certos tipos de plantas, marfim, dinheiro, etc. As penalizações por violações da legislação devem também ser realçadas.

Informação sobre os canais das Alfândegas (sistema de canal duplo)

Deve ser apresentada informação sobre como o sistema de canal duplo funciona e como os passageiros à chegada declaram as mercadorias nas Alfândegas. Isto deve incluir exemplos de formulários aduaneiros a serem completados.

Penalizações por transgressão dos regulamentos aduaneiros

Um conjunto detalhado de informações deve ser fornecido, indicando quais as penalizações que um viajante deve esperar receber se apanhado deliberadamente a transgredir a lei.

Contactos (incluindo endereço de e-mail) para outras informações

A informação para os viajantes sobre os contactos das Alfândegas, particularmente um endereço de e-mail público, deve ser fornecida para permitir ao público fazer perguntas específicas.

Ligações com outros sites relevantes, particularmente da Imigração e da Agricultura

As ligações com outros websites do Governo, tais como o da Imigração, do Turismo e da Agricultura devem, sempre que possível, ser estabelecidas para auxiliar os visitantes a obter informação completa sobre todos os procedimentos necessários, exigidos na chegada ao país.

Informações disponíveis em várias línguas

O turismo é uma parte muito importante da economia de muitos países. Números significativos de visitantes podem não falar a língua nativa do país que estão a visitar. As alfândegas devem ter disponível informação para os viajantes em várias outras línguas.

Acesso a publicações oficiais

O acesso a várias publicações oficiais, brochuras, etc. deve estar disponível para *download* ou pedido por meio do website. Deve ser dada atenção ao formato usado para os documentos que são disponibilizados para *download*.

Informações destinadas aos operadores comerciantes

- Resumo geral sobre as Alfândegas.
- Resumo dos procedimentos aduaneiros e da legislação.
- Legislação nacional incluindo normas aduaneiras de todos os procedimentos das Alfândegas.
- Informação sobre os direitos e pauta.
- Taxas de câmbio.
- Detalhes das proibições e restrições.
- Detalhes sobre como completar uma declaração aduaneira.
- Decisões sobre classificação.
- Penalizações por transgressões aduaneiras.
- Contactos para informação (incluindo endereço de e-mail).
- Ligações com outras agências do governo.
- Acesso a publicações oficiais.

Resumo dos procedimentos aduaneiros e legislação aduaneira

Esta secção proporcionará um resumo geral dos vários procedimentos e legislação aduaneira sob os quais as alfândegas operam. Deve ser considerada como uma introdução ampla às actividades aduaneiras. Devem ser estabelecidas ligações para explicações mais detalhadas sobre procedimentos específicos ou secções da legislação nacional.

Legislação nacional incluindo regulamentações aduaneiras aplicáveis a todos os procedimentos das Alfândegas

A colocação na WWW de textos da legislação nacional cobrindo o comércio internacional (importações, exportações, trânsito, etc.) é uma necessidade básica de um website das Alfândegas. Contudo, em muitos casos a legislação está em texto simples sem quaisquer ligações de hipertexto. Para tornar isto mais útil aos importadores, as administrações aduaneiras devem estabelecer, onde possível, ligações de hipertexto com referências importantes em toda a estrutura dos documentos.

Mecanismos de busca[4] devem também estar disponíveis no website para permitir a condução de buscas de palavra-chave.

Informação sobre os direitos e tarifas

Informação básica sobre pautas e taxas de impostos para várias classes de mercadorias deve estar disponível. Acesso a uma versão electrónica completa da pauta nacional seria mais vantajoso. Todavia, no mínimo uma cópia da versão impressa da pauta deve estar disponível em um formato "pdf" (formato de documento portátil). Isto permitirá ao interessado efectuar o *download* do documento somente para consulta e impressão.

Taxas de câmbio

Uma lista das taxas oficiais de câmbio da moeda para propósitos aduaneiros deve ser um elemento básico a ser incluído no website.

Detalhes das proibições e restrições

Detalhes das mercadorias proibidas ou restritas, mercadorias cobertas por quota e proibições ou restrições similares devem ser realçados. As condições especiais para importação ou exportação de tais mercadorias devem estar claramente indicadas.

Detalhes sobre como completar uma declaração aduaneira

Um guia do utilizador sobre como completar uma declaração aduaneira é útil para os operadores e melhora a qualidade dos dados inseridos nos sistemas aduaneiros. Grande parte das administrações aduaneiras já possui este tipo de guia num formato de papel. As administrações aduaneiras devem converter este guia num formato que pode ser colocado na web, e tal "guia de formação" deve ser desenvolvido num programa completamente interactivo.

Decisões sobre classificação

Frequentemente, os operadores necessitam de informação sobre as questões de classificação. Por conseguinte, todas decisões oficiais sobre classificação devem estar disponíveis no website, reduzindo assim a necessidade de contactar directamente os funcionários das Alfândegas para informação.

Penalizações por transgressão dos regulamentos aduaneiros

Um conjunto detalhado de informações deve ser fornecido, indicando quais as penalizações que um operador pode esperar receber se apanhado a transgredir a lei deliberadamente.

Contactos (incluindo endereço de e-mail) para outras informações

À semelhança da informação para os viajantes devem ser fornecidos detalhes dos contactos (incluindo endereço de e-mail) dos funcionários aduaneiros que lidam com questões específicas.

Ligações com outras agências do governo

Ligações com outros websites do governo, como por exemplo, o Ministério do Comércio e o das Finanças e da Câmara do Comércio de Indústria devem ser incluídas.

[4] Software usado para realizar pesquisas de palavras-chave em documentos num site.

Acesso a publicações oficiais

O acesso a várias publicações oficiais, brochuras, etc. deve estar disponíveis para "*downloading"* ou "*ordering"* através do website. Deve ser prestada consideração ao formato usado para os documentos que são disponibilizados para "*downloading"*.

Desenvolvimento das aplicações de informática na web

A informação a ser disponibilizada para os operadores e viajantes pode tornar-se estática, isto é, os leitores podem receber a informação e imprimi-la, mas geralmente não podem integrá-la nas suas próprias aplicações. As administrações aduaneiras devem desenvolver aplicações interactivas que podem ser usadas quer por clientes externos quer por funcionários internos.

X

X X

Apêndice 11 – Recomendações da OMA sobre o Guia de Transferência de Dados da OMA

CONSELHO DE
COOPERAÇÃO ADUANEIRA TC2-3845

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA[5]
CONCERNENTE AO USO DO GUIA DE TRANSFERÊNCIA DE DADOS DA OMA PARA AS MESSAGENS EDIFACT/ALFÂNDEGAS DAS NU
(21 de Junho de 1995)

O CONSELHO DE COOPERAÇÃO DAS ALFÂNDEGAS,

DESEJANDO facilitar o intercâmbio da informação entre as Administrações aduaneiras e entre as administrações aduaneiras e os operadores utilizadores,

CONSIDERANDO que as mensagens EDIFACT/NU podem ser usadas independentemente da área de aplicação e que o seu uso generalizado no comércio internacional facilitará imensamente a movimentação da carga,

CONSIDERANDO TAMBÉM, que é desejável que um conjunto de normas internacionalmente acordadas e universalmente aplicáveis para o uso de mensagens EDIFACT/Alfândegas das NU seja aplicado no Intercâmbio Electrónico de Dados.

RECOMENDA que os membros do Conselho de Cooperação Aduaneira e todos os membros da Organização das Nações Unidas ou suas agências especializadas e Uniões Aduaneiras ou Económicas devem adoptar o Guia de Transferência de Dados da OMA para as mensagens EDIFACT/NU como um documento de referência padrão para o desenvolvimento de todos os Guias de Implementação paras as mensagens EDIFACT/NU utilizadas pelas Alfândegas no intercâmbio de dados electronicamente entre as Administrações aduaneiras e entre as Administrações aduaneiras e os operadores utilizadores,

SOLICITA aos membros do Conselho de Cooperação Aduaneira e aos membros da Organização das Nações Unidas ou as suas agências especializadas e as Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação, que notifiquem o Secretário Geral do Conselho de Cooperação Aduaneira a data a partir da qual aplicarão a Recomendação e as condições da sua aplicação. O Secretário-geral transmitirá esta informação às Administrações aduaneiras de todos os membros do Conselho de Administração Aduaneira. Ele transmitirá também às Administrações aduaneiras dos membros da Organização das Nações Unidas ou às suas agências especializadas e às Uniões Aduaneiras ou Económicas que tenham aderido a presente Recomendação.

X
X X

[5] "Conselho de Cooperação Aduaneira" (CCA) é o nome oficial da Organização Mundial das Alfândegas (OMA)

Apêndice 12 – Recomendações da OMA sobre as necessidades de dados para Informação Antecipada sobre Viajantes (IAV)

CONSELHO DE
COOPERAÇÃO ADUANEIRA TC2-3844

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA CONCERNENTE À ADERÊNCIA AOS PADRÕES RELACIONADOS COM A NECESSIDADE DE DADOS PARA INFORMAÇÃO AVANÇADA SOBRE VIAJANTES (IAV)
(6 de Julho de 1993)

O CONSELHO DE COOPERAÇÃO ADUANEIRA,

OBSERVANDO o aumento de risco que representam os passageiros das companhias aéreas particularmente com respeito ao trafico de drogas e o terrorismo internacional,

OBSERVANDO o uso de Intercambio Electrónico de Dados (EDI) pelas transportadoras e pelas autoridades aduaneiras e o potencial beneficio que o uso desta tecnologia pode trazer,

RECONHECENDO que a transmissão electrónica de dados relacionados com os passageiros pode resultar na saída mais célere dos passageiros e pode trazer importantes benefícios para o controlo pelas autoridades aduaneiras,

CONSIDERANDO o Anexo J.1 da Convenção de Quioto o qual requer, nomeadamente, que as aplicações informáticas implementadas pelas autoridades aduaneiras usem padrões internacionalmente aceites,

DESEJANDO particularmente simplificar e harmonizar os arranjos sobre interface entre as transportadoras (aéreas) e as autoridades aduaneiras, particularmente no que concerne ao uso padronizado de elementos de dados, códigos e sintaxes de mensagens,

RECOMENDA que os membros do Conselho e os membros da Organização das Nações Unidas ou as suas agências especializadas e as Uniões Aduaneiras ou Económicas, devem aderir a padrões estabelecidos nas Directivas conjuntas CCC/IATA sobre Informação Avançada sobre Passageiros e quaisquer versões actualizadas ou revisadas destes padrões, para o intercambio electrónico de dados sobre os passageiros,

SOLICITA os membros do Conselho e os membros da Organização das Nações Unidas ou as suas agências especializadas e as Uniões Aduaneiras ou Económicas que aderirem a esta recomendação, que notifiquem o Secretario geral do Conselho da data a partir da qual aplicarão a Recomendação e as condições da sua aplicação. O Secretário geral transmitira esta informação às administrações aduaneiras de todos os membros do Conselho. Ele também transmitirá às administrações aduaneiras dos membros da Organização das Nações Unidas ou às suas agências especializadas e às Uniões Aduaneiras ou Económicas que tenham aceite esta Recomendação.

X
X X

Apêndice 13 – Recomendações da OMA sobre o uso da UNTDED

CONSELHO DE
COOPERAÇÃO ADUANEIRA TC2-3842

RECOMENDAÇÃO DE 26 DE JUNHO DE 1990[6]
DO CONSELHO DE COOPERAÇÃO ADUANEIRA CONCERNENTE AO USO DO DIRECTÓRIO DE ELEMENTOS DE DADOS COMERCIAIS DAS NAÇÕES UNIDAS (UNTDED)

O CONSELHO DE COOPERAÇÃO DAS ALFÂNDEGAS,

DESEJANDO facilitar o intercâmbio internacional de dados entre as administrações aduaneiras e, entre as administrações aduaneiras e os utilizadores comerciais,

CONSIDERANDO que é desejável que nomes de elementos de dados, descrições de elementos de dados e representações de caracteres acordados internacionalmente e universalmente aplicáveis sejam usados em tal intercâmbio de dados,

CONSIDERANDO que é desejável que os mesmos nomes, descrições e representações sejam usados para dados, independentemente do contexto no qual os dados comerciais estão a ser intercambiados (por exemplo, entre a transportadora e o exportador, importador e exportador, alfandegas e importador, etc.),

OBSERVANDO que estes elementos de dados padrão podem ser usados com quaisquer métodos de intercâmbio de dados, em documento papel, ou em outros meios de comunicação de dados, podem ser seleccionados para transmissão um a um, ou usados dentro de um sistema particular de regras de intercâmbio, por exemplo EDIFACT/ONU,

OBSERVANDO TAMBÉM que um subconjunto de UNTED constitui EDIFACT DATA, o Reportório de Elementos de Dados EDIFACT (EDED) também recomendado pelo Conselho de Cooperação Aduaneira, particularmente, para uso no Intercâmbio Electrónico de Dados (EDI),

CONSIDERANDO que o Reportório foi aceite pela Organização dos Padrões Internacionais como um padrão internacional, Secções 1, 2, 3, 3, 4 e 9 do Reportório constituindo o Padrão Internacional ISO 7372,

RECOMENDA que os membros do Conselho e todos os membros da Organização das Nações Unidas ou suas agências especializadas e Uniões Aduaneiras ou Económicas devem usar os nomes dos dados, descrições e representações dos caracteres contidos no Directório dos Dados Comerciais das Nações Unidas (UNTDED) e futuras versões actualizadas deste Directório no intercâmbio de dados electrónicos entre as administrações aduaneiras e entre as administrações aduaneiras e outros utilizadores do comércio.

[6] A presente Recomendação substitui a Recomendação do Conselho de 21 Junho de 1988 relativa à UNTDED

SOLICITA aos membros do Conselho e aos membros da Organização das Nações Unidas ou suas agências especializadas e às Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação, que notifiquem o Secretário-geral a sua aceitação, e a data a partir da qual eles aplicarão a Recomendação, e as condições da sua aplicação.

O Secretário-geral transmitirá esta informação às administrações aduaneiras de todos os membros. Transmitirá também esta informação às administrações aduaneiras de países não membros ou Uniões Aduaneiras ou Económicas que aderiram esta Recomendação.

X

X X

Apêndice 14 – Recomendações da OMA sobre o uso das regras de EDIFACT

CONSELHO DE
COOPERAÇÃO ADUANEIRA TC2-3841

RECOMENDAÇÃO DE 26 DE JUNHO DE 1990[7]

DO CONSELHO DE COOPERAÇÃO ADUANEIRA CONCERNENTE AO

USO DAS REGRAS UN/EDIFACT PARA A TROCA ELECTRÓNICA DE DADOS

O CONSELHO DE COOPERAÇÃO ADUANEIRA,

DESEJANDO facilitar o intercambio internacional de dados entre as administrações aduaneiras e, entre as administrações aduaneiras e os utilizadores comerciais,

CONSIDERANDO que é desejável que um conjunto internacionalmente acordado e universalmente aplicável de regras para estruturação de tais dados, deve ser usado em tal intercâmbio de dados,

NOTANDO que a Comissão Económica das Nações Unidas para a Europa das Nações Unidas (CEE/ONU) desenvolveu um conjunto abrangente de padrões, directórios e directivas para uso nos intercâmbios electrónicos, conhecido como EDIFACT/ONU (Intercambio Electrónico de Dados para a Administração, Comércio e Transporte) é definido no Anexo à presente Recomendação,

CIENTE que as normas, os Reportórios e as directivas EDIFACT/ONU podem ser usados independente da área de aplicação e que o seu uso disseminado no comércio internacional facilitará grandemente o movimento da carga.

NOTANDO que certos elementos das regras EDIFACT/ONU estão na natureza dos padrões que devem ser estritamente respeitados para o sucesso do intercâmbio de dados (por exemplo as Regras Sintaxe DIFACT),

NOTANDO TAMBÉM que certos outros elementos das regras EDIFACT estão na natureza de directivas, cujo uso é altamente recomendado (por exemplo, directivas de concepção de mensagem),

RECOMENDA, que os membros do Conselho e todos os membros da Organização das Nações Unidas ou suas agencias especializadas e as Uniões Aduaneiras ou Económicas, devem aplicam as regras EDIFACT/ONU conforme definido no Anexo a esta Recomendação, e futuras actualizações das versões destas regras para a preparação de mensagens electrónicas para serem intercambiadas entre as administrações aduaneiras e as administrações aduaneiras e outros utilizadores comerciais.

[7] Nota: A presente Recomendação substitui a Recomendação do Conselho, de 21 de junho de 1988, relativa às regras da sintaxe EDIFACT.

SOLICITA aos membros do Conselho e aos membros da Organização das Nações Unidas ou suas agências especializadas e às Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação, que notifiquem o Secretário-geral de sua aceitação, e a data a partir da qual eles aplicarão a Recomendação, e as condições da sua aplicação. O Secretário-geral transmitirá esta informação às administrações aduaneiras de todos os membros. Transmitirá também esta informação às administrações aduaneiras de países não membros ou Uniões Aduaneiras ou Económicas que aceitaram a presente Recomendação.

*

* *

DEFINIÇÃO DE EDIFACT/ONU

EDIFACT/ONU: Regras da Organização das Nações Unidas para o Intercambio Electrónico de Dados para a Administração, Comércio e Transporte. Elas constituem um conjunto de padrões, directórios e directivas acordados internacionalmente para o intercâmbio electrónico de dados estruturados, e em particular aqueles relacionados com o comércio de mercadorias e serviços, entre sistemas independentes de informação informatizada.

Recomendadas no quadro das Nações Unidas, as regras são aprovadas e publicadas pela ONU/CE no Reportório das Nações Unidas para o Intercâmbio de Dados Comerciais (UNTDID) e são mantidos atualizados em aplicação de procedimentos igualmente acordados entre si.

UNTDED inclui:

- As Regras de Sintaxe EDIFACT (ISO 9735);
- As Directivas de concepção de mensagem;
- As Directivas de implementação de Sintaxe;
- O Reportório de Elementos de Dados EDIFACT, EDED (um subconjunto de UNTDED);
- A Lista de Códigos EDIFACT, EDCL;
- O Reportório de elementos de dados compostos EDIFACT, EDCD;
- O Reportório de segmentos padrão EDIFACT, EDSD;
- O Reportório UNSM EDIFACT, EDMD;
- Regras Uniformes de Conduta para o Intercâmbio de Dados Comerciais por Transmissão (UNCID);
- Material explicativo, conforme apropriado.

x
x x

Apêndice 15 – Recomendação da OMA sobre o uso de códigos para elementos de dados

CONSELHO DE
COOPERAÇÃO ADUANEIRA TC2-383

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA CONCERNENTE AO USO DE CÓDIGOS PARA A REPRESENTAÇÃO DE ELEMENTOS DE DADOS

(26 de Junho de 1996)[8]

O CONSELHO DE COOPERAÇÃO ADUANEIRA,

DESEJANDO facilitar o intercambio internacional de dados entre as administrações aduaneiras e, entre as administrações aduaneiras e os intervenientes no comércio internacional,

CONSIDERANDO que é desejável que códigos universalmente aplicáveis e internacionalmente acordados devam ser usados para a representação de elementos de dados em tais intercâmbios,

CONSIDERANDO e apoiando os padrões internacionais adoptados pela Organização Internacional de Padronização (ISO) concernente ao uso de códigos ou estruturas de códigos para a representação de dados,

CONSIDERANDO e apoiando as Recomendações adoptadas pelo Grupo de Trabalho sobre Facilitação dos Procedimentos do Comércio Internacional da Comissão Económica para a Europa (ECE/UN) que recomenda o uso de códigos ou estruturas de códigos para a representação de elementos de dados para propósitos do comércio internacional,

CONSIDERANDO que os códigos ou estruturas de códigos referidos nos Anexos a esta Recomendação oferecem uma base adequada para a representação dos elementos de dados no intercâmbio de dados,

RECOMENDA que os membros do Conselho e os membros da Organização das Nações Unidas ou suas agencias especializadas, e as Uniões Aduaneiras ou Económicas devem usar os códigos ou as estruturas de codificação especificadas nos Anexos a esta Recomendação e futuras versões actualizadas ou revisadas destes códigos ou estruturas de codificação para a representação dos dados no intercambio de dados entre as administrações aduaneiras e entre as administrações aduaneiras e os intervenientes no comércio internacional sempre que haja a necessidade para uma designação codificada,

[8] Esta recomendação substitui a Recomendação do Conselho de 22 de maio de 1984 sobre o uso de códigos e incorpora as Recomendações T2-3831 (Códigos de países ISO-alpha-2) e T2-3832 (Códigos de meios de transporte)

SALIENTA que a aceitação desta Recomendação requer a aceitação da Recomendação e de pelo menos um Anexo, e que cada Anexo deve ser considerado como uma Recomendação separada,

SOLICITA aos membros do Conselho e aos membros da Organização das Nações Unidas ou suas agências especializadas e às Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação, que notifiquem o Secretário-geral do Conselho a data a partir da qual eles aplicarão a Recomendação, e as condições da sua aplicação. O Secretário-geral transmitirá esta informação às administrações aduaneiras de todos os Membros. Transmitirá também esta informação às administrações aduaneiras de países não membros ou Uniões Aduaneiras ou Económicas que aceitaram esta Recomendação.

x

x x

ANEXO I

Pessoas

1. Estrutura de codificação recomendada

Em relação à concepção de um código para pessoas (por exemplo: fornecedores, consignadores, exportadores, consignatários, importadores e declarantes, etc.), devem ser usadas as directivas gerais relativas à codificação de pessoas que foram preparadas pelo Grupo de Trabalho da CCA sobre as aplicações informáticas nas Alfândegas.

Estas directivas gerais, que foram desenvolvidas de forma a fornecer auxílio prático para as Administrações aduaneiras a nível nacional e que são compatíveis com o Padrão Internacional ISO 6523 (Intercambio de dados – Estrutura para a identificação de organizações), estão contidas no Arquivo sobre informatização das operações aduaneiras.

2. Descrição Sumária

As directivas gerais promovem o uso de um método uniforme de codificação de pessoas naturais e legais envolvidas em operações de comércio internacional e de interesse aduaneiro (por exemplo, importadores, exportadores, despachantes, etc.). Em particular, as directivas tratam da função dos códigos, pessoas identificadas, a escolha de códigos, a extensão e o formato dos códigos, a identificação de outros elementos, a identificação de fornecedores estrangeiros, o uso de caracteres de verificação, e considerações sobre critérios e sistemas a serem tomados em conta no desenvolvimento de códigos.

Conforme indicado acima, as directivas são compatíveis com o Padrão Internacional ISO 6523 que especifica a seguinte estrutura para identificação das organizações para propósitos de intercâmbio de dados:

a) um Código Internacional de Designação (ICD) (código fixo de 4 dígitos de extensão);

b) um código da organização; e

c) um nome da organização. O código da organização consiste em até 14 caracteres que identifica uma organização de forma única dentro de um esquema de codificação da organização. O código da organização pode envolver o uso de caracteres alfabéticos, numéricos e alfanuméricos e é recomendado que o código contenha um caracter de verificação que possa ser incluído dentro do código da organização ou num campo separado.

XXX

ANEXO II

Marcas de identificação de contentores

1. Códigos recomendados

Chama-se a atenção para o código ISO contido no Padrão Internacional 6346 (contentores de frete – Codificação, identificação e marcação) para a representação de dados relativos aos contentores de frete usados em meios de transporte diferentes do aéreo e para o código desenvolvido pela IATA para a representação de dados concernentes aos contentores de frete aéreo.

Sempre que sejam capturados e processados dados de identificação de contentores pelas Alfandegas, é recomendado que sejam proporcionados 17 caracteres para os sistemas ADP e documentos associados, de maneira a acomodar o código ISO (um possível total de 17 caracteres) e as actuais e futuras versões do código da IATA (9 e 12 caracteres respectivamente).

2. Descrição Sumária

A. Código ISO

O Padrão Internacional 6346 estabelece um sistema de código de marcação alfanumérico de 17 caracteres para contentores de frete e proporciona uma única identificação internacional por meio de um código do proprietário, um número de série, e um código do país, um sistema de verificação de dígitos para verificar a exactidão do registo do código do proprietário e o número de série, bem como a informação concernente ao tamanho do contentor e características do tipo.

B. Código IATA

O código desenvolvido pela IATA para a representação de dados concernentes aos contentores de frete aéreo consiste actualmente de 9 caracteres alfanuméricos (tipo da unidade, tamanho e compatibilidade, número de série e código do proprietário). Em 1990, o código da IATA passou a consistir de 12 caracteres alfanuméricos incluindo um dígito de verificação.

XXX

ANEXO III

Datas

1. Código recomendado

A representação fornecida na Recomendação ECE No.7 (representação numérica de datas, horas, e intervalos de tempo) que está baseada, nomeadamente, no Padrão Internacional 2014 (Escrita de datas de calendário em forma totalmente numérica) e no Padrão Internacional 3307 (Intercâmbio de informação – representações da hora do dia) deve ser usada para a representação de datas do calendário e horas do dia (por exemplo, data e hora de partida, data e hora de chegada, data do contrato, data de câmbio, data de aceitação da declaração das mercadorias, data de desalfandegamento, etc.).

2. Descrição sumária

A Recomendação Nº.7 da CEE/ONU (representação numérica de datas, horas, e períodos de tempo) está baseada, nomeadamente, nos Padrões Internacionais ISO 2014 e 3307.

A norma ISO 2014 diz respeito a escrita de datas do calendário Gregoriano em forma totalmente numérica, representadas pelos elementos ano, mês, dia, recomenda que todas as datas numéricas para representação da hora local sejam escritos na ordem seguinte: ano – mês – dia (por exemplo: AAAAMMDD) e deve consistir de quatro, dois e dois dígitos para representar o ano, o mês e o dia, respectivamente.

A norma ISO 3307 visa estabelecer representações uniformes do tempo baseadas num sistema de 24 horas. Ele proporciona um meio para representação da hora local na forma digital para o propósito de intercâmbio de informação entre os sistemas de dados. A hora local é definida como hora do relógio em uso público no ponto de origem. No sistema de 24 horas, a hora local pode ser expressada por combinações dos elementos do tempo: horas, minutos e segundos, por exemplo, horas e minutos (HHMM).

Em relação às datas do calendário, chama-se a atenção para o facto de que a Recomendação ECE No.7 preveja o uso de apenas dois caracteres para representar o ano (AAMMDD por exemplo).

XXX

ANEXO IV

Moedas

1. Códigos recomendados

O código alfabético ISO de três letras para moedas contido no Padrão Internacional 4217 (Códigos para a representação de moedas e fundos) deve ser usado para a representação de moedas.

2. Descrição sumária

A norma ISO 4217 oferece a estrutura para um código alfabético com três letras e um código equivalente de três dígitos numéricos para a representação de moedas e fundos.

Os dois primeiros caracteres (mais à esquerda) do código alfabético para moedas da norma ISO 4217 proporcionam um único código para a autoridade monetária à qual está atribuído. Onde praticável, é derivado do código de país ISO alpha-2 contido na norma ISO 3166 (Códigos para a representação de nomes de países) que é recomendado pelo Conselho de Cooperação Aduaneiro e pelo Grupo de Trabalho sobre Facilitação dos Procedimentos do Comércio Internacional da Comissão Económica para a Europa (CEE/ONU). O terceiro caracter (mais à direita) do código alfabético é um indicador, preferencialmente mnemónico, derivado do nome da principal unidade monetária ou fundo. Em aplicações não bancárias, os primeiros dois caracteres (mais à esquerda) são suficientes para identificar uma moeda. O código numérico da moeda é derivado, onde possível, dos Códigos Padrão de Países ou Áreas das Nações Unidas.

A Recomendação Nº 9 adoptada em Fevereiro de 1978 pelo Grupo de Trabalho sobre Facilitação Procedimentos do Comércio Internacional da Comissão Económica para a Europa (CEE/ONU), recomenda o uso do código ISO alfabético de três letras de moeda para a representação de moedas para fins do comércio internacional.

XXX

ANEXO V

Códigos dos Países

1. Códigos recomendados

Os códigos alfa-2 de representação de países preconizados pela norma internacional ISO 3166, referidos na Recomendação Nº.3 da CEE/ONU devem ser usados para a representação dos nomes de países no comércio internacional.

Todavia, deve ser observado que a aceitação desta Recomendação da OMA não exclui o uso de outros códigos referidos norma ISO 3166 para a representação de nomes de países para certas aplicações (por exemplo, o código de país ISO alfa-3 para os passaportes legíveis por máquinas, conforme o estabelecido nas Directivas do CCA/IATA sobre Informação Avançada sobre Passageiros). A aceitação da Recomendação também não exclui o uso de códigos não-ISO para propósitos nacionais ou internos no caso de países pertencentes a uma União Aduaneira ou Económica.

2. Descrição sumária

O código ISO alfa-2 relativo a países consiste num código alfabético de duas letras.

XXX

ANEXO VI

Descrições das mercadorias

e posições pautais ou estatísticas

1. Estrutura de codificação recomendada

O Sistema Harmonizado de Descrição e Codificação de Mercadorias deve ser usado.

2. Sumário descritivo

O Sistema Harmonizado de Descrição e Codificação de Mercadorias é uma nomenclatura multiuso com seis dígitos para bens transportáveis, que responde simultaneamente às necessidades das Autoridades aduaneiras, dos especialistas das estatísticas envolvidos no comércio externo ou produção, transportadoras e produtores. O Sistema Harmonizado é adequado para o processamento e transmissão automática de dados e proporciona uma terminologia e código comuns, identificando especificamente 5.019 grupos de mercadorias resultantes de uma expansão detalhada de 1.241 subposições de quatro dígitos. Estes últimos resultam de uma revisão e actualização bastante extensiva, não apenas em detalhes mas também na estrutura, pelo Conselho de Cooperação Aduaneira em Nomenclatura (CCAN). O Sistema Harmonizado pode ser subdividido ainda mais, onde necessário, para atender necessidades nacionais e internacionais.

XXX

ANEXO VII

Procedimentos Aduaneiros

1. Código recomendado

As directivas gerais e o código de um dígito desenvolvido pelo Grupo de Trabalho do CCA sobre aplicações informáticas para as Alfândegas devem ser usados para a representação de procedimentos aduaneiros. As directivas gerais e o código de um dígito estão contidos no Arquivo sobre informatização das operações aduaneiras.

2. Sumário descritivo

O código para a representação de procedimentos aduaneiros desenvolvidos pelo Grupo de Trabalho CCA sobre aplicações informáticas para as Alfândegas é um código de um dígito de nível amplo dentro do qual os principais procedimentos aduaneiros são identificados e dentro dos quais os utilizadores podem desenvolver códigos únicos para atender necessidades nacionais e internacionais.

XXX

ANEXO VIII

Unidades de medida

1. Códigos recomendados

Os códigos contidos na Recomendação Nº.20 da CEE/ONU (Códigos para unidades de medida usados no comércio internacional) devem ser usados para representação de unidades de medida.

2. Sumário descritivo

Os códigos da unidade de medida desenvolvidos pela CEE/ONU consistem de um código alfabético de comprimento fixo (três letras), e um código numérico de comprimento fixo (três dígitos).

XXX

ANEXO IX

Código do Modo de Transporte

1. Códigos recomendados

Os códigos contidos na Recomendação Nº.19 da CEE/ONU (Códigos para o modo de transporte e os correspondentes meios de transporte usados no comércio internacional) devem ser usados para a representação de modos de transporte.

2. Descrição sumária

Os códigos de modos de transporte desenvolvidos pela CEE/ONU consistem de um código numérico de um único dígito. Todavia, há previsão para a possibilidade de um segundo dígito numérico onde o código básico necessite ser subdividido.

x
x x

Apêndice 16 – Recomendações da OMA sobre informação aduaneira processada por computador

ORGANIZAÇÃO MUNDIAL DAS ALFÂNDEGAS[9]

RECOMENDAÇÃO DA ORGANIZAÇÃO MUNDIAL DAS ALFANDEGAS RELATIVA À TRANSMISSÃO E AUTENTICAÇÃO ELECTRÓNICAS DE INFORMAÇÕES ADUANEIRAS E DE OUTRAS INFORMAÇÕES REGULADORAS RELEVANTES

(16 de Junho de 1981 revisado 24 de Junho de 2005)

A ORGANIZAÇÃO MUNDIAL DAS ALFÂNDEGAS,

DESEJOSA em capacitar as administrações aduaneiras e os agentes económicos internacionais a fazer maior uso dos seus sistemas informáticos, tornando possível para os declarantes transmitirem informação aduaneira por meios electrónicos ou outros automáticos,

CONSIDERANDO que o processamento de dados automatizados, e-commerce incl. o Intercâmbio Electrónico de Dados (EDI) e técnicas de segurança torna possível transmitir, validar e autenticar informação aduaneira processada por computador (tal como declarações de mercadorias, informação dos manifestos, informação de licenças, etc.) ao contrário de documentação em papel e assinatura manual; que estes métodos incluem o uso de palavras-chaves únicas ligadas ao declarante e transmitidas com a informação, chaves de software para a codificação dos dados e a geração de assinaturas electrónicas; que, de acordo com as disposições da legislação nacional ou sob os termos de um compromisso assinado pelo declarante, o uso de tais técnicas de segurança para a transmissão de informação aduaneira pode ser considerada tão vinculativa para o declarante como uma assinatura manual na documentação em papel,

TOMANDO EM CONTA que "a Recomendação sobre autenticação de documentos comerciais por meios outros que que não a assinatura", também adoptada em Março de 1979 pelo Grupo de Trabalho acima mencionado, que salienta que adopção geral de meios electrónicos ou outros meios automáticos de transferência de dados requer mudanças na actual legislação nacional e Convenções internacionais e nas actuais práticas comerciais no concernente a assinaturas,

TOMANDO TAMBÉM EM CONTA o "Modelo de Lei sobre o Comércio Electrónico" da Comissão das Nações Unidas sobre a Lei do Comércio Internacional (UNCITRAL), adoptado pelas Nações Unidas em Dezembro de 1996 e o "Modelo de Lei sobre Assinaturas Electrónicas", adoptado pelas Nações Unidas em Dezembro de 2001 como referencias úteis para o desenvolvimento do e-commerce nacional e legislação sobre as assinaturas digitais,

RECOMENDA que os membros do Conselho e os membros da Organização das Nações Unidas ou suas agências especializadas e as Uniões Aduaneiras ou Económicas devem:

1. Permitir, sob as condições a serem estabelecidas pelas autoridades aduaneiras, os declarantes usarem vários meios electrónicos (incluindo redes adicionadas, Internet, redes de informática sem fio, discos, fitas, etc.) para a transmissão de informação

[9] Criada em 1952 com o nome de Conselho de Cooperação Aduaneira (CCA).

aduaneira às autoridades aduaneiras para o processamento automático e para receber uma resposta automática para tal informação, a partir das Alfândegas;

2. Aceitar, sob as condições determinadas pelas autoridades aduaneiras, informação aduaneira de declarantes e outras agências do governo transmitida através do uso de meios electrónicos, validada e autenticada por tecnologia de segurança, sem a necessidade de produzir documentação em papel com uma assinatura manual.

3. Assegurar, onde os governos não operam um "Guiché Único" electrónico para os declarantes submeterem informação para transacções transfronteiriças internacionais de uma só vez para um ponto de acesso único, que as necessidades e especificações técnicas concernentes à autenticação de trocas electrónicas de informação sejam coordenadas entre as agências governamentais envolvidas;

4. Aceitar, onde o reconhecimento legal de informação aduaneira transmitida electronicamente ainda não esteja resolvida, que as Alfândegas autorizem os declarantes, sob as condições estabelecidas pelas Alfândegas ou outras autoridades competentes, produzir informação aduaneira em papel comum;

5. Aceitar, onde a segurança EDI e as técnicas de processamento automático são usadas, mas onde devido a restrições legais, a produção de documentação em papel e de assinaturas manuais ainda são exigidas, a periódica submissão de documentação em papel ou o seu armazenamento nas instalações do declarante, sob as condições estabelecidas pelas Alfândegas;

SOLICITA aos membros do Conselho e aos membros da Organização das Nações Unidas ou suas agências especializadas, e as Uniões Aduaneiras ou Económicas que aceitaram esta Recomendação para notificarem o Secretário-geral do Conselho a data a partir da qual eles passarão a aplicar a Recomendação e as condições da sua aplicação. O Secretário-geral transmitirá esta informação às administrações aduaneiras de todos os membros do Conselho. Ele transmitirá também esta informação às administrações dos membros da Organização das Nações Unidas ou às suas agencias especializadas e às Uniões Aduaneiras ou Económicas que aderiram a esta Recomendação.

x x x

Apêndice 17 – Recomendações da OMA sobre o uso dos padrões do CCC/IATA

CONSELHO DE
COOPERAÇÃO ADUANEIRA TC2-3843

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA RELATIVA AO USO DE CÓDIGOS DOS PADRÕES CCC/IATA SOBRE O INTERCÂMBIO DE DADOS
(21 de Junho de 1988)

O CONSELHO DE COOPERAÇÃO ADUANEIRA,

OBSERVANDO o alto nível de informatização na indústria da aviação e o crescente número de administrações aduaneiras que estão a introduzir técnicas de informática,

OBSERVANDO o crescimento do uso do Intercambio Electrónico de Dados (EDI) no comércio mundial e os benefícios de um ambiente comercial sem papel,

CIENTE que o interface dos sistemas automatizados das companhias aéreas e das administrações aduaneiras resultam na redução do volume de papéis,

RECONHECENDO que o interface do processamento automatizado dos dados relacionados com a carga resultam num desalfandegamento célere das consignações aéreas e têm importantes benefícios do ponto de vista do controlo aduaneiro,

CONSIDERANDO o Anexo J.1 da Convenção Internacional sobre a simplificação e harmonização dos procedimentos aduaneiros (18 de Maio de 1973) que requer, nomeadamente, aplicações informáticas implementadas pelas autoridades aduaneiras a usar padrões aceites internacionalmente,

DESEJANDO particularmente simplificar e harmonizar as disposições quanto ao interface entre as companhias aéreas e as autoridades aduaneiras, particularmente, com relação ao uso de elementos padrão de dados, códigos e sintaxe de mensagens,

RECOMENDA que os membros do Conselho e os membros da Organização das Nações Unidas ou suas agências especializadas e Uniões Aduaneiras ou Económicas devem usar os padrões estabelecidos no Manual sobre Padrões de Intercâmbio de Dados do CCA/IATA e as futuras versões actualizadas ou revisadas no estabelecimento de interfaces entre os sistemas automatizados das Alfândegas e companhias aéreas,

SOLICITA aos membros do Conselho e os membros da Organização das Nações Unidas ou suas agências especializadas, e às Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação que notifiquem o Secretário-geral do Conselho a data a partir da qual eles passarão a aplicar a Recomendação e as condições da sua aplicação. O Secretário-geral transmitirá esta informação às administrações aduaneiras de todos os membros do Conselho. Ele transmitirá também esta informação às administrações dos membros da Organização das Nações Unidas ou suas agências especializadas e às Uniões Aduaneiras ou Económicas que aceitaram esta Recomendação.

----VVV----

Apêndice 18 - Recomendação do Conselho de Cooperação Aduaneira relativa à utilização do Modelo de Dados da OMA

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA RELATIVA Á UTILIZAÇÃO DO MODELO DE DADOS DA OMA

(27 Junho de 2009)

O CONSELHO DE COOPERAÇÃO ADUANEIRA,

DESEJANDO facilitar as trocas internacionais de dados entre Alfândegas bem como entre as Alfândegas e as agências de controle fronteiriço, os operadores comerciais e as outras partes envolvidas nas transacções internacionais e nos movimentos transfronteiriços de mercadorias,

CONSIDERANDO que é desejável recorrer a normas internacionais na definição de elementos de dados e elaboração das mensagens electrónicas a utilizar nessas transacções internacionais,

CONSIDERANDO que o Modelo de Dados da OMA

(i) representa o conjunto máximo de dados exigidos para as informações necessárias antes da chegada ou da partida, para a liberação e o desembaraço das mercadorias e dos meios de transporte na importação, na exportação e em trânsito nas fronteiras.

(ii) foi desenvolvido utilizando um conjunto harmonizado de dados exigidos pelas Alfândegas Membro e várias agências de controle fronteiriço, e

(iii) baseia-se em normas internacionais amplamente adoptadas e reconhecidas.

RECOMENDA que, na medida do possível, os Membros do Conselho e todos os Membros da Organização das Nações Unidas ou de suas agências especializadas bem como as Uniões Aduaneiras e Económicas:

1. adoptem o Modelo de Dados da OMA para identificar e definir todos os dados oficiais exigidos nas fronteiras no âmbito das formalidades referentes à chegada e à partida, e aos regimes de importação, exportação e trânsito.

2. utilizem os elementos de dados da OMA, seus nomes e seus números de referência e (ID da OMA), suas descrições e os modos de representação de seus caracteres (inclusive as listas de códigos sugeridos) para descrever e compor as mensagens electrónicas.

3. utilizem as mensagens electrónicas padronizadas descritas no Modelo de Dados da OMA para as mensagens electrónicas entre os Governos bem como entre os Governos e os operadores comerciais.

SOLICITA aos membros do Conselho e a todos os membros da Organização das Nações Unidas ou suas agências especializadas, e às Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação que notifiquem o Secretário-geral do Conselho a data a partir da qual eles passarão a aplicar a Recomendação e as condições da sua aplicação. O Secretário-geral transmitirá esta informação às Administrações Aduaneiras de todos os membros do Conselho. Ele transmitirá também esta informação às administrações dos membros da Organização das Nações Unidas ou suas agências especializadas e às Uniões Aduaneiras ou Económicas que aceitaram esta Recomendação.

*
* *

Apêndice - 19 Recomendação do Conselho de Cooperação Aduaneira[10] relativa à utilização das Informações Antecipadas sobre os Viajantes (IAV) e do Registo de Nomes dos Viajantes (RNV) para assegurar a eficiência dos controles aduaneiros

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA[11] RELATIVA À UTILIZAÇÃO DAS INFORMAÇÕES ANTECIPADAS SOBRE OS VIAJANTES (IAV) E DO REGISTO DE NOMES DOS VIAJANTES (RNV) PARA ASSEGURAR A EFICIÊNCIA DOS CONTROLES ADUANEIROS

(Junho de 2012**)**

O CONSELHO DE COOPERAÇÃO ADUANEIRA,

CIENTE da ameaça contínua e crescente que não deixam de representar as formas graves de criminalidade transnacional, e nomeadamente o tráfico ilícito de droga e de outras mercadorias contrabandeadas, que é bastante preocupante para o bem-estar social, a segurança e a prosperidade das nações do mundo inteiro,

CIENTE do crescimento contínuo do volume de viagens transfronteiriças e dos desafios que isto cria para a facilitação da circulação dos viajantes legítimos,

TENDO EM CONTA as disposições da Convenção de Quioto Revista[12] e, nomeadamente, as do Capítulo 6 do Anexo Geral sobre os controles aduaneiros e do Capítulo 1 do Anexo Específico J sobre os Viajantes,

RECONHECENDO que as Alfândegas têm como responsabilidade primária o controlo dos movimentos transfronteiriços de mercadorias, meios de transporte e pessoas, e que elas estão, portanto, colocadas idealmente para prevenir, detectar e impedir o trafico ilícito de drogas e de outras mercadorias contrabandeadas nas fronteiras antes que estas se dispersem no território dos diferentes países,

CIENTE dos incidentes que provam a existência de um elo estreito entre as formas graves de criminalidade transnacional e o terrorismo, e da necessidade de diminuir os riscos que representam os viajantes,

RECONHECENDO que a melhor forma de alcançar o equilíbrio apropriado entre as necessidades em matéria de luta contra a fraude aduaneira e a facilitação das viagens legítimas consiste na luta contra a fraude aduaneira baseando-se na informação, e que o uso das IAV e/ou do RNV para avaliar os riscos ajudaria consideravelmente as Alfândegas a desenvolver e explorar a informação mais útil para o controle dos viajantes,

[10] Conselho de Cooperação Aduaneira é o nome oficial da Organização Mundial das Alfândegas (OMA).
[11] Conselho de Cooperação Aduaneira é o nome oficial da Organização Mundial das Alfândegas (OMA).
[12] Convenção Internacional sobre a Simplificação e a Harmonização dos Procedimentos Aduaneiros (revista).

DESEJANDO harmonizar os acordos celebrados entre as Alfândegas e as empresas, particularmente no que toca à transmissão electrónica das IAV e/ou do RNV em conformidade com os formatos das mensagens e com os elementos de dados padronizados à nível internacional,

ESTIMANDO que o controle eficiente das formas graves de criminalidade transnacional, e nomeadamente do trafico ilícito de drogas e de outras mercadorias contrabandeadas nas fronteiras pode ser amplamente facilitado/apoiado pela cooperação entre as Alfândegas e outras instituições competentes em matéria de controle nas fronteiras a nível nacional e internacional, e que a troca de informações podem ajudar significativamente a avaliação do risco e identificação e, consequentemente, melhorar a facilitação das viagens de carácter lícito,

RECOMENDA aos Membros do Conselho e às Uniões Aduaneiras ou Económicas:

1. que se assegurem de que a prevenção, detecção e repressão da criminalidade transnacional grave, nomeadamente do trafico ilícito de drogas e de outras mercadorias contrabandeadas, sejam incentivadas e permaneçam uma das prioridades dos programas e estratégias de luta contra a fraude das Alfândegas,

2. que envidem esforços no sentido de obter a cooperação das companhias aéreas e outras sociedades internacionais de transporte de viajantes para ajudar as Alfândegas a cumprir a sua missão,

3. que utilizem as informações prévias, a saber, as IAV e/ou o RNV, para avaliar os riscos ligados aos viajantes e:

    - estabelecer prerrogativas legais que permitam obter o acesso às IAV e/ou ao RNV, ou de exigir a sua transferência, seu uso e seu arquivo, em conformidade com as modalidades fixadas e o âmbito dos dados exigidos para este fim, e de implementar mecanismos de protecção dos dados pertinentes,

    - aderir às normas, formatos e procedimentos técnicos fixados nas directivas reconhecidas a nível internacional, e

    - na medida do possível, participar dos trabalhos de concepção ou de actualização das normas, procedimentos e formatos técnicos internacionais, bem como das melhores práticas relativas à sua aplicação,

4. que promovam a cooperação com as outras Alfândegas e as apoiem, de acordo com o quadro jurídico nacional, inclusive a troca de informações e de experiência no uso das IAV e/ou do RNV com vista à identificação mais eficiente dos viajantes potencialmente de alto risco.

CONVIDA os Membros do Conselho e das Uniões Aduaneiras ou Económicas que aceitam a presente Recomendação a notificarem o Secretário-geral do Conselho a data a partir da qual eles passarão a aplicar a Recomendação e as condições da sua aplicação.

Apêndice 20 - Recomendação do Conselho de Cooperação Aduaneira[13] Relativa à Desmaterialização dos Documentos de Suporte

RECOMENDAÇÃO DO CONSELHO DE COOPERAÇÃO ADUANEIRA[14] RELATIVA À DESMATERIALIZAÇÃO DOS DOCUMENTOS DE SUPORTE

(Junho de 2012)

O CONSELHO DE COOPERACAO ADUANEIRA,

TENDO EM CONTA que grande parte das Alfândegas implementou sistemas automatizados de desembaraço aduaneiro de mercadorias e comprometeu-se em aplicar as tecnologias de informação para apoiar as operações aduaneiras, quando for rentável e eficaz para as Alfândegas e para os operadores comerciais;

CONSIDERANDO que a utilização dos documentos em suporte papel no comércio internacional é onerosa, morosa e propicia erros e irregularidades,

TENDO EM CONTA as disposições do Capítulo 3 do Anexo Geral da Convenção de Quioto Revista[15] relativa à apresentação electrónica dos documentos de suporte às Alfândegas,

RECONHECENDO a concepção rápida de soluções rentáveis, seguras e fiáveis para os sistemas de gestão e de conservação dos documentos electrónicos, e a adopção generalizada dessas soluções pelos meios comerciais e as administrações,

RECONHECENDO que as organizações internacionais, os serviços públicos e as associações profissionais implementam, cada vez mais, formatos padronizados para os documentos electrónicos tais como licenças, certificados e autorizações, e incentivam a sua utilização ao longo de todas as transacções comerciais internacionais,

COM VISTA a promover as transacções electrónicas para o desembaraço aduaneiro como variante das exigências documentais sob papel,

DESEJANDO reduzir os custos do comércio e simplificar os procedimentos comerciais aliviando a carga que representa a entrega, o arquivo e a apresentação dos documentos suporte originais sob suporte papel ao longo dos procedimentos aduaneiros, e

DESEJANDO melhorar o controle aduaneiro recorrendo eficazmente às verificações automatizadas e adoptando o princípio da gestão de riscos,

RECOMENDA aos Membros do Conselho e a todos os Membros da Organização das Nações Unidas ou suas agências especializadas, e às Uniões Aduaneiras ou Económicas, na medida do possível:

---

[13] Conselho de Cooperação Aduaneira é o nome oficial da Organização Mundial das Alfândegas (OMA).

[14] Conselho de Cooperação Aduaneira é o nome oficial da Organização Mundial das Alfândegas (OMA).

[15] Convenção Internacional sobre a Simplificação e a Harmonização dos Procedimentos Aduaneiros (revista).

(1) que identifiquem os documentos suporte que devem normalmente acompanhar os manifestos de carga e as declarações de mercadorias e determinem a necessidade de apresentar esses documentos para fins de desembaraço aduaneiro a fim de os eliminar;

(2) que suprimam a obrigatoriedade de apresentar os documentos suporte sob suporte papel se os mesmos já foram apresentados sob o formato electrónico;

(3) que procedam à liberação e ao desembaraço aduaneiro da mercadoria unicamente com base em uma declaração electrónica e em uma verificação automatizada;

(4) que façam com que os sistemas automatizados de desembaraço aduaneiro possam verificar automaticamente as informações contidas nos documentos suporte desmaterializados quando essas informações estão disponíveis electronicamente:

a) nas bases de dados das outras administrações públicas;

b) nos ambientes de "*janela única"* (e sistemas comunitários de mercadorias);

c) nos repertórios privados.

CONVIDA os membros do Conselho e os membros da Organização das Nações Unidas ou suas agências especializadas, e às Uniões Aduaneiras ou Económicas que aceitarem esta Recomendação a notificarem o Secretário-geral do Conselho a data a partir da qual eles passarão a aplicar a Recomendação e as condições da sua aplicação. O Secretário-geral transmitirá esta informação às administrações aduaneiras de todos os membros do Conselho. Ele transmitirá também esta informação às Administrações Aduaneiras dos membros da Organização das Nações Unidas ou suas agências especializadas e às Uniões Aduaneiras ou Económicas que aceitaram a presente Recomendação.

X
X X