Banco de Portugal

Carta Circular nº 10/2001/DSBDR de 17-05-2001

ASSUNTO: **Prestação de serviços financeiros através da Internet: Recomendações prudenciais.**

Tem-se assistido, nos últimos anos, a um aumento do uso de meios electrónicos na prestação de serviços pelas instituições de crédito e sociedades financeiras. Em particular, a *Internet* tem-se desenvolvido rapidamente, nos tempos mais recentes, como um novo canal de distribuição de serviços financeiros. Se por um lado, este meio de comunicação veio criar novas oportunidades para as instituições financeiras, proporcionando, nomeadamente, redução de custos, uma mais fácil expansão internacional e uma maior disponibilidade para oferecer produtos "por medida", por outro lado, a entrada de novos fornecedores no mercado e a intensificação da concorrência - a que acrescem os riscos associados a algumas das características da tecnologia utilizada pela *Internet* - são motivos de preocupação para as instituições envolvidas, bem como para as autoridades encarregadas da sua supervisão prudencial.

Conquanto os actuais requisitos de fundos próprios e as demais regras prudenciais se apliquem da mesma forma às actividades bancárias tradicionais e à banca electrónica, os canais electrónicos de distribuição de serviços financeiros colocam questões prudenciais que devem ser abordadas de um modo diferente, quer pelas instituições, quer pelas autoridades de supervisão.

Neste contexto, o Banco de Portugal entendeu oportuno transmitir um conjunto de normas dirigidas às instituições que recorrem à rede *Internet*, como canal de distribuição dos seus serviços, para serem tidas em conta, no âmbito da sua organização e controlo interno; encontrando-se, porém, a prestação de serviços financeiros por via electrónica ainda numa fase inicial do seu desenvolvimento, considerou-se ser mais adequado dar àquele normativo o carácter de recomendações, numa primeira fase, a fim de evitar que um carácter imperativo do mesmo pudesse, potencialmente, restringir a inovação tecnológica neste domínio.

Assim, no documento anexo são abordados os principais riscos a que as instituições que recorrem à *Internet* se encontram expostas, com particular relevância para as instituições que dispõem de *websites* transaccionais, seguindo-se um conjunto de recomendações que as mesmas devem observar ao nível da sua organização e do seu controlo interno. Em anexo ao referido documento, são apresentados, a título de ilustração, um conjunto de aspectos concretos que requerem uma atenção particular e que permitirão às instituições verificar o nível de adequação da organização existente ou projectada.

O Banco de Portugal propõe-se, após um certo período, avaliar a adequação das presentes recomendações, verificando se se torna necessário proceder à sua adaptação, quer por virtude da evolução tecnológica, entretanto ocorrida, quer por exigências da abordagem prudencial a nível internacional.

Enviada a:
Instituições de Crédito, Sociedades Financeiras, Sociedades Gestoras de Participações Sociais e Outras Sociedades Financeiras.

Serviços financeiros prestados através da *Internet*: recomendações prudenciais

I – Introdução

1. Ao longo das duas últimas décadas, a natureza dos canais de distribuição dos serviços financeiros mudou profundamente em função dos desenvolvimentos tecnológicos ocorridos. As ATM's, os pagamentos através de cartões electrónicos e a banca telefónica foram introduzidos já há algum tempo. Presentemente, a *Internet* está gradualmente a ganhar relevância como meio de distribuição, diferindo dos anteriores pela acessibilidade e cobertura muito mais amplas. Apesar de o número de clientes da banca electrónica ainda ser limitado, aquele número poderá crescer substancialmente num prazo relativamente curto. Este crescimento será estimulado pelos desenvolvimentos esperados relativamente à segurança das transacções através da *Internet* e pela disponibilização de livre acesso a esse meio de comunicação.

2. Embora o presente documento aborde primordialmente a prestação de serviços financeiros através da *Internet,* o seu âmbito de aplicação deverá ser entendido como abrangendo qualquer prestação de serviços financeiros que envolva a transferência de informação através de dados electrónicos entre partes através de uma rede. Essa rede pode ser uma rede de computadores, tal como a *Internet,* mas também pode ser uma rede de telecomunicações, incluindo uma rede de telecomunicações móveis, ou uma rede de televisão, incluindo a rede de televisão por cabo.

3. Um grande número de instituições de crédito e de sociedades financeiras portuguesas dispõe de um *site* na *Internet*. Através deste *website,* uma instituição pode atingir diferentes objectivos. Se apenas pretender fornecer informações sobre a instituição, sobre a sua gama de produtos e serviços, sobre a sua rede de agências e a sua estrutura tarifária, estamos perante um ***website* puramente informativo**. Se o *site* comportar funções pedagógicas e de consulta, estamos na presença de um ***website* interactivo.** No caso de o *site* permitir o fornecimento de serviços financeiros, como sejam a transferência de fundos, a realização de pagamentos, a contratação de créditos ou ainda realizar operações de compra ou de venda de instrumentos financeiros (investir em linha), falamos de um ***website* transaccional.**

4. Dado os riscos a que se encontram associados, são principalmente os ***websites* transaccionais** que merecem uma atenção particular sob o ponto de vista prudencial.

5. No presente documento enumeram-se as principais disposições regulamentares e prudenciais que, em aplicação, nomeadamente do disposto nos artigos 73.º e 93.º, nº1, do Regime Geral das Instituições de Crédito e Sociedades Financeiras, as instituições devem ter em conta na elaboração da sua organização e do seu controlo interno. Uma *check-list,* anexa ao documento, inventaria uma série de matérias concretas que requerem uma atenção particular e para as quais se formulam recomendações, que deverão permitir às instituições que recorrem à *Internet* verificar a adequação da sua organização.

6. Para efeitos do presente documento, entende-se por instituições as instituições de crédito e as sociedades financeiras, autorizadas em Portugal, que através de um *website* oferecem ou prestam serviços bancários e serviços de investimento. Sem prejuízo das competências das autoridades de supervisão do país de origem, no domínio da organização e do controlo interno, as presentes orientações aplicam-se igualmente às sucursais das instituições de crédito e de sociedades financeiras da União Europeia na medida em que aquelas orientações fazem parte integrante das disposições aplicáveis em Portugal por razões de interesse geral, entre as quais as regras de conduta.

II – Recomendações prudenciais

A – Princípios e riscos associados à prestação de serviços financeiros através da *Internet*

7. Sem prejuízo do respeito pelo quadro das disposições legais e regulamentares que se aplicam à prestação de serviços financeiros, as instituições devem dispor de uma estrutura e de uma organização adequadas, de mecanismos de controlo e de segurança no domínio informático, bem como de procedimentos de controlo interno apropriados, a fim de cobrir os riscos específicos associados ao novo canal de distribuição.

8. Estes riscos – cuja ocorrência pode ter um impacto importante sobre a situação financeira da instituição – englobam nomeadamente:

   a) **O risco legal,** ou seja, o risco de perdas resultante de uma inadequada conformidade com as normas legais e regulamentares aplicáveis. A utilização de um novo canal de distribuição obriga a instituição a examinar uma série de novas situações jurídicas, em Portugal ou no estrangeiro, que requerem um enquadramento adequado. Este risco é particularmente importante no caso da prestação de serviços transfronteiras, caso em que as instituições têm de respeitar regras emitidas noutros países, podendo existir alguma incerteza acerca da sua interpretação com respeito à *Internet.* Este é um risco particular para as instituições cujas actividades electrónicas são desenvolvidas, no todo ou em parte, por organizações externas *(outsourcing).*
   b) **O risco operacional:** quando relacionado com as actividades desenvolvidas através da *Internet*, este risco refere-se, principalmente, a aspectos de segurança, incluindo a verificação da identidade e da autenticidade das pessoas, à inibição de acessos não autorizados ao sistema e à protecção da privacidade. Os novos serviços, que podem influenciar de forma significativa o exercício da actividade e a estrutura financeira da instituição, pressupõem a existência de novos sistemas e de novos procedimentos, bem como de novos clientes, novas contrapartes e novos fornecedores de serviços, o que implica que as operações devem ser seguidas pelos colaboradores da instituição, os quais deverão ter recebido formação específica neste domínio.
   c) **O risco de reputação:** a instituição pode conhecer uma degradação da sua reputação se a prestação de serviços através da *Internet* for deficiente ou não fiável, se não responder às expectativas dos utilizadores e do público, ou se apresentar lacunas ou comportar infracções em termos das disposições gerais e regulamentares portuguesas e/ou estrangeiras. Dado que a velocidade da realização das operações através da *Internet* é muito mais rápida do que nos outros canais de distribuição, este tipo de risco é mais elevado do que para a prestação de serviços financeiros nos moldes tradicionais.
   d) **O risco estratégico,** ou seja, o risco de um efeito adverso nos lucros como resultado de uma inadequada resposta a mudanças ocorridas no mercado, ou de uma incorrecta decisão ou da incorrecta implementação das decisões.
   e) **O risco de liquidez:** o risco de a instituição não se encontrar em condições de cumprir tempestivamente as suas obrigações de pagamento por falta de meios líquidos. A *Internet* possibilita que os clientes pesquisem facilmente qual a instituição que oferece melhores condições (por exemplo a taxa de depósitos mais elevada). Quer isto dizer que se houver uma mudança na taxa de juro, os clientes irão trocar de instituição a uma larga escala e muito rapidamente, o que significa que as instituições poderão experimentar grandes flutuações na sua liquidez.

B – Recomendações relativas à organização e ao controlo interno das instituições.

B.1. Generalidades

1. Antes de abrir um *website*, a instituição deve adaptar a sua organização e o seu controlo interno em função dos riscos identificados e, se necessário, testar os sistemas. A instituição deverá, para esses efeitos, ter em conta as orientações prudenciais a seguir enunciadas, quando elas respeitam, nomeadamente, à política geral da instituição, bem como sobre aspectos organizacionais específicos ligados à oferta de serviços através da *Internet*, tais como o enquadramento jurídico e operacional da actividade, a identificação de clientes, etc. São igualmente relevantes os aspectos que tratam do respeito pelas regras de conduta e o respeito das obrigações que cabem à instituição quando os serviços fornecidos através da *Internet* apresentam um carácter transfronteiras.

2. Uma *check-list* detalhada, junta em anexo, enumera por tema – a título de comentário – uma série de pontos concretos e de recomendações sobre a organização e o controlo interno. Esta lista poderá servir de guia à instituição para verificar o carácter adequado da sua prestação (ou do seu projecto de prestação) de serviços financeiros através da *Internet.*

B.2. Aspectos de política

3. O órgão de administração da instituição deve definir a sua política e a sua estratégia para o projecto *Internet* bem como para a organização e acompanhamento das operações em questão. A concepção e aplicação de estratégias a nível da *Internet* deverá ser objecto de uma análise cuidadosa, devendo as suas consequências ser bem compreendidas pelos órgãos de gestão. Neste âmbito, podem referir-se os pontos seguintes:

   a) Definição da política geral, financeira e comercial;
   b) Determinação da forma e do conteúdo do *website;*
   c) Fixação das opções técnicas e da política de segurança;
   d) Determinação da gestão dos riscos e do envolvimento dos diferentes níveis de controlo da instituição (controlo interno, auditoria interna e externa, revisor oficial de contas);
   e) Exame e controlo das implicações e riscos jurídicos;
   f) Determinação dos meios e procedimentos em matéria de conservação de dados.

B.3. Relações contratuais

1. A instituição deve dar especial atenção ao enquadramento jurídico da actividade, recorrendo, se necessário, a consultoria jurídica externa, acerca, nomeadamente, das relações com o fornecedor da tecnologia, com os utilizadores do serviço *Internet*, bem como com as contrapartes envolvidas nesta actividade.

2. As instituições devem fornecer aos potenciais clientes uma informação adequada sobre os serviços *on-line* que se propõem prestar e conceder uma atenção especial à redacção dos contratos (novos ou adaptação dos existentes), regulamentos ou condições gerais. O contrato deve incluir uma descrição precisa da natureza e do âmbito dos serviços fornecidos.

3. Relativamente à relação "instituição/fornecedor da tecnologia", é muito importante que as instituições possam dispor de garantias suficientes no que se refere à capacidade financeira do fornecedor, bem como da fiabilidade, integridade, segurança de funcionamento e desenvolvimento futuro da tecnologia fornecida. Estas garantias devem assegurar a continuidade da prestação de serviços.

B.4. Segurança

4. A instituição deve colocar em funcionamento um dispositivo que garanta uma segurança adequada do seu *website*, da sua infra-estrutura e das operações e deve dispor, igualmente, de planos de contingência adequados para o caso em que a prestação de serviços em linha seja interrompida. A verificação deste dispositivo deve ser efectuada através dos sistemas de controlo interno e ser contemplada nas actividades de auditoria interna e/ou externa da instituição.

B.5 Aspectos operacionais

5. A instituição deve acompanhar de forma adequada as operações que lhe são transmitidas através da *Internet* e prever procedimentos que permitam garantir o normal desenvolvimento das operações e controlar os riscos incorridos. A instituição deve assegurar que os colaboradores que utilizam (ou sejam susceptíveis de vir a utilizar) as aplicações *Internet*, tenham recebido formação adequada.

6. Convém notar, por outro lado, que o respeito de certas disposições legais ou regulamentares implica que a instituição possa suspender a execução de transacções por conta dos clientes a fim de que possa realizar controlos de conformidade e/ou possa recusar a sua execução (por exemplo em caso de suspeita de branqueamento de capitais.).

B.6. Identificação do cliente à distância

7. O artigo 3.º do Decreto-Lei nº 313/93, de 15 de Setembro, bem como a Instrução do Banco de Portugal nº 70/96, estabelecem deveres especiais de identificação dos clientes sempre que as instituições se proponham iniciar relações de negócio ou efectuar transacções ocasionais cujo montante, isoladamente ou em conjunto, atinja ou ultrapasse 2 500 000$00, quer estas operações se efectuem presencialmente quer não. A regulamentação impõe a recolha dos elementos de identificação exigidos para a abertura de contas de depósito e a extracção de cópias dos respectivos documentos comprovativos, os quais deverão ser conservados nos prazos estabelecidos no art.º 9.º do referido Decreto-Lei nº 313/93.

8. Torna-se, assim, evidente que a ausência de contacto directo com o cliente não pode pôr em causa o respeito por parte da instituição da sua obrigação de identificação dos clientes. Procedimentos particulares são, pois, necessários, com o objectivo de encontrar um equilíbrio entre, de um lado, um certo grau de flexibilidade para adaptação ao progresso técnico, e de outro, a garantia de uma identificação correcta. Se uma instituição pretender concluir contratos ou operações à distância sem que exista um contacto presencial, ela deve colocar em funcionamento procedimentos de identificação dos clientes que satisfaçam as condições enunciadas pela Instrução do Banco de Portugal nº 70/96, relativa à prevenção do branqueamento de capitais, nomeadamente:

   a) estes procedimentos devem garantir uma identificação adequada dos clientes, em conformidade com a regulamentação portuguesa;
   b) eles devem permitir assegurar os deveres especiais de diligência que competem às instituições, no caso em que se supõe, ou se dispõe de indicações que permitam crer que o cliente evita precisamente um contacto presencial para esconder a verdadeira identidade e/ou que se trata de uma questão de branqueamento de capitais;
   c) eles devem ser objecto de uma atenção particular por parte dos auditores internos e externos.

B.7. Medidas e procedimentos visando assegurar o respeito pelas regras de conduta

1. As instituições que prestam serviços financeiros através da *Internet*, devem tomar as medidas necessárias para respeitar as regras de conduta que lhes são aplicáveis, nomeadamente as disposições constantes do Título VI, Capítulo I (art.º 73.º e seguintes) do Regime Geral das Instituições de Crédito e Sociedades Financeiras. As instituições devem, por outro lado, tomar as medidas adequadas para respeitar as obrigações de diligência, neutralidade, lealdade, discrição e respeito consciencioso dos interesses que lhes estão confiados, nas relações que estabelecem com os seus clientes.

2. A relação à distância que, em caso de prestação de serviços *on-line*, pode ser um dado constante, tanto quando do início da relação de negócios, como no seguimento da execução das transacções, exclui um certo número de contactos e de intervenções "humanas" clássicas que, noutros casos, podem assegurar uma troca de informações entre o intermediário financeiro e o investidor. Torna-se, pois, importante que a instituição assegure que os serviços prestados à distância correspondem bem ao perfil do cliente (por exemplo, os seus conhecimentos e a sua experiência em matéria de investimentos, a sua situação financeira, os seus objectivos de investimento).

3. Recomenda-se, igualmente, o fornecimento aos clientes de uma informação adequada sobre os riscos ligados à prestação de serviços através da *Internet* e aos instrumentos financeiros, bem como sobre o funcionamento e as regras dos mercados nos quais os clientes negoceiam.

4. No que se refere às transacções em concreto, salienta-se a necessidade de as instituições disporem de meios suficientes para identificar eventuais operações anormais.

B.8. Carácter transfronteiriço dos serviços oferecidos ou prestados

5. Num *website* que tem, por definição, um âmbito internacional, a oferta e a prestação de serviços podem revestir um carácter transfronteiriço.

6. No caso da prestação de serviços no âmbito do Espaço Económico Europeu, a instituição deve ter em consideração as obrigações de notificação que lhe impõe a regulamentação aplicável. No que se refere às obrigações de notificação, as autoridades de supervisão têm, até ao momento, adoptado o ponto de vista seguinte: considera-se que uma prestação de serviços reveste natureza transfronteiriça não só quando a prestação característica do serviço tem lugar no território de um outro Estado-Membro, mas igualmente quando a instituição tenta captar investidores desse outro

Estado-Membro, seja deslocando-se, seja recorrendo a técnicas de venda à distância ou a publicidade de tipo não generalista.

7. No que se refere, em particular, à utilização de um *site* na *Internet*, várias autoridades de supervisão estrangeiras consideram que a oferta, através da *Internet*, de serviços ou de instrumentos provenientes do estrangeiro é classificada como tendo lugar sobre o seu território quando esta oferta é endereçada ou posta à disposição de investidores no referido território. Quando da apreciação desses critérios, procura-se determinar se aspectos específicos desse país são visados (língua utilizada, preços expressos na moeda desse país, indicação de moradas locais de contacto), se as transacções ou serviços são efectivamente realizados através do *website* e se os investidores locais são atraídos por *e-mail* ou por outras técnicas de comunicação.

8. A instituição deve pois, previamente, definir claramente os seus objectivos comerciais e verificar, quando se dirige a clientes do território de outro Estado, através do *site* na *Internet*, se cumpre as regras desse Estado. Para evitar que as suas iniciativas sejam mal compreendidas em países não visados, a instituição deve tomar uma ou várias das medidas de precaução seguintes:

   a) Mencionar no seu *website* que o mesmo se dirige aos investidores de uma zona geográfica determinada, para a qual a instituição se encontra devidamente autorizada pelas autoridades do país em causa;
   b) Verificar se o conteúdo do *website* ou de qualquer outro instrumento de promoção não é incompatível com a zona geográfica visada (por exemplo se o *website* não se dirige a investidores britânicos, não devem ser mencionados endereços no Reino Unido, nem preços em GBP);
   c) Proteger e controlar o acesso ao *site* prevendo a utilização de palavras chave para a totalidade ou para parte do *site*, devendo estas palavras ser comunicadas apenas a pessoas que façam parte do grupo alvo;
   d) Tomar contacto com as autoridades de controlo locais tendo em vista assegurar que o *website* se encontra em conformidade com a legislação do país em causa.

Anexo: Check-list

Este anexo enumera uma série de aspectos que requerem uma atenção particular, assim como um conjunto de recomendações no domínio da organização e do controlo interno das instituições que oferecem ou prestam serviços através da *Internet*.

a) <u>Definição da política relativa aos serviços *Internet*</u>

Para definir as suas políticas, a administração da instituição deverá levar em linha de conta os seguintes aspectos:

1) *Definição da política geral, financeira e comercial*: importância da oferta de produtos e serviços através da *Internet* na oferta geral de serviços e produtos da instituição; estratégia e situação desta oferta relativamente à concorrência, exame das necessidades e expectativas dos clientes; natureza e origem dos clientes alvo1; influência da oferta através da *Internet* sobre a rede de retalho; estrutura tarifária; orçamento e afectação de recursos humanos2; influência possível da actividade desenvolvida através da *Internet* sobre a estrutura da instituição e sobre o seu grau de adequação de fundos próprios; forma e conteúdo do *website*; ligação ao *website* da autoridade de supervisão; referência aos sistemas de garantia de depósitos e de indemnização dos investidores.
2) *Fixação das opções técnicas e da política sobre o plano da segurança*: escolha do modelo e dos sistemas; escolha da entidade que irá assegurar o desenvolvimento e a manutenção dos sistemas, quer recorra a estruturas internas ou a entidades especializadas externas; estabelecimento de uma planificação para o desenvolvimento e para a entrada em produção das novas aplicações (ciclo de vida das aplicações, e procedimentos de teste antes da entrada em produção de novos módulos).
3) *Gestão de riscos*: identificação dos riscos, procedimentos para reporte dos riscos à administração e o seu acompanhamento por parte daquele órgão; gestão dos riscos informáticos e compatibilização dos novos sistemas com a infra-estrutura informática existente; elaboração de políticas de segurança adequadas ou adaptação das existentes; estabelecimento de procedimentos escritos para as operações autorizadas3 e fixação de limites por investidor, por operação, por unidade de tempo; designação dos responsáveis dentro da instituição (administração, órgão operacional) pela colocação em curso da política e pelo funcionamento diário do *site*, nomeadamente no que se refere ao seu acesso e ao seu funcionamento, bem como para o exercício do controlo das operações4; introdução de procedimentos e de controlos internos para visar ou aprovar a correspondência electrónica entre os funcionários da instituição e o público; estabelecimento de procedimentos de controlo interno e de integração das operações *Internet* no plano de auditoria;
4) *Exame e controlo das implicações e riscos jurídicos*, nomeadamente no que se refere às relações com os clientes (compreendendo a política em matéria de protecção dos dados pessoais e da privacidade), com as contrapartes e os fornecedores de serviços; o uso, o registo e a protecção de marcas; a regulamentação das bolsas às quais é dado acesso ou às quais as operações são comunicadas;
5) *Determinação dos meios e procedimentos em matéria de conservação de dados*, constituição e conservação dos registos e dos suportes das transacções5 (relativamente às operações, às informações fornecidas6; aos *e-mails* e à correspondência enviada e recebida; aos dados pessoais recebidos); o carácter durável e inalterável desses registos, a sua disponibilidade e acessibilidade (interna e externa, como por exemplo pelas autoridades competentes); os procedimentos referidos devem abordar o modo e a duração da conservação dos dados relativos ao *site* e regular, nomeadamente, a conservação das versões sucessivas de um *website*, assim como as possibilidades de consulta dos registos relativos a todas as ofertas e operações efectuadas;

---

1 Se clientes profissionais ou não profissionais, investidores interessados em actividades de negociação ou em investimentos a mais longo prazo.

2 É importante saber se a instituição dispõe de capacidade financeira suficiente para desenvolver o projecto e para o sustentar.

3 Pode-se pensar em estabelecer limites relativamente aos instrumentos financeiros com os quais o investidor *Internet* pode operar, a frequência e a natureza das operações.

4 Se um *website* transaccional (por exemplo com uma gama de bolsas situadas com fusos horários diferentes) está aberto 24 horas sobre 24 e 7 dias sobre 7, devem ser tomadas medidas para exercer um controlo adequado durante os dias de fim de semana, de férias ou de fecho.

5 Certas autoridades de controlo aceitam que os dados sejam conservados em suporte electrónico na condição que, em caso de solicitação, eles possam ser impressos em papel no próprio dia.

6 Recomenda-se conservar, a título de prova, os conselhos fornecidos em matéria de investimentos através do *website*.

conservação dos dados relativos à identificação dos clientes (identificação por contacto presencial ou à distância); conservação dos documentos contratuais originais assinados pelos clientes; conservação dos dados relativos às interrupções que tenham afectado a prestação de serviços (data e duração, causas, consequências, medidas tomadas, reclamações,…).

b) <u>Enquadramento jurídico</u>

Para estabelecer o quadro jurídico da actividade exercida através da *Internet*, a instituição poderá tomar em consideração os elementos seguintes:

Fornecedor da tecnologia

1) No processo de escolha do fornecedor da tecnologia, a instituição deverá estar atenta à respectiva situação financeira, à sua reputação, à sua experiência, ao seu *Know-how*, aos resultados obtidos em projectos similares e ao seu programa de actividades, os quais devem oferecer garantias para o desenvolvimento da tecnologia acordada.
2) Delimitar as responsabilidades entre as partes, obter garantias para a continuidade da prestação de serviços (documentação, manutenções regulares, tempos de resposta em caso de falha, período de pré-aviso em caso de resolução do contrato de modo a que a instituição possa proceder à substituição atempadamente,…). A utilização, por terceiros, de dados dos clientes deverá ser objecto de especial atenção, face à legislação aplicável.
3) A eventual menção, através do *website*, do nome ou do logotipo do fornecedor ou do seu produto não pode induzir os investidores em erro quanto à identidade do prestador dos serviços financeiros e do fornecedor da tecnologia7.

Enquadramento contratual instituição - cliente

1) Prever uma troca de informações entre as partes antes da conclusão do contrato (informações centradas, nomeadamente, sobre os objectivos e a capacidade financeira do cliente, as condições gerais das operações e os riscos associados, as tarifas, a protecção da privacidade…).
2) Conveniência da utilização de códigos pessoais e de palavras chave.
3) Definir o objectivo do contrato: quais são os serviços de investimento e os serviços auxiliares fornecidos via *Internet* e quais os serviços excluídos.
4) Regular a responsabilidade da sociedade em caso de atrasos nos diferentes estados da execução das ordens, em casos de falhas ou de sobrecargas, quer estes problemas sejam imputáveis à instituição quer a terceiros.
5) Regular a responsabilidade no que se refere à integridade das comunicações (codificação, acessos não autorizados, protecção contra vírus).
6) Organizar a prova, entre as partes, da existência de um contrato e do seu conteúdo;
7) Organizar a prova, entre as partes, relativamente às operações introduzidas na *Internet* (força probatória dos movimentos electrónicos).
8) Estabelecer o perfil do cliente, aprofundar os seus conhecimentos em matéria de investimentos e sondar a sua capacidade financeira; fixar limites por cliente/operação/unidade de tempo em função do perfil estabelecido.
9) Definir as operações autorizadas, a sua frequência, a sua natureza e a cobertura requerida;
10) Estipular que, em princípio, o cliente (que não seja uma outra instituição financeira autorizada) não pode, via o serviço em linha, receber ou executar ordens de outros investidores, não conhecidos da instituição8.
11) Definir a utilização das contas (transferências, pagamentos, …).
12) Definir as modalidades de comunicação de documentos9.

---

7 Torna-se conveniente, por exemplo, evitar que o nome comercial e o logotipo do sistema de transmissão de ordens assim como a apresentação do fornecedor deste sistema sejam postos em evidência sobre o *site* da instituição de modo a que o visitante creia que o fornecedor é igualmente o prestador dos serviços financeiros.

8 Dada a informação oferecida por certos sistemas *on-line* de negociação de títulos, existe o perigo que certos clientes *Internet* utilizem a sua conta e as suas facilidades para executar igualmente ordens de terceiros. Tais contas podem ser detectadas através de uma análise da frequência e do volume das operações, pela constatação do facto de que várias transacções são efectuadas no mesmo dia para o mesmo instrumento e no mesmo sentido.

9 Se estes documentos são enviados por *e-mail*, pode ser útil prever procedimentos de acusação de recepção. Para dispor de um meio de controlo suplementar, é sugerido o envio de certos documentos por correio (notas de suporte das operações, extractos).

13) Precisar o direito aplicável ao contrato.

c) <u>Aspectos técnicos e segurança</u>

Relativamente à segurança podem ser referidos os seguintes pontos:

1) Garantir a segurança da sua própria infra-estrutura informática impedindo todo o acesso a pessoas desconhecidas /não habilitadas.
2) Aplicar as medidas de precaução adaptadas ao contexto tecnológico actual (noutras palavras, devem existir garantias de actualização permanente com a melhoria tecnológica disponível).
3) Regular a atribuição e a utilização de palavras chave (integridade dos ficheiros de clientes, fluxos de informações);
4) Assegurar a integridade operacional do sistema: fiabilidade, capacidade suficiente para evitar sobrecargas ou falhas em "horas de ponta" ou em caso de elevada volatilidade dos mercados, planos de contingência e de *backup*, possibilidade de utilização, em caso de falha, de meios de comunicação alternativos com o envio de mensagens aos clientes precisando, se possível, a duração da interrupção dos serviços, pessoal qualificado para tratar as comunicações *Internet* e as instruções de negociação.

A instituição poderá mandar executar, periodicamente, testes por especialistas externos, obtendo certificados de aprovação que ofereçam aos clientes do *site* um certo número de garantias, por exemplo, no que se refere à integridade das transacções e à segurança.

d) <u>Aspectos operacionais</u>

No que se refere ao funcionamento de um *site* transaccional, os pontos seguintes são importantes:

1) Fornecer uma formação adequada aos colaboradores da instituição que utilizam (ou são susceptíveis de vir a utilizar) as aplicações *Internet*.
2) Implementar e controlar os critérios de validação das instruções transmitidas e prever um acompanhamento adequado das transacções realizadas pelo cliente a fim de identificar as operações anormais.
3) Implementar sistemas de análise para detectar operações que possam estar ligadas ao branqueamento de capitais.
4) Efectuar controlos aos diferentes estados de execução e tratamento de uma ordem, para permitir resolver atempadamente os eventuais problemas causados pelas validações externas e internas, a anulação ou a modificação pelo investidor de ordens ainda não executadas, a expiração das ordens quando o título sofre uma intervenção técnica ou financeira, a execução e a eventual anulação da execução de ordens, o envio dos documentos de suporte electrónicos com aviso de recepção e o seu envio pelo correio;
5) Controlar a informação no *website*: esta informação deve responder às mesmas condições que a informação, as brochuras e a publicidade que o intermediário difunde pelos canais tradicionais.
6) Relativamente à utilização de *links*10 no *website* da instituição financeira, examinar a conformidade destas ligações, a sua oportunidade, os procedimentos de declaração e as suas implicações ao nível da responsabilidade da instituição.
7) Examinar a utilização, por terceiros, de *links* ao *website* da instituição: um terceiro mal intencionado pode, por exemplo, tentar criar para ele próprio uma certa credibilidade estabelecendo ligações a *websites* de instituições reconhecidas e reputadas, prática apelidada de "branqueamento de reputação".

10 Os *links* podem ser colocadas à saída do *website*, por forma a chamar a atenção do investidor que deixou o *website* da instituição e que entra, eventualmente, num ambiente não regulamentado.