INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Desenvolvimento de Plataformas Multicanal

ANDRÉ TIAGO NUNES CARVALHAS
Outubro de 2016

POLITÉCNICO
DO PORTO

Desenvolvimento de Plataformas Multicanal

Internet & Mobile Banking

André Tiago Nunes Carvalhas

Dissertação submetida ao Instituto Superior de Engenharia do Porto
para a obtenção do grau de
Mestre em Engenharia Informática

Orientadores

Prof. Doutor Jorge Pinto Leite
Departamento de Informática – ISEP

Prof. Doutor Constantino Martins
Departamento de Informática – ISEP

Eng. Rui Pinto
ITSector - Sistemas de Informação S.A.

Instituto Superior de Engenharia do Porto

Porto, 23 de Outubro de 2016

Nas grandes batalhas da vida
o primeiro passo para a vitória
é o desejo de vencer.
Mahatma Gandhi

Agradecimentos

Um especial agradecimento aos meus pais, por me apoiarem incondicionalmente nesta etapa e por não me deixarem nunca desistir dos meus sonhos, mostrando-me o caminho a seguir. À minha irmã, Carina, pelo apoio e pela amizade. Obrigado por demonstrares que as dificuldades podem ser ultrapassadas. Ao pequeno Duarte, que apesar de tão pequeno é já um grande pilar na minha vida, ajudando-me a ultrapassar os momentos mais complicados de todas as caminhadas.
Aos orientadores, Constantino Martins, Jorge Pinto Leite, por toda a ajuda no desenvolvimento do projeto.
Ao Rui Pinto, por toda a ajuda fornecida na construção da solução e por todo o *know-how* fornecido.
À minha namorada, Mizé. Sem ela este projeto não teria acontecido. Por todo o seu apoio, carinho, amor, um especial agradecimento.
Aos meus amigos Carlos, Vanessa, Andreia, André, Rita, Ana e Eduarda por todos os momentos de diversão e pela forte amizade que permitiram construir.
Aos amigos ITSector, pelo bom ambiente de trabalho criado e pelo apoio na realização do projeto.
Aos meus avós, que embora não estejam cá, foram concerteza importantes nesta jornada.
À restante família e amigos por estarem presentes.

Resumo

A Internet causou uma revolução em grande parte dos processos dos bancos, criando oportunidades e gerando necessidades até então desconhecidas. Os Sistemas de Informação, ferramentas indispensáveis para uma gestão moderna das actividades bancárias, também foram influenciados pela evolução constante da tecnologia e as facilidades oferecidas para a popularização do uso da Internet. Rumo a uma crescente necessidade de modernização, agilidade, eficiência, eficácia e segurança que são exigidos das actividades bancárias, actualmente, a tecnologia da Web é exibida como uma opção viável para melhorar o desempenho das entidades bancárias.

Esta dissertação procura colmatar as necessidades sentidas pelo Banco Poupança e Crédito, através do desenvolvimento de uma plataforma de Internet Banking com um impacto considerável no quotidiano do cliente que traduza o aumento de fidelidade e de angariação de clientes.

Os objetivos propostos podem ser sintetizados no estudo de normas de segurança a aplicar, desenvolvimento do Internet Banking, disponibilização de serviços para consumo no desenvolvimento de aplicações móveis e ainda o desenvolvimento de uma plataforma de gestão de contratos.

A plataforma desenvolvida foi inserida no mercado angolano, onde tem tido uma aceitação elevada. Têm sido, desde então, registados aumentos significativos de clientes a aderir ao serviço, atestando assim a qualidade da plataforma nos principais fatores de satisfação: lista de operações disponíveis, inovação e segurança.

Palavras-Chave: Internet; Banco; Internet Banking; Multicanal; Segurança.

Abstract

Internet has caused a revolution in many processes of the banks, creating opportunities and necessities that were not known before. Information systems, fundamental tools in the day to day activity of banks were also upgraded due to improvements in the technology of those and the increasing use of Internet by the consumers.
With a new demand for more agility, efficiency,security and modernization, banking has relied on web technology to improve its performance.
This dissertation tries to tackle the necessities felt by Banco PoupanÃ§a e CrÃ©dito by creating a Internet Banking platform with a significative impact in the day to day of its client with the aim of translating that into an increasing fidelity and to attract new customers. The established objetives can be sintetized in the study of security measures to apply, Internet Banking development, disponibilization of services for the development of mobile apps and of a platform of contract management.
This platform was put to the test in the Angolan market where it was received with enthusiasm. Since then it had an increase of customers using this service whom were very happy with some of its features : Operations available to use, Innovation and Security.
Keywords: Internet; Bank; Internet Banking; Multichannel; Security

Conteúdo

Lista de Figuras

Lista de Tabelas

Acrónimos e Símbolos

APP	Aplicações Móveis
ATM	Terminais Multibanco
BMA	Banco Millennium Atlântico
BPC	Banco Poupança e Crédito
CLR	*Common Language Runtime*
CSRF	*Cross Site Request Forgery*
DLI	Documento de Liquidação de Impostos
DMZ	*DeMilitarized Zone*
DNS	*Domain Name System*
DSE	Direção de Pagamentos e Serviços Eletrónicos
DWR	*Direct Web Remoting*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
EDM	*Entity Data Model*
EF	*Entity Framework*
EMIS	Empresa Interbancária de Serviços
EMP	*Emerging Market Payments*
ESB	*Enterprise Service Bus*
EV	*Extended Validation Certificate*
FTP	*File Transfer Protocol*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol*
IB	*Internet Banking*
IBAN	*International Bank Account Number*
IP	*Internet Protocol Address*
IVR	*Interactive Voice Response*
JIT	*Just In Time*
JSON	*JavaScript Object Notation*
JVM	*Java Virtual Machine*
LINQ	*Language Integrated Query*
MSMQ	*Microsoft Message Queue*
NIB	*Número de Identificação Bancária*
ORM	*Object-relational Mapping*

REST	*Representational State Transfer*
SGBD	Sistema de Gestão de Bases de Dados
SMS	*Short Message Service*
SQL	*Structured Query Language*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*
TI	Tecnologias de Informação
UI	*User Interface*
VPN	*Virtual Private Network*
WCF	*Windows Communication Foundation*
XML	*eXtensible Markup Language*
XSS	*Cross-Site Scripting*

Capítulo 1

Introdução

Para todo e qualquer banco é essencial disponibilizar aos seus clientes consultas e operações eletrónicas nas suas contas bancárias da forma mais simples e amigável possível.
As plataformas utilizadas podem ser variadas, desde as caixas multibanco (doravante chamadas ATM) através de serviços de Internet / mobile banking ou mesmo através de serviços de SMS banking.
Num país grande e em constante evolução, como é o caso de Angola, local onde será instalada a plataforma, é necessário existir um serviço que possa cobrir estas necessidades. A inexistência deste pode acarretar a perda de clientes assim como a não abertura de inúmeros balcões que, consequentemente, podem contribuir para a não expansão do banco no mercado em que está inserido.
É também necessário ter em conta que Angola é considerado um país com algum nível de corrupção (International 2016). O seu índice de corrupção, aliado ao facto de ser um país que peca na inovação dos serviços que dispõe, obrigam a disponibilização de um serviço que seja confortável para o utilizador final, fazendo com que este seja seguro, inovador e apelativo.
Com a proliferação de equipamentos móveis, importa prever que o acesso ao Internet Banking possa ser multiplataforma. Assim, as facilidades de acesso alargam-se dos sistemas habituais para outros dispositivos, como tablets. A abertura a este tipo de dispositivos permite (ou quase obriga) ao planeamento e/ou disponibilização de aplicações (app) disponíveis para as principais famílias de dispositivos móveis.

1.1 Motivação

Após a identificação de vários ataques à plataforma de Internet banking implementada e detida pelo BPC (Banco de Poupança e Crédito) e após a perceção da deficiência que esta apresenta no que toca ao número de operações a que os seus clientes têm acesso, foi decidido pela Direção de Pagamentos e Serviços Eletrónicos (DSE) do banco que deveria ser desenvolvida uma nova plataforma de Internet Banking (IB) para disponibilização aos clientes.
É ainda importante que com o desenvolvimento da nova plataforma todos os segmentos de cliente sejam abordados, de forma a manter a fidelização de clientes particulares ou empresas uma realidade, o que ajudará o banco no seu processo de crescimento e afirmação no mercado angolano.

1.2 Objetivos

O objetivo principal prende-se pelo desenvolvimento de uma plataforma multicanal, que, ligada ao core bancário, permita ao cliente efetuar transações sem ser necessária a sua presença no balcão, ou seja, um IB. Sabendo da existência de dois tipos de cliente será necessário o desenvolvimento de uma plataforma orientada para clientes particulares e uma outra orientada para empresas.
Como objetivos específicos desta dissertação pretende-se:

- Analisar e sistematizar o problema anteriormente descrito de forma mais pormenorizada e, em particular, identificar as limitações da plataforma multicanal, ligadas ao core bancário;
- Descrever e sistematizar os processos de plataformas multicanal; transações ligadas ao core bancário ou outros, analisando os problemas de segurança associados;
- Identificar, descrever e sistematizar as abordagens existentes que, de forma isolada ou em conjunto, podem contribuir para suprir as limitações identificadas;
- Identificar normas de segurança;
- Desenvolvimento de um backoffice da aplicação para gestão de contratos de adesão, estatísticas, gestão de equipas e utilizadores, entre outros;

- Desenvolvimento da plataforma multicanal ligada ao core bancário;
- Disponibilização de serviços a serem consumidos pelas plataformas Mobile;
- Realizar um estudo de caso que demostre a validade da abordagem e a utilidade da ferramenta desenvolvida.

Esta dissertação procura, em primeiro lugar, o estudo de vários aspetos de segurança a ter em conta no desenvolvimento de uma solução IB. Na área da informática, serão estudados termos como phishing, malwares, SQL Injection, assim como as respetivas soluções de prevenção para cada um dos casos.
Para além deste estudo de normas de segurança, procura-se aplicar os conhecimentos adquiridos para a construção de uma solução que pode ser uma mais valia no mercado bancário Angolano. É expectável que esta seja uma solução inovadora, segura, fiável e que traga ao cliente conforto de utilização.

1.3 Metodologia

Definidos os objetivos, numa primeira instância será necessário analisar o valor que uma plataforma como um IB pode trazer para o BPC. Estando analisada esta variável, torna-se necessário estudar todos os fatores de segurança que podem prejudicar o bom funcionamento da solução, ou seja, analisar os métodos de ataque a sites expostos na Internet, assim como os respetivos métodos de prevenção.
Após análise e desenvolvimento de requisitos, desde a lista de operações a disponibilizar até à interface esperada, pode ser realizada uma avaliação do resultado obtido através da realização de inquéritos e de estudo estatístico do número de adesões e operações.

1.4 Organização do documento

O presente documento está dividido em 6 capítulos. O presente capítulo apresenta uma breve introdução da temática da dissertação. O segundo capítulo apresenta uma análise de valor do projeto, avaliando o impacto de um IB no desenvolvimento de uma entidade bancária e a apresentação do modelo Canvas orientado ao projeto. O terceiro capítulo apresenta um estado da arte, sendo iniciado pela apresentação de vários conceitos de segurança que devem ser tidos em conta quando é proposto o desenvolvimento de um Internet banking, sendo dividido entre métodos de ataque

e métodos de prevenção. Ainda neste capítulo, são analisadas duas plataformas Internet Banking instaladas no mercado angolano.A primeira é a solução que o BPC tinha implementada no início do projeto e a segunda, a solução do Banco Millenium Atlântico (BMA).
o quarto capítulo descreve o design solução, apresentando a lista de operações a realizar / disponibilizar no BPCNet, as funcionalidades presentes em Backoffice e também as entidades externas que devem participar no projeto de forma a cumprir os objetivos.
O quinto capítulo demonstra a implementação do projeto, evidenciando a arquitetura do sistema aplicacional, as ferramentas utilizadas para o desenvolvimento, algumas das interfaces do sistema e ainda as metodologias de segurança adotadas.
Por fim, o capítulo 6 apresenta os resultados de uma avaliação feita à plataforma.

Capítulo 2

Análise de Valor

Ao longo deste capítulo será efetuada uma análise de valor do projeto, indicando quais as expectativas no desenvolvimento deste. Será ainda feita uma análise do projeto utilizando o Modelo Canvas.

2.1 Impacto de um Internet Banking numa entidade bancária

Segundo Porter (2001), uma entidade apenas se consegue distinguir das concorrentes inseridas no mercado apresentando uma vantagem competitiva sustentável, que pode ser decorrente de uma eficácia operacional ou de um ótimo posicionamento estratégico. A Internet, hoje em dia, apesar de ser uma ferramenta importante e poderosa (precisamente pela sua característica de sistema aberto) não provoca uma vantagem operacional à entidade. Esta afirmação é justificada pela utilização de arquiteturas de sistemas e ferramentas de desenvolvimento que permitem que as aplicações criadas/compradas por uma entidade possam ser facilmente copiadas pelos concorrentes.

Desta forma, se uma empresa não consegue, apenas com a disponibilização de novas ferramentas, manter uma eficácia operacional superior aos seus competidores, não conseguirá sustentar a sua vantagem competitiva. Como resultado, deve não só utilizar este tipo de ferramentas, mas também competir no mercado de uma forma distinta e inovadora, ou seja, escolher um conjunto de atividades para fornecer uma proposição única de valor aos clientes.

Para Parasuraman and Grewal (2000), a qualidade dos serviços aumenta o valor percebido pelo cliente. Para além disto, apresentam ainda 5 boas razões para julgar

a qualidade de serviços: confiança, disponibilidade; garantia; empatia; tangibilidade. Aqui, a confiança no serviço é a principal dimensão que ajuda o cliente a ver um maior valor neste. Os autores referem ainda que a perceção de valor é uma variável de construção dinâmica, onde a ênfase de cada componente das 5 acima referidas varia no ciclo temporal do relacionamento do cliente com a entidade.
A perceção de valor pelo cliente pode ser dividida em 4 componentes:

- Valor da aquisição: estes são os benefícios monetários que o cliente acredita que irá obter ao comprar um produto / serviço;
- Valor da transação: prazer que o cliente obtém ao realizar uma boa transação;
- Uso: diretamente relacionado com a utilidade do produto / serviço;
- Resgate: benefício residual na troca, final de vida ou término do serviço;

Para Oliver (1999), o que também precede a fidelização de um cliente é a satisfação que este tem ao utilizar o produto. Ainda de acordo com Oliver, a satisfação não pode ser automaticamente traduzida em fidelização, devendo ser considerada um passo necessário para a sua formação. A fidelização de um cliente apenas é atingida de uma forma completa quando houver outros fatores envolvidos, tais como determinação pessoal e ligação social. Para que a satisfação afete a fidelização, esta deve ser frequente e cumulativa.
Tomiuk and Pinsonneault (2001) ajudaram com estudos que permitem estabelecer relações entre fidelização de clientes e indicadores de performance financeira. Precisamente no estudo sobre o impacto do comércio eletrónico na fidelização do cliente, relatam que o canal eletrónico pode ser tanto prejudicial como benéfico, tendo em conta as preferências do cliente. Por norma, se um cliente está interessado em estabelecer um relacionamento pessoal com os funcionários de uma agência bancária, a construção de uma ferramenta eletrónica pode prejudicar a fidelização do cliente. Por contrário, se o cliente procura a relação eficácia / eficiência do serviço bancário, uma plataforma eletrónica pode muito bem tornar-se em algo que fideliza ou cativa um cliente. Como resultado, a fidelidade do cliente é afetada pela performance das tecnologias aplicadas, da gama de serviços oferecidos através dos canais eletrónicos e ainda pelos fatores de inovação tecnológica apresentados.
Meuter (2000) realizaram estudos sobre a utilização, por parte dos clientes, de tecnologias de self-service providenciadas por entidades bancárias, tais como: telefone, contact centers, Internet e quiosques. O resultado foi claro: o nível de satisfação

do cliente é diretamente proporcional ao auxílio prestado por estas tecnologias em várias situações, como por exemplo:

1. Obtenção de dinheiro num ATM em períodos de fim-de-semana (em que as agências bancárias estão fechadas);
2. Dificuldade na deslocação a uma agência do banco por incompatibilidade com o horário que praticam, dificuldade no acesso, etc.;
3. Funcionamento correto do serviço.

A relevância do comércio eletrónico pela Internet para os bancos é apresentada no estudo de Zilber and Caçador (2003). Neste artigo são identificadas algumas iniciativas dos bancos para dinamização das novas tecnologias em sistemas bancários, tais como:

1. Apresentação de novas funcionalidades e novos produtos no IB;
2. Permitir acesso ao IB através da utilização de smartphones e tablets;
3. Cartões de crédito eletrónicos;
4. Envio de extratos bancários por correio eletrónico.

Analisando agora o impacto do IB na fidelização dos clientes, Diniz (2000) indica que a implementação de serviços bancários pela Internet tem várias vantagens, entre elas: redução de custos, utilização do próprio serviço como canal de promoção e divulgação e também a melhoria do relacionamento com o cliente.
A utilização da Internet para a realização de operações bancárias pode levar a uma redução de custos para a entidade bancária, por exemplo: o custo da realização de uma operação na Internet pode traduzir-se em apenas 1% do custo que o banco teria ao executar a mesma operação numa agência. No entanto, a redução de custos causada pela possível substituição do canal agência bancária pelo canal Internet pode entrar em conflito com o pouco desenvolvimento do país e com a dificuldade que a população tem em aceder a novas tecnologias (Zilber and Caçador 2003). Assim, o banco deve não só optar pela redução de custos, mas também pela melhoria da relação com os clientes. Ao disponibilizar um IB, o cliente fará as suas operações em casa e frequentará as agências com menos regularidade, permitindo aos funcionários destas a prestação de um melhor serviço ao cliente (melhoria da relação). Torna-se também mais fácil para o funcionário da agência fazer a captação de clientes para a

plataforma online.
Albertin (1999) defende que a relação cliente banco pode sofrer melhorias quando são disponibilizados Internet Bankings e defende ainda que estas plataformas devem ser utilizadas de forma a apurar variadas informações sobre os clientes. Desta forma, seria facilitada a personalização de produtos e serviços bancários. Os fatores que mais influenciam a satisfação dos clientes que utilizam comércio eletrónico estão apresentados seguidamente e são baseados nos estudos de Turban (2000), Szymanski and Hise (2000) e ainda Ramos and Costa (2000).
Segundo Turban:

- Qualidade da plataforma online:
  - Segurança;
  - Confiabilidade;
  - Usabilidade;
  - Velocidade de operação;
  - Conteúdo;
- Serviços disponíveis ao cliente;
- Atratividade de preços;
- Logística de Suporte.

Na opinião de Szymanski e Hise:

- Conveniência;
- Oferta de produtos;
- Informação de produtos;
- Projeto da plataforma online;
- Segurança Financeira;

Por fim, de acordo com Ramos e Costa:

- Performance do IB:
  - Rapidez de carregamento;
  - Funcionalidade das transações;
  - Informação sobre produtos e serviços.

2.2 Apresentação de Modelo Canvas

Para a plataforma proposta e sabendo desde já a importância de um Internet banking para os clientes de um banco, será apresentado um modelo Canvas (figura 2.1) que fará o resumo de múltiplas variáveis do projeto.

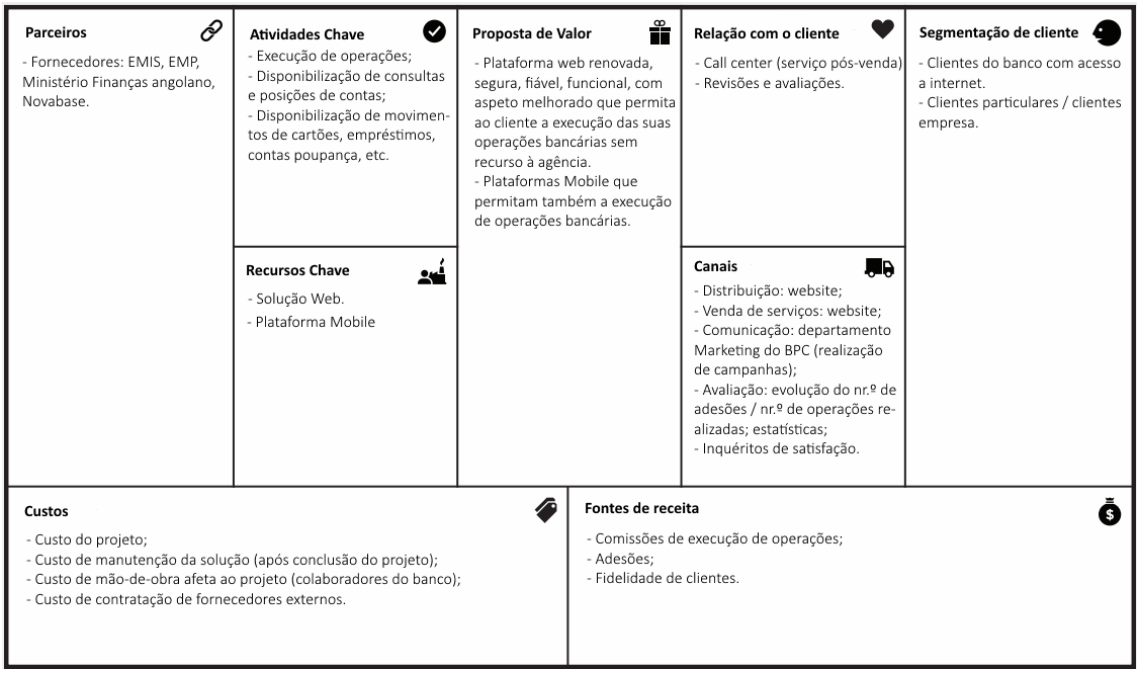


Fig. 2.1: Modelo Canvas do Projeto

O objetivo principal do projeto é coincidente com a proposta de valor. É desejado que no final da implementação seja disponibilizada uma plataforma *web* renovada, segura, fiável, funcional, com aspeto melhorado e que permita ao cliente a execução das suas operações bancárias sem recurso à agência. É ainda desejado que sejam disponibilizadas plataformas mobile, para dispositivos móveis, utilizadas com a mesma finalidade da plataforma browser.

As atividades chave serão então a execução de operações, a disponibilização de consultas / posições de contas e ainda a disponibilização de movimentos de cartões, empréstimos, contas poupança, etc. Estas atividades só serão possíveis com a intervenção de parceiros que são as entidades que fornecem os serviços. A EMIS (Empresa Interbancária de Serviços) fornecerá serviços para pagamentos de serviços, carregamentos, recargas e pagamentos parametrizáveis. A EMP (Emerging Market Payments) fornecerá informações, detalhes, movimentos e cancelamentos de cartões de crédito e débito. O Ministério das Finanças Angolano é responsável por fornecer serviços para pagamentos ao Estado (DLI - Documento de Liquidação de

Impostos). Por fim, a Novabase fornecerá os serviços que permitem a ligação ao core bancário através da plataforma ESB (Enterprise Service Bus).
Todos estes serviços estarão disponíveis para duas linhas de clientes, que se podem dividir em clientes particulares e empresas que possuam acesso a serviços de Internet. A disponibilização da solução *web* e da plataforma mobile podem ser feitos por diversos canais, sendo que o canal de distribuição e de venda de serviços são coincidentes e traduzem-se no na solução *web* e nas app disponibilizadas. O canal de comunicação está a cargo do departamento de marketing do BPC através da realização de campanhas. A avaliação do projeto será possível através da evolução do número de adesões / operações, apresentação de estatísticas e realização de inquéritos de satisfação de inquéritos ao cliente final.
O projeto tem ainda custos associados, como por exemplo:

- Custo do projeto;
- Custo de manutenção da solução (após conclusão do projeto);
- Custo de mão de obra afeta ao projeto (colaboradores do banco);
- Custo de contratação de fornecedores externos.

As receitas do projeto podem ser encontradas nas comissões de execução de operações, na cobrança de adesões ao serviço e ainda na maior fidelidade de clientes, que após se encontrarem satisfeitos com a aplicação a utilizarão de forma mais intensiva.

2.3 Conclusão

A inovação tecnológica e o grande avanço que a Internet teve nas últimas décadas revolucionaram o sistema financeiro. Isto leva as entidades bancárias a optarem, cada vez mais, por atrair os seus clientes para ambientes virtuais, nomeadamente IB's, de forma a eliminar em muitos momentos a presença física de clientes na agência.
A inovação, segurança e quantidade de operações disponíveis para realização são os principais fatores de satisfação de um cliente que utilize um IB. Desta forma, podemos definir a proposta de valor do projeto como sendo: Implementação de uma plataforma *web* renovada, segura, fiável, funcional, com aspeto melhorado e que permita ao cliente a execução das suas operações bancárias sem recurso à agência.

Capítulo 3

Estado da Arte

Ao longo deste capítulo serão apresentados conceitos e noções que é necessário ter em conta no desenvolvimento de uma plataforma de IB assim como alguns dos ataques mais efetuados às mesmas e respetivas formas de prevenção.
Para melhor análise e definição dos principais objetivos do projeto foram analisadas diferentes plataformas que apresentam o mesmo tipo de funcionalidades. Assim sendo, neste capítulo serão descritas as ferramentas BPCNet - IFM do Banco Poupança e Crédito e ainda a ferramenta Atlantico Directo do Banco Millennium Atlantico.

3.1 Métodos de ataque a Internet Banking

O aumento da utilização da Internet torna imediatamente consequente o aumento da utilização de serviços *online* e de acordo com uma análise feita pela Angola (2012) ao sector financeiro Angolano: *Serviços como o Mobile e o Internet Banking [...] começam a surgir de forma mais massificada e a ser cada vez mais requeridos e usados por diferentes segmentos de clientes.*
A relação entre o crescimento da Internet e o aumento do número de fraudes cometidas *online* existe e torna-se numa preocupação real quando estamos sobre a perspetiva de um Internet banking que, entre outras coisas, permite a um cliente executar a gestão do seu património dentro do banco.
A fraude utilizando Internet é definida como sendo a distorção intencional da verdade de um facto, com perspetiva de obtenção de lucro ilegal através da utilização de serviços de rede, como por exemplo *e-mails* ou páginas disponíveis em domínios de Internet. (Lau 2006)

Com o desenvolvimento exponencial e incontrolado da Internet e de todos os seus conteúdos foram surgindo especialistas na área que utilizam toda a sua experiência na execução de ações menos legais. Muitas destas pessoas são especialistas na execução de ataques à informação constantemente carregada nos ambientes visitados ou mesmo a informações armazenadas pelas próprias organizações ou utilizadores. Os mais conhecidos são os *hackers*, que utilizam vários métodos e tipos de ataque para atingirem os seus objetivos.
Os ataques descritos de seguida são alguns dos mais utilizados:

3.1.1 *Phishing*

O *phishing* é um termo criado para descrever as fraudes caracterizadas pelo envio de mensagens não solicitadas, isto é, são enviadas mensagens em que o remetente se faz passar por uma instituição conhecida, como um banco, empresa ou *site* popular. O objetivo da mensagem é induzir que o utilizador aceda a páginas falsificadas (por exemplo, uma simples página HTML com o mesmo *layout* que a página inicial de um Internet banking), páginas estas desenvolvidas com o intuito de obter os dados pessoais e financeiros dos utilizadores. Também é usado o termo *phishing* para descrever mensagens que induzem à instalação de código malicioso ou então mensagens que possuam formulários para preenchimento e envio de dados pessoais. (Lau 2006).

3.1.2 *Malware*

Os *malwares* podem ser encontrados em várias formas. Desde *vírus, worms, spywares, keyloggers, rootkits, backdoors*, cavalos de troia, etc.
O objectivo principal dos *malwares* é infiltrar dados ou mesmo espiar ou danificar computadores. Segundo Wendel (2011) são programas de computadores criados e instalados em sistemas computacionais.
Alguns dos *softwares* maliciosos existentes no quotidiano possuem a função de *sniffer*. Um *sniffer* por norma, fica alojado na memória de computadores ou servidores analisando todo o tráfego da interface de uma rede. Todas as informações, sejam estas originadas num servidor FTP (*File Transfer Protocol*), uma página de chat ou mesmo na introdução de um e-mail, são capturadas. Utilizando estas informações, todos estes dados são transformados em texto puro de forma a serem lidos (Freitas 2007).

3.1.3 *Pharming*

O *pharming* é um conceito relativamente recente no mundo das fraudes executadas em serviços de IB. (Lau 2010). A execução deste mecanismo é tão simples como realizar um redireccionamento da vítima para páginas falsas de instituições financeiras. Ao invés da utilização de *e-mails*, são utilizadas falhas de segurança dos serviços de DNS que resultam no acesso do utilizador às páginas disponibilizadas pelos bancos. Mesmo que o utilizador digite o endereço correto no *browser*, a falha no DNS (*Domain Name System*) provocará o redirecionamento para a página maliciosa (Lau 2010).

O ataque acontece quando o intruso descobre o IP (*Internet Protocol*) do servidor DNS e manipula a cache do servidor de DNS para que este devolva uma página errada ao cliente, mesmo tendo este consultado o endereço correto. A figura 3.1 ilustra o esquema de montagem de um ataque de *pharming*.

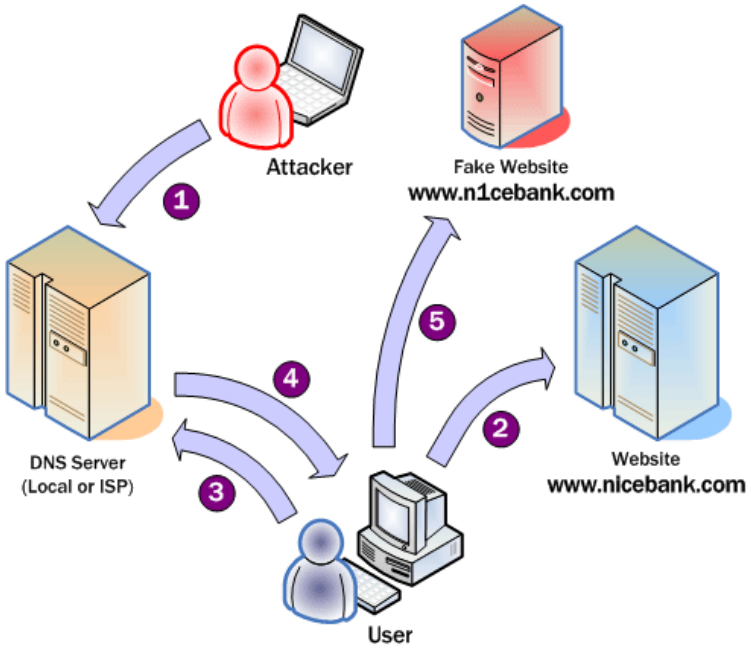


Fig. 3.1: Funcionamento do método de ataque *Pharming* (Fonte: http://features.en.softonic.com/6-tips-for-shopping-online-without-getting-scammed)

3.1.4 *SQL Injection*

Structured Query Language (SQL) é a linguagem quase universal das bases de dados utilizadas pela maioria das aplicações. Através do uso desta linguagem é permitido

o armazenamento, manipulação e recuperação de dados.
SQL Injection é por norma um ataque utilizado de forma a permitir a autenticação de um utilizador que não está habilitado ao uso da aplicação. A ideia generalista do *SQL Injection* é convencer a aplicação a executar código SQL que não é expectável em determinados momentos.
A não prevenção contra ataques de *SQL Injection* é algo que pode deixar as aplicações em grande risco, e podem contribuir para:

- Acesso e alteração de informações privadas / sensíveis;
- Perdas financeiras;
- Roubo de informações do cliente, como por exemplo, número de cartão de crédito.

Para melhor entendimento do termo *SQL Injection* é necessário haver um bom entendimento do tipo de comunicações que ocorrem entre o utilizador e uma aplicação *web* (Gadgil 2013). Estas comunicações são apresentadas na Figura 3.2.

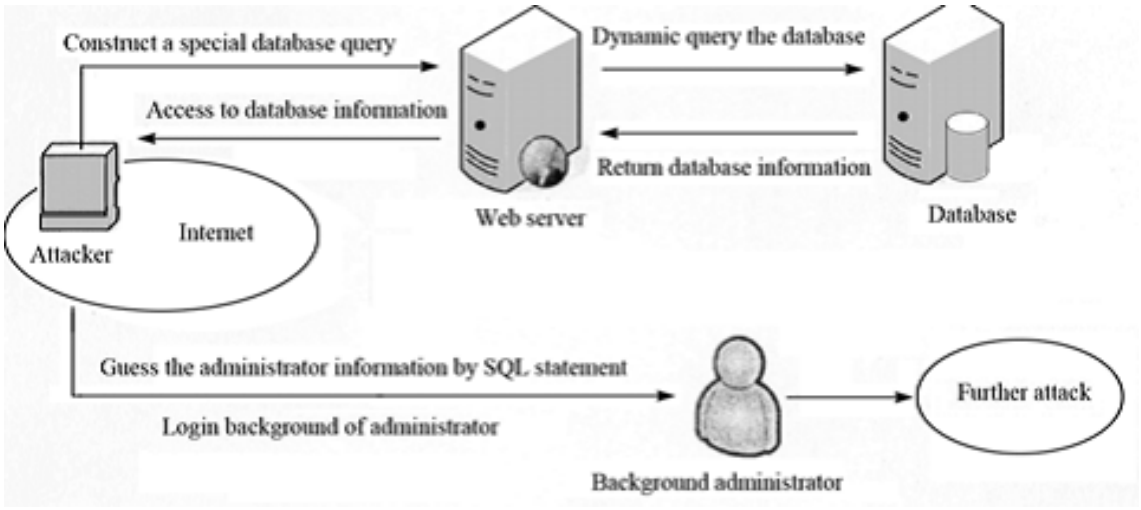


Fig. 3.2: Ataque por *SQL Injection* Fonte: Gadgil (2013)

3.1.5 *XSS- Cross-Site Scripting*

Um *cookie* é um pequeno pacote de dados enviado de um website para o browser do utilizador quando este visita o site. Cada vez que o utilizador visita o site novamente, o browser envia o cookie de volta para o servidor para notificar atividades

prévias do *user*. Os *cookies* foram designados para ser um mecanismo fiável de forma a que os sites visitados se recordem de informações da atividade do utilizador, tais como: palavras passe gravadas, itens adicionados a um carrinho de compras numa loja online, links que foram clicados anteriormente, entre outros.
Cross Site Scripting (XSS) é um dos ataques mais comuns a serem realizados em aplicações *web*. Este tipo de ataque é entendido como sendo um ataque à privacidade dos clientes de um determinado *site* que pode levar a uma rutura total de segurança, visto que os detalhes do cliente são roubados e podem ser manipulados. Estes ataques envolvem três partes intervenientes: o atacante, um cliente e o próprio *website*. O principal objetivo do ataque XSS é roubar os cookies do cliente, ou qualquer outra informação sensível, que possa identificar o cliente dentro o *website*. Com esta informação na mão, o atacante pode continuar a agir como o sendo o utilizador a interagir com o *site*.
Os ataques XSS ocorrem quando páginas geradas dinamicamente permitem ao utilizador o preenchimento de *inputs* que não estão corretamente validados. Isto permite que um atacante injete código *JavaScript* malicioso na página, permitindo a execução deste código enquanto o utilizador utiliza a aplicação. (Klein 2002)
Segundo Spett (2005), esta vulnerabilidade é normalmente vista em:

- Motores de busca que transmitem ao utilizador as palavras digitadas para pesquisa;
- Mensagens de erro que devolvem ao utilizador a string que continha o erro;
- Formulários que são preenchidos, onde os valores são depois apresentados ao utilizador;
- Fóruns Web que permitem aos utilizadores a publicação das suas próprias mensagens.

3.1.6 *Cross Site Request Forgery (CSRF)*

Os ataques CSRF permitem a simulação de ações de um utilizador num *site* (o *site* destino) a partir de um outro *site* (o *site* atacante). Normalmente estes ataques são usados de forma a executar ações escolhidas pelo atacante usando a sessão autenticada da vítima. Se a vítima estiver autenticada no site alvo, um atacante pode forçar o *browser* da vítima a executar ações no *site* do alvo. (Blatz 2011)
A figuras 3.3 e 3.4 ajudam a detalhar este tipo de ataques, comparando as ações

de um utilizador quando este visita um *website* com as ações executadas simultaneamente num ataque deste género.

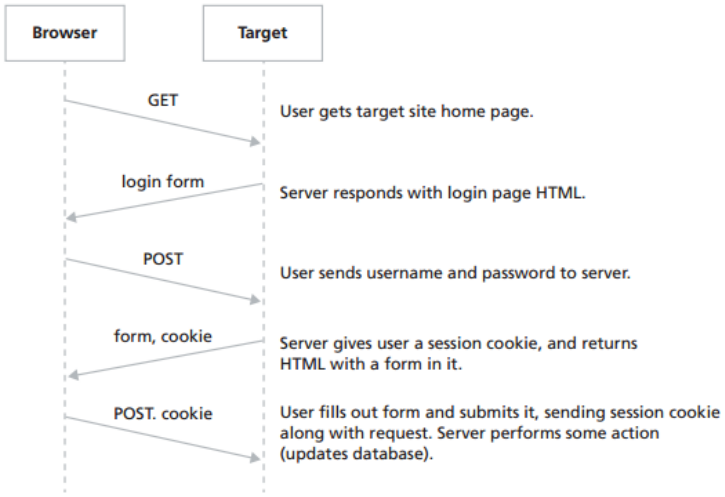


Fig. 3.3: Ações executadas na visita de um utilizador ao *website* alvo. Fonte: Blatz (2011)

Algumas das formas de prevenção aos ataques acima mencionados, vão ser descritos de seguida.

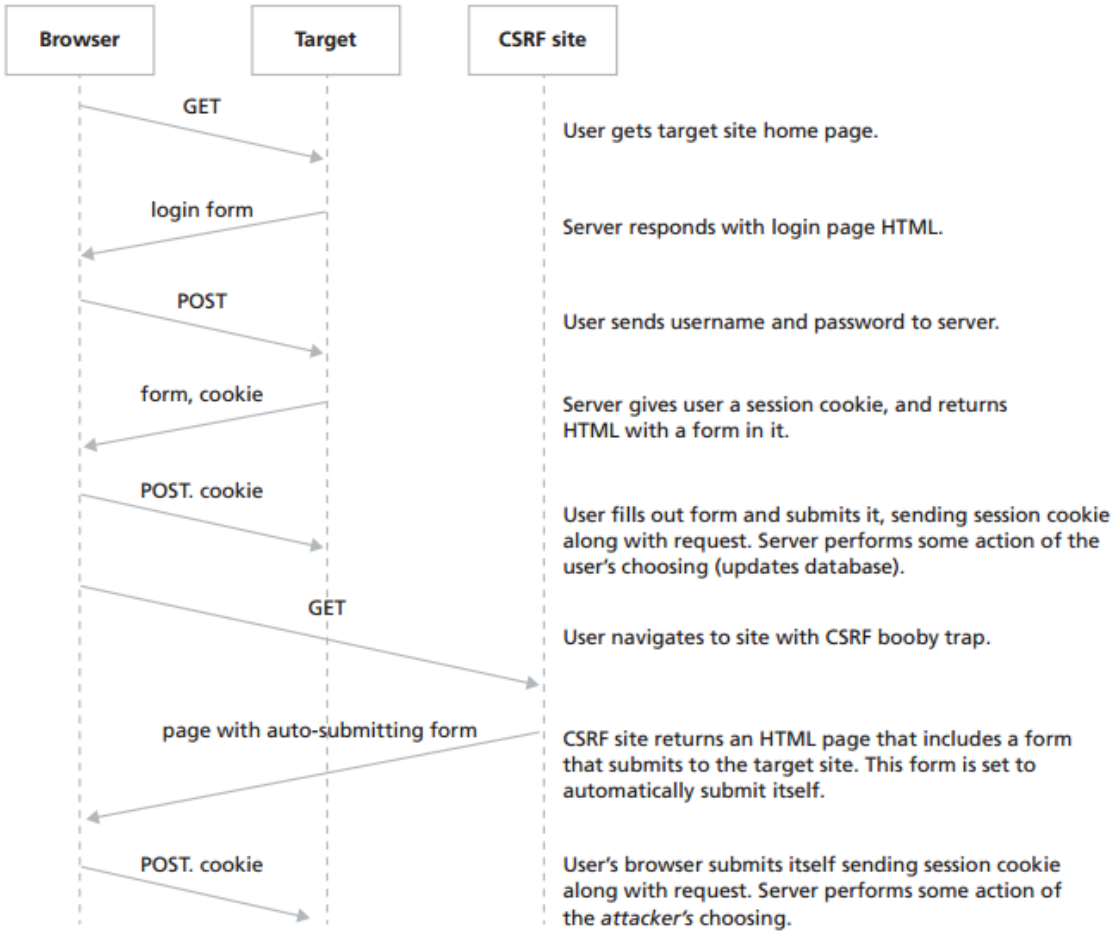


Fig. 3.4: Ações executadas num ataque CRSF. Fonte: Blatz (2011)

3.2 Métodos de prevenção de ataques

A prevenção de ataques a um Internet banking é uma responsabilidade repartida entre três camadas distintas que podemos facilmente identificar:

1. Camada Física;

2. Camada Lógica;

3. Camada Humana.

Tab. 3.1: Domínios de prevenção de ataques num Internet Banking.

Domínio	Funções / Tarefas	Camada
Arquitetura e modelos de segurança	• Definição da arquitetura e metodologia de segurança para proceder à sua implementação; • Definição da constituição do hardware da plataforma, servidores necessários, assim como as caraterísticas dos mesmos; • Escolha dos modelos de segurança.	Física
Sistemas de controlos de acesso	• Definição, monitorização e controlo dos procedimentos de acesso; • Definição da metodologia de acesso, isto é, tomada de decisão sobre os métodos de autenticação utilizados, podendo variar entre senhas, cartões matriz, SMS token, sistemas de autenticação biométricos, etc.	Física
Telecomunicações e Redes	• Prevenção de ataques, deteção de intrusos, correção de erros, de forma a mantar a comunicação confidencial, constantemente disponível e íntegra; • Definição de filtros de acesso (firewalls), portas de acesso; • Administração do uso dos protocolos de comunicação na rede (TCP/IP, SMTP, PPP, PAP).	Física
Desenvolvimento da aplicação	• Definição e gestão dos diversos tipos de software a utilizar, assim como a sua implementação; • Criação e gestão da base de dados.	Lógica

Criptografia	• Avaliação da segurança necessária para os vários tipos de funcionalidades; • Desenvolvimento de métodos de encriptação de dados; • Definição de certificados digitais	Lógica
Práticas de gestão de segurança	• Promoção da consciencialização e educação de práticas de segurança.	Humana
Segurança de operações	• Execução de auditorias aos registos de operações, monitoriza e resolve problemas.	Humana
Plano de continuidade e plano de recuperação	• Análise do impacto da plataforma no negócio; • Desenvolvimento de planos de contingência;	Humana

3.2.1 *DMZ (DeMilitarized Zone)*

A DMZ é considerada uma área intermediária entre a rede interna e externa, onde os servidores que recebem tráfego externo estão hospedados de maneira separada da rede interna de uma empresa. (O'Donnell 2002)
A principal função de uma DMZ é restringir, da melhor forma, possíveis danos causados por potenciais invasores. (O'Donnell 2002)
A DMZ permite que utilizadores externos acedam aos servidores localizados na rede de perímetro, evitando ao mesmo tempo o acesso à rede corporativa interna. Podemos então resumir o papel da DMZ como sendo uma rede tampão entre a rede externa e interna. (O'Donnell 2002)
A configuração de uma DMZ é realizada através do uso de equipamentos de Fi-

rewall, que vão realizar o controlo de acesso entre a rede local, a Internet e a DMZ. (O'Donnell 2002) Os equipamentos colocados na DMZ devem ser configurados de modo a funcionar com o mínimo de recursos possíveis ao oferecer um determinado serviço. Além disso, o comprometimento de um equipamento qualquer situado na DMZ não deve servir para o comprometimento de equipamentos e/ou serviços da rede interna, ou seja, qualquer tentativa de ataque deve ficar confinada aos equipamentos situados na DMZ. (O'Donnell 2002)

3.2.2 Certificados Digitais

Secure Sockets Layer (SSL) é um protocolo desenvolvido pela Netscape, que permite a transmissão segura de informações através da Internet. O SSL usa um sistema de criptografia que utiliza duas chaves para encriptar dados - uma chave pública conhecida de todos e uma chave privada ou secreta conhecida apenas pelo destinatário da mensagem. (Ristic 2014)

A qualidade da proteção dada pelo SSL depende inteiramente da chave privada, na qual as bases de segurança são fundadas, e o certificado, que comunica a identidade do servidor aos visitantes. (Ristic 2014)

É importante utilizar RSA 2048-bit ou ECDSA (*Elliptic Curve Digital Signature Algorithm*) de complexidade equivalente na criação de chaves privadas em todos os servidores. Chaves com esta força são seguras e devem continuar a sê-lo num período de tempo considerável. Se for necessário chaves maiores que 2048 bits podem considerar-se chaves ECDSA que tendem a ter melhores características de performance. (Ristic 2014)

Recomenda-se um certificado SSL EV (Extended Validation Certificate) pois fornece mais garantias ao utilizador final, na medida em que fornece mais informação relativamente à entidade responsável pelo website visitado. Informações como domínio, nome da entidade, localização, etc. podem ser consultados neste tipo de certificado.

Fig. 3.5: Identificação de um certificado digital SSL EV

Fig. 3.6: Identificação de um certificado digital normal

Suporte de protocolos

Segundo Ristic (2014), existem 5 protocolos na família do SSL/TLS (*Transport Layer Security*): SSL v2, SSL v3, TLS v1.0, TLS v1.1 e TLS v1.2. Destes:

- SSL v2 é inseguro e não deve ser usado;
- SSL v3 é muito antigo e obsoleto. Dado que faltam algumas funcionalidades chave e praticamente todos os clientes suportam TLS 1.0 ou melhor, não deve ser suportado o SSL v3 a menos que exista uma boa razão para tal;
- TLS v1.0 é ainda largamente seguro; não são conhecidos nenhuns problemas de segurança maiores quando usado com o protocolo HTTP. Quando usado com HTTP, com uma configuração cuidada, pode ser tornado praticamente seguro
- TLS v1.1 e v1.2 têm como problema a vulnerabilidade a ataques Poodle;
- TLS v1.2 deve ser o protocolo principal. Esta versão é superior pois oferece algumas funcionalidades importantes que não estavam disponíveis em versões anteriores do protocolo. Se a plataforma de servidores (ou qualquer dispositivo intermédio) não suportar TLS v1.2, deve ser planeado o upgrade rapidamente. Se o provedor de serviço de Internet não suportar TLS v1.2, deve ser pedido o upgrade.
  De forma a suportar clientes (browsers) mais antigos, deve continuar a ser suportado o TLS v1.0 e o TLS v1.1 nos próximos tempos.

3.3 BPCNet IFM (Banco Poupança e Crédito)

O IFM era a plataforma Internet Banking anteriormente existente no Banco de Poupança e Crédito (BPC).
O IFM é um serviço que permite ao cliente (após adesão) várias tarefas. De forma muito sumária o cliente pode:

- Ler e enviar mensagens ao administrador do sistema;
- Ver os detalhes, movimentos, saldo, extrato das últimas 20 transações e atividades das suas contas;
- Realizar transferências para as suas contas e para as contas dos seus benificiários;

- Ver o estado das transferências;
- Configurar a sessão;
- Alterar ID, Senha e Palavra Secreta;
- Contactar o banco.

Para que o cliente possa aceder ao referido serviço, deverá ter em sua posse os dados de acesso atribuídos pelo balcão.

3.3.1 Páginas de acesso

Dados de Acesso

Após habilitar o cliente o banco concede ao mesmo os dados de acesso ao serviço. O login na aplicação é feito através deste ecrã, que permite ao cliente introduzir no campo Nome de Acesso o seu ID e no campo Palavra-Chave a palavra-passe fornecidos no balcão.

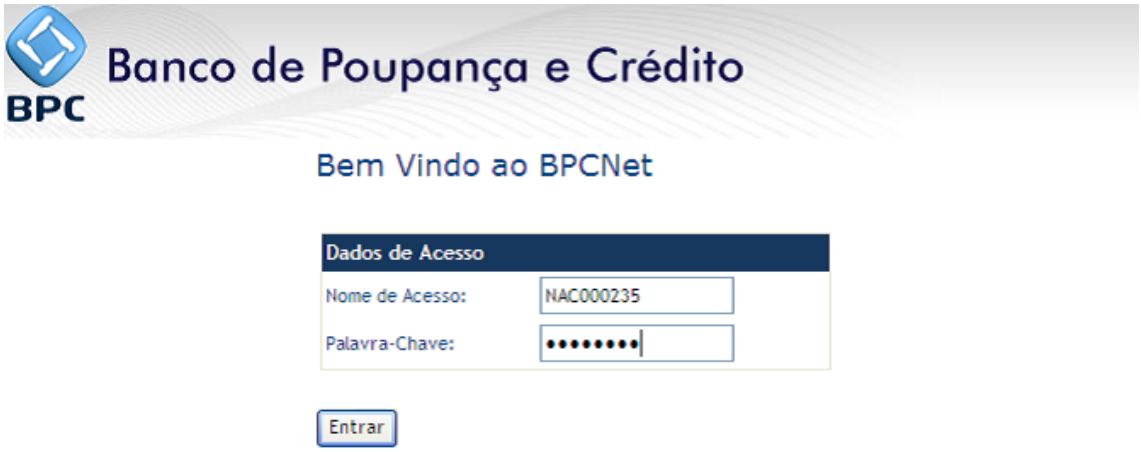


Fig. 3.7: Inserção de dados de acesso

Palavra Secreta

A Palavra Secreta é um código de segurança adicional criado pelo cliente que será solicitado pelo sistema sempre que quiser aceder ao BPCNET. Se é a primeira vez que acede ao serviço, após ter preenchido os dados de acesso no sistema, o cliente deverá criar uma palavra secreta de sua conveniência com as características indicadas

na figura 3.8 Nos próximos acessos o sistema não solicitará que o utilizador crie outra Palavra Secreta.

Fig. 3.8: Criação de Palavra Secreta

Desta forma, sempre que o cliente aceder ao BPCNET e após ter inserido os Dados de Acesso, o sistema solicitará a introdução de caracteres aleatórios da Palavra Secreta.

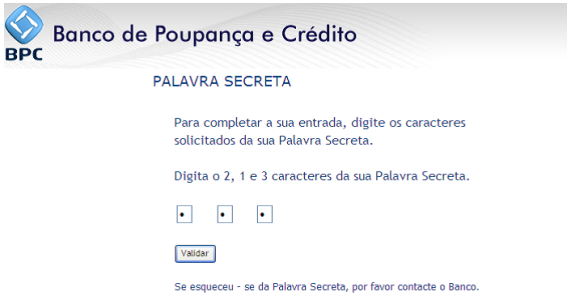


Fig. 3.9: Inserção Aleatória da Palavra Secreta

Mudança da Palavra Chave

No primeiro acesso, o sistema solicitará ao cliente que mude a sua Palavra-Chave, o que não ocorrerá nos próximos acessos.

3.3.2 Menu

O menu principal do IFM apresenta do lado esquerdo a lista de todas as operações disponíveis na plataforma, devendo o cliente escolher qual delas pretende utilizar:

Fig. 3.10: Alteração da palavra-chave

Fig. 3.11: Menu Principal

Meu Correio Seguro

Esta opção permite ao cliente compor, enviar, receber e apagar mensagens trocadas entre si e o banco.

Minhas Contas

Nesta opção o sistema dá a possibilidade de visualizar os Detalhes da Conta, Movimentos na Conta (Extrato das ultimas 20 transações) e todas as contas que o cliente possui num determinado balcão. (Figura 3.13)
Conforme podemos ver na figura 3.14 (d), o IFM permite a consulta dos movimentos da conta, no entanto, esta consulta está restringida aos últimos 20 movimentos, não sendo possível fazer pesquisa por data.

(a) (b)

Fig. 3.12: Interface de Correio Seguro: (a) Lista de Mensagens; (b) Eliminar Mensagens.

Fig. 3.13: Lista de Contas

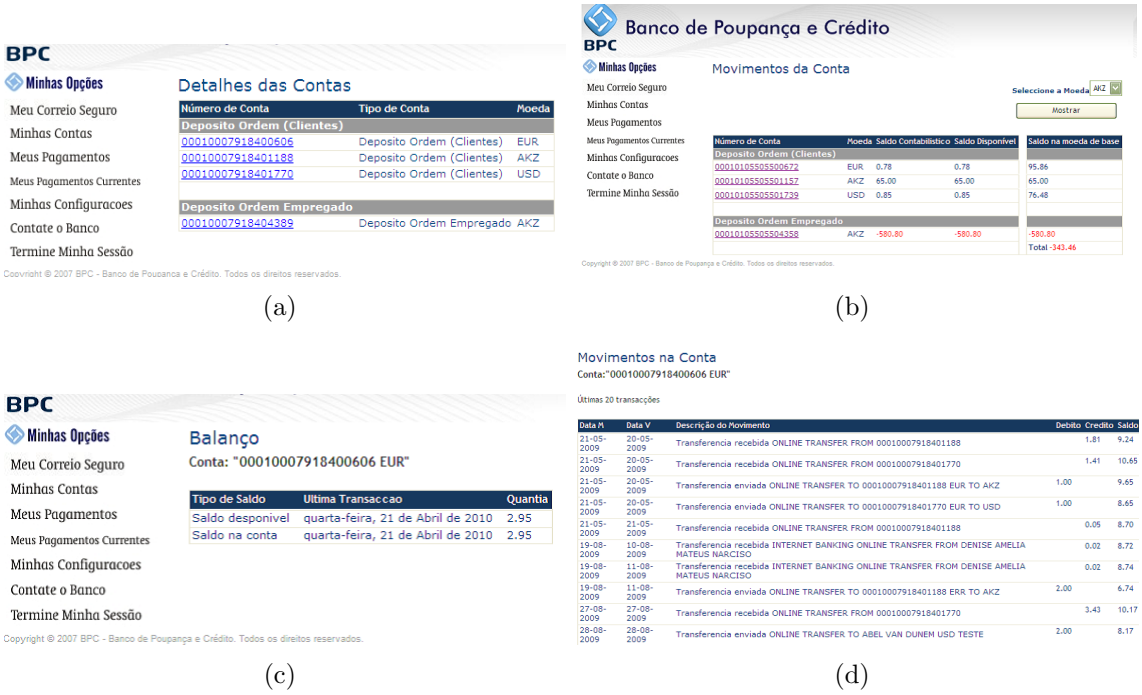
Pagamentos

Os pagamentos, no IFM são considerados como sendo transferências feitas dentro de um limite monetário e legal entre as contas do próprio cliente ou então entre o cliente e um conjunto de beneficiários definidos pelo próprio.

Para o caso de transferências entre as próprias contas do cliente, é necessário que ele selecione a conta a debitar e a creditar, digite a quantia a ser transferida e que escolha a data de execução da transferência. Pode ainda indicar uma descrição para o movimento. É ainda permitido que sejam efetuadas transferências para um beneficiário ou para um grupo de beneficiários. Este processo funciona, inicialmente, através de um contacto com o administrador do sistema para que este crie um ou mais beneficiários associados ao cliente, e apenas a partir daqui se torna possível efetuar a transferência.

Configurações

O menu configurações permitem alterar os dados demográficos do cliente, o seu User ID, palavra passe, e palavra secreta. (Figura 3.17)



(a) (b)

(c) (d)

Fig. 3.14: Contas: (a) Detalhe, (b) Lista para visualização de movimentos, (c) Saldo e (d) Movimentos.

Contacte o Banco

Permite o envio de mensagens para o administrador de sistema (Figura 3.18)

Sessões

O menu principal possui ainda a opção de terminar a sessão, que limpará a sessão iniciada pelo utilizador no Internet banking. (Figura 3.19 a))

Existe ainda um mecanismo de segurança que permite que a sessão seja dada como expirada quando o cliente está autenticado sem atividade na plataforma há mais de 10 minutos (Figura 3.19 b))

Fig. 3.15: Pagamentos

Fig. 3.16: Transferência entre Minhas Contas

3.3.3 Considerações finais

Ao analisar o IFM podem notar-se, em primeira mão vários problemas:

1. Falta de preocupação com o design da aplicação;

2. Pouca oferta de produtos / transações / serviços ao cliente (não existem referências a cartões de crédito, empréstimos, cheques, pagamentos de serviços, carregamentos, etc.);

3. Falhas de segurança no que respeita a mecanismos de validação de segundas linhas (sms tokens, cartões matriz);

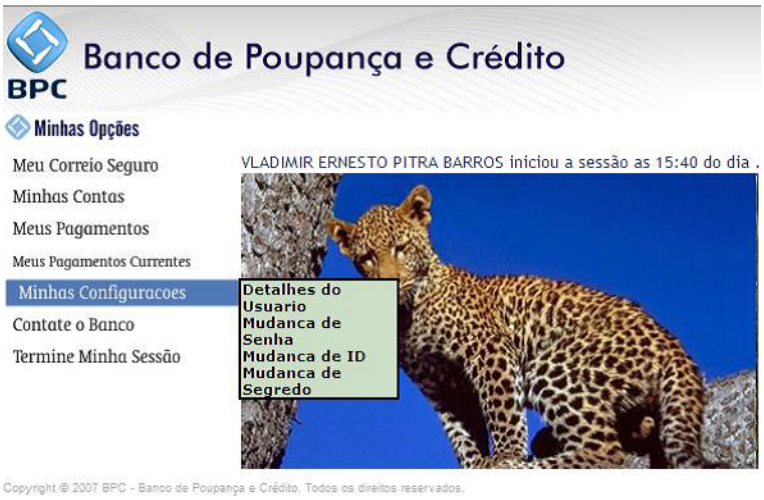


Fig. 3.17: Menu Configurações

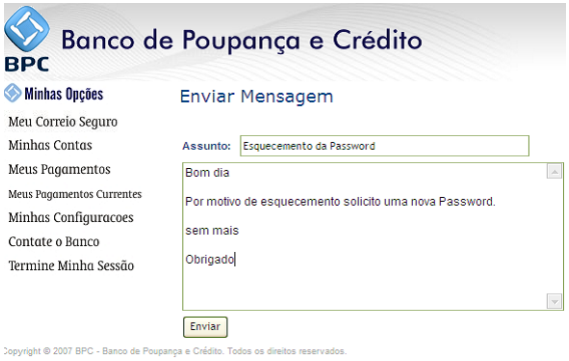


Fig. 3.18: Envio de Mensagem

4. Demasiada dependência do administrador do sistema para a criação de beneficiários, para possibilitar a transferência bancária entre contas de outrem;

5. Consultas movimentos / balanços limitadas;

6. A plataforma é geral para qualquer que seja o tipo de cliente (particular ou empresa);

7. Não existe mecanismo de gestão de contratos...

(a) (b)

Fig. 3.19: Sessões no IFM: (a) Sessão terminada; (b) Sessão expirada.

3.4 Atlantico Directo (Banco Millennium Atlântico)

O Atlantico Directo é o sistema de IB desenvolvido pela ITSector para o Banco Millennium Atlantico. O Banco Millennium Atlântico é um dos principais concorrentes do Banco Poupança e Crédito no sector financeiro angolano. Seguidamente serão apresentadas algumas das funcionalidades disponibilizadas pela plataforma, assim como alguns ecrãs ilustrativos.

3.4.1 Funcionalidades Atlantico Directo

Até à data, o Atlantico Directo apenas está disponível para clientes particulares e está disponível no endereço: https://ibparticulares.atlantico.ao
Após o ecrã de acesso, o Atlantico Directo apresenta um dashboard que permite ter um resumo do saldo da conta e da posição do cliente dentro do banco (Figura 3.20).

A lista de funcionalidades do Atlantico Net é extensa e compreende várias operações que estamos acostumados a fazer, podendo tornar-se numa plataforma muito útil para o cliente.
As transações existentes são as seguintes:

- Consultas, detalhes, movimentos de contas assim como de NIB/IBAN (Número de identificação bancária / *International Bank Account Number*);
- Cheques: Consulta, requisição cancelamento;
- Transferências: transferências nacionais, agendamento de transferências;
- Pagamentos: pagamento de serviços, recargas;

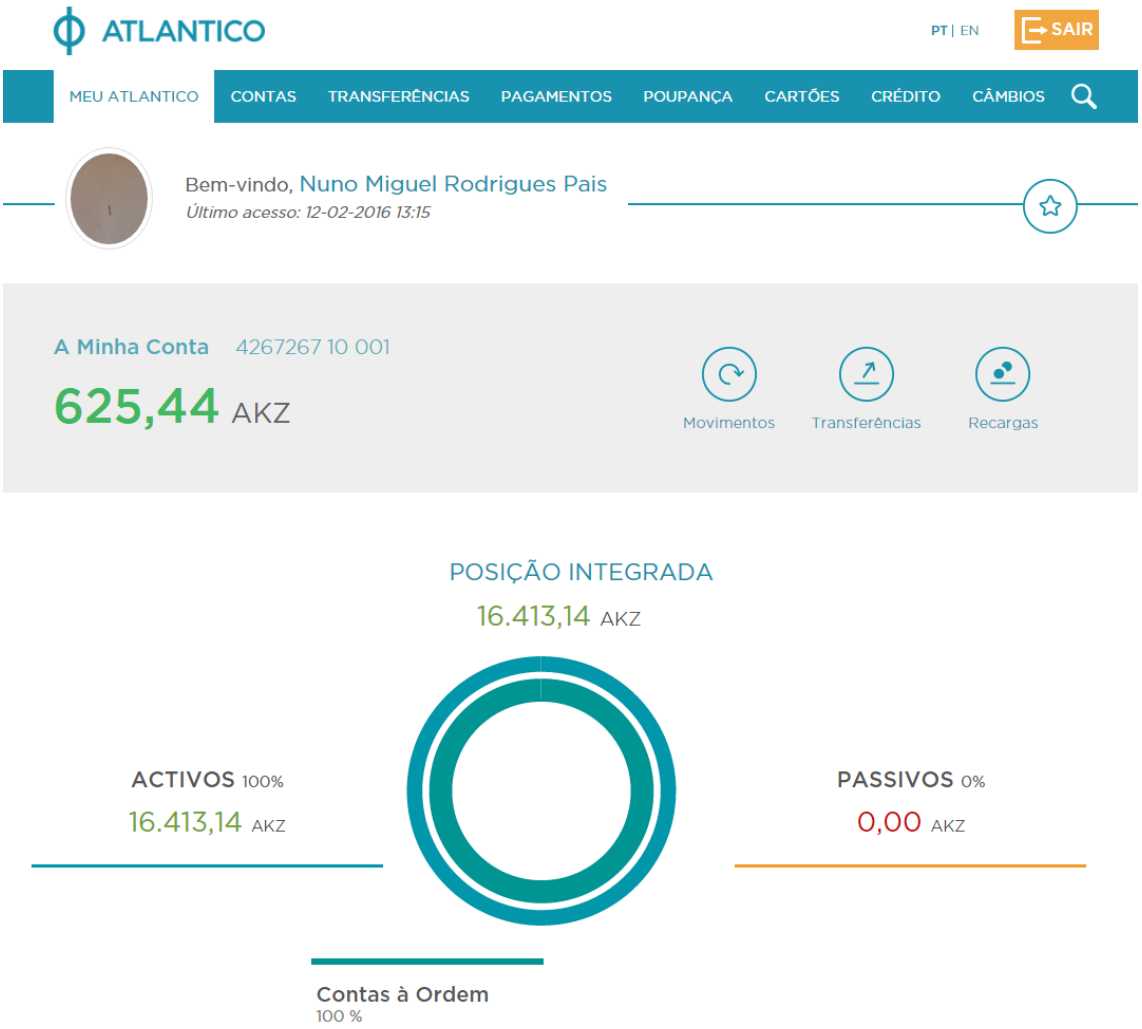


Fig. 3.20: Dashboard Inicial Atlantico Directo

- Poupanças: detalhes, movimentos, constituição;
- Cartões de débito e crédito: consulta, movimentos, cancelamento de cartões de crédito.

O Atlantico Net tem ainda disponível na App Store aplicações para iPad e iPhone e na Google Store aplicações para sistemas Android.

3.5 Conclusão

O espectro de ataques disponíveis a plataformas de Internet obriga a uma análise rigorosa de todos os métodos de prevenção possíveis.

Analisando a plataforma apresentada na secção 3.3, e sabendo em primeira mão que é uma solução que não apresenta grandes preocupações em relação à segurança financeira do cliente, o projeto a desenvolver torna-se numa grande mais valia. O projeto trará aos clientes do maior banco angolano a possibilidade de executarem de forma confortável um grande número de operações.
Analisando outras plataformas existentes no mercado angolano, como é o exemplo da apresentada na secção 3.4, conseguimos apurar ainda melhor a necessidade do BPC em desenvolver uma plataforma renovada e inovadora.
Desta forma, o projeto é de facto de uma importância extrema para o desenvolvimento do banco, na medida em que possibilitará ao banco o seu reposicionamento no mercado angolano como um banco inovador, seguro, fiável e com especial atenção aos principais interesses dos seus clientes.

Capítulo 4

Desenho da solução

O desenho da solução torna-se importante para a definição de um conjunto de objetivos que permitam a conclusão do objetivo inicial.
A lista de operações a realizar é importante, na medida em que este será um dos principais fatores de satisfação dos clientes.
Como tal, ao longo do capítulo serão apresentadas considerações acerca das principais funcionalidades que devem ser disponibilizadas no IB e também no Backoffice.

4.1 Operações a realizar no BPCNet

Para satisfazer as necessidades dos clientes, é importante apresentar um conjunto de operações vasto, que permitam ao utilizador fazer a maior parte das suas operações bancárias na comodidade do seu lar. Como tal, a figura 4.1 ilustra quais as principais transações que serão desenvolvidas no âmbito do projeto.

É expectável que todas as operações, para efeitos de débitos, registo de movimentos, ou mesmo consulta de dados sobre contas, sejam comunicadas em tempo real com o core bancário, o Equation / Mysis.
Existem no entanto grupos de transações / operações que não dependem apenas do core bancário para registo do movimento ou mesmo o débito da operação na conta. No caso dos pagamentos / carregamentos, é necessária a intervenção de entidades externas, que comunicam a execução dos pagamentos aos beneficiários.
Para pagamento de serviços, recargas, carregamentos ou paramentos parametrizáveis é necessária a intervenção da EMIS. A estrutura de comunicação com os serviços da EMIS será explicada mais a frente no relatório.

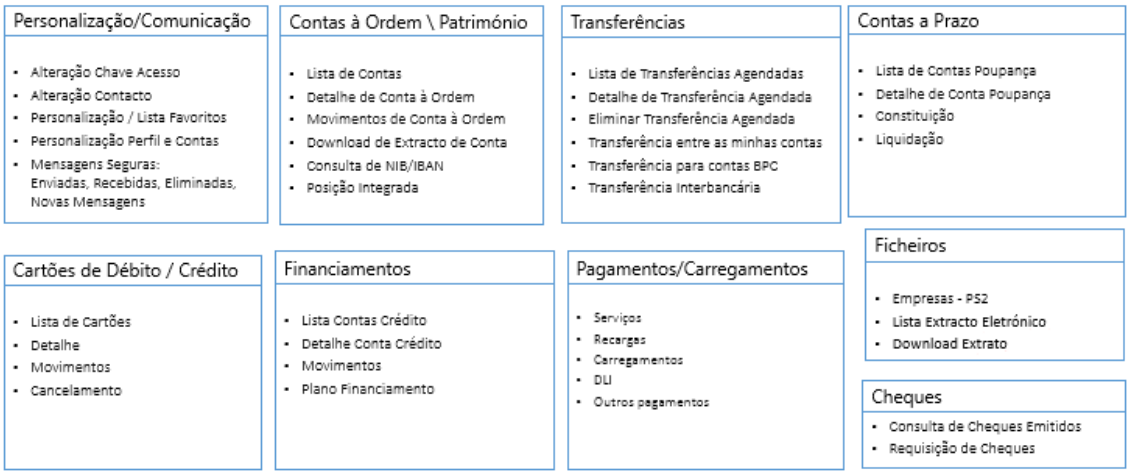


Fig. 4.1: Lista de funcionalidades a apresentar no BPCNet

Os pagamentos de DLI (Documento de Liquidação de Impostos) é também dependente de um webservice já disponibilizado pelo Ministério de Finanças Angolano, que permite a comunicação da execução do pagamento por parte do cliente ao governo Angolano.
Por fim, nas listas, detalhes, movimentos e cancelamentos de cartões de crédito, são utilizados serviços disponibilizados pela EMP. A estrutura de comunicação com a EMP será também explicada mais adiante no relatório.

O diagrama apresentado na figura 4.1 ajuda a fazer um sumário das operações e ainda a identificar qual o tipo de operações que exige autenticação de 2º nível.

Analisando a figura, podemos rapidamente concluir que existirão perfis diferentes no acesso ao IB: clientes particulares e empresas.
As operações disponibilizadas podem dividir-se em diferentes segmentos: consultas e operações.
Para a execução de uma consulta (detalhes de conta, movimentos de créditos, extratos) não será requerida qualquer autenticação depois do utilizador possuir uma sessão válida.
Na execução de uma operação, e sempre que existir uma alteração de património, o cliente é obrigado a ultrapassar o mecanismo de autenticação de segundo nível, através da utilização do seu cartão matriz ou então *SMS Token*.

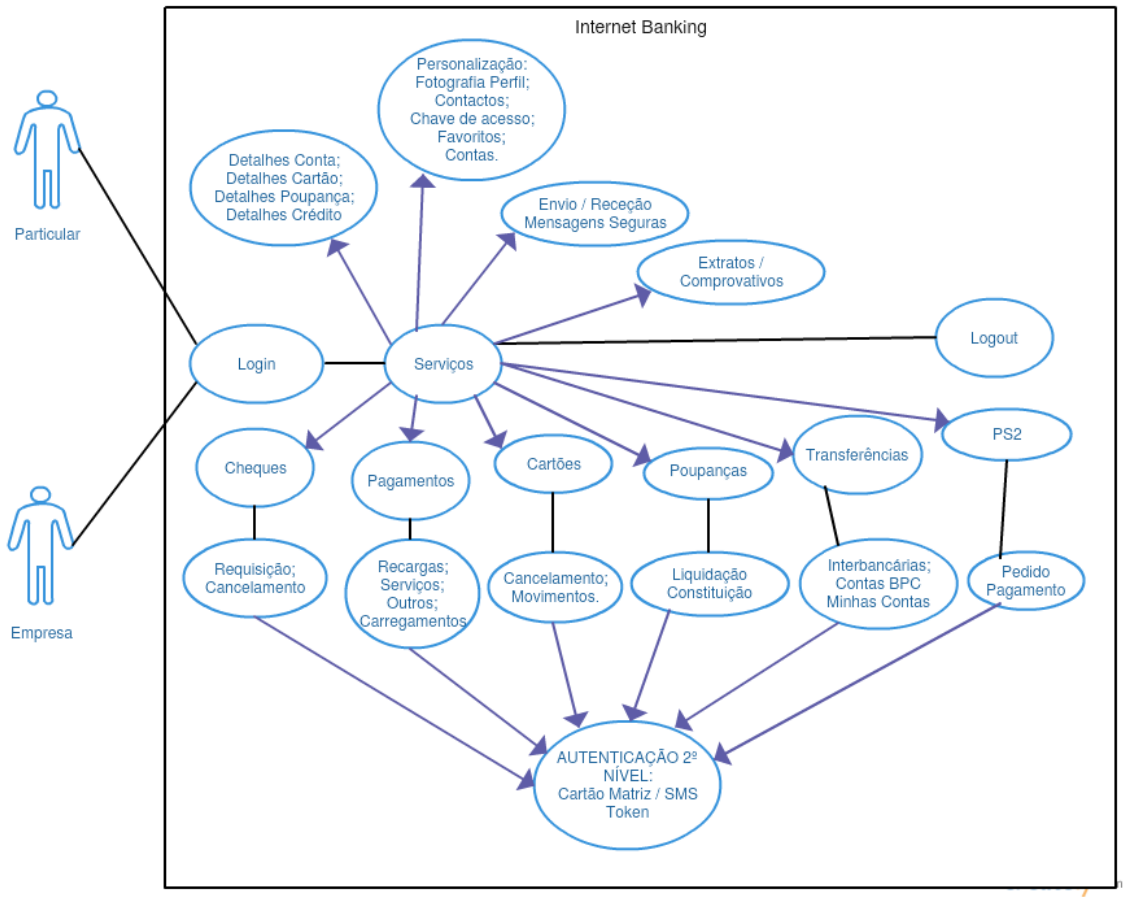


Fig. 4.2: Diagrama de operações disponíveis

4.2 Funcionalidades disponíveis em Backoffice

O backoffice da aplicação será disponibilizado na intranet do BPC e será utilizado pelos colaboradores do banco para a criação de processos de adesão ao IB. Para além da criação de processos de adesão, será permitido aos colaboradores efetuarem a gestão de contratos, consulta de estatísticas, geração de envelopes de segurança e cartões matriz e respetiva atribuição destes aos balcões / agências do banco.

4.2.1 Workflow de adesão

A adesão ao serviço de canais eletrónicos é o primeiro passo para que um cliente do banco possa usufruir de um modo confortável, seguro e ágil de um serviço de canais não presenciais para as operações do dia-a-dia.
Este processo é bastante sensível a nível de segurança, pois é necessário garantir que

os dados do cliente (códigos de acesso, chaves de ativação, etc.) não caem nas mãos erradas.

Um dos desafios é garantir a nível da própria instituição que os seus colaboradores não tenham permissões para aceder indevidamente a informação sensível do processo de adesão grande parte dos casos de fraude bem-sucedidos são de origem ou envolvimento dos colaboradores da empresa.

Por outro lado, os meios de transporte de correspondência do país são motivo de preocupação devido a violação da correspondência por parte dos próprios serviços dos correios ou terceiros ou ainda devido ao furto e extravio da correspondência por este motivo não devemos recorrer a este meio como garantia da entrega da informação importante para a ativação do serviço (carta de ativação do serviço).

Assim sendo, a principal preocupação neste processo é garantir que um colaborador não tenha a capacidade de, sozinho, aceder a toda informação e a todas as etapas.

Outro ponto importante na garantia da segurança deste processo é a entrega, no próprio balcão, de um envelope selado com as credenciais de segundo nível, que o cliente irá usar para ativar o serviço e posteriormente para aprovar as operações.

Para o caso das empresas, o processo de adesão é mais complexo pois temos a necessidade de definir as regras de segurança do contrato (p.e. funcionalidade disponíveis, autorizados, limites, regras de assinaturas, etc).

A figura 4.3 representa todas as ações executadas para que a adesão de um cliente fique concluída com sucesso.

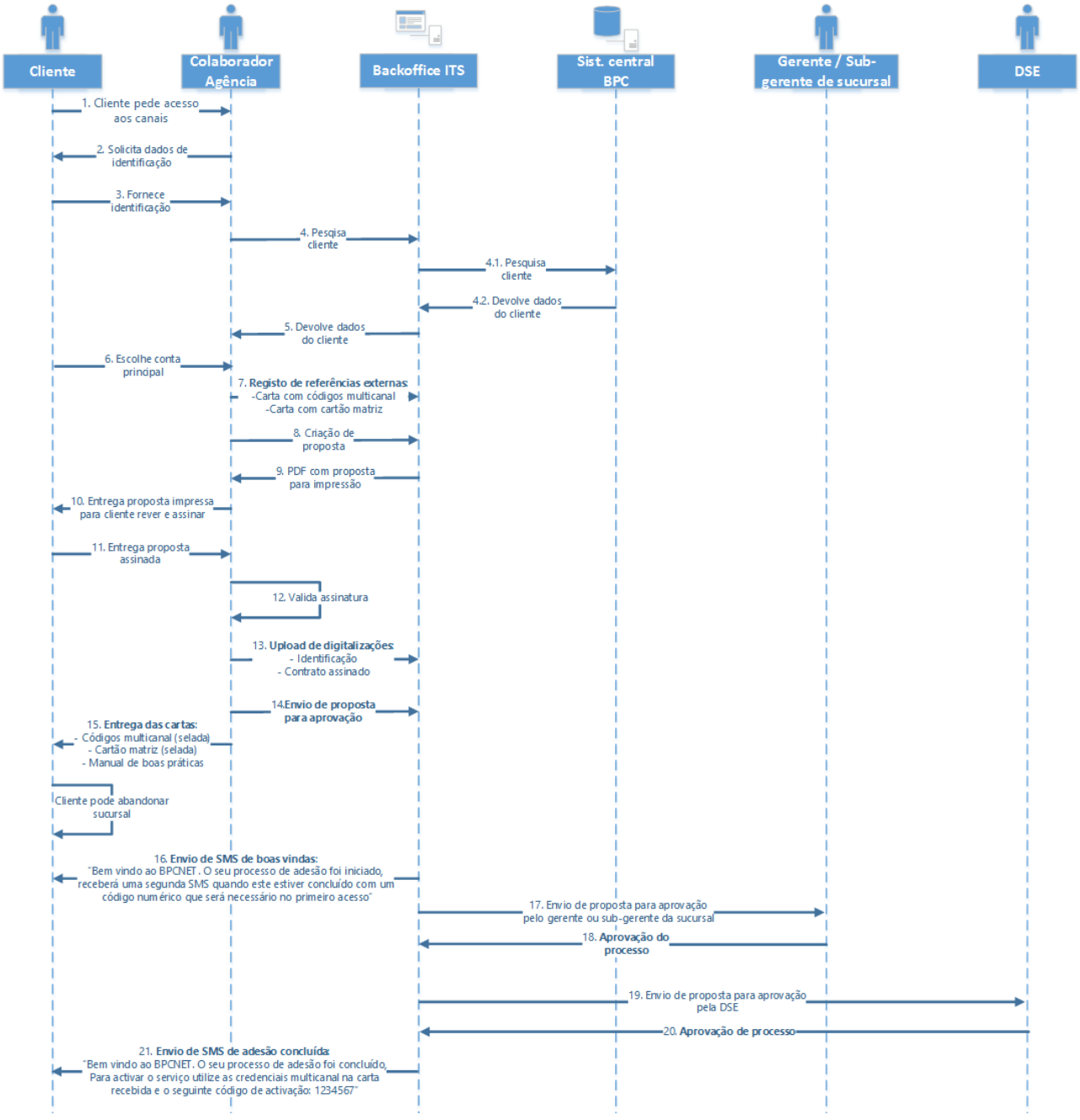


Fig. 4.3: Workflow de adesão ao Internet banking

4.3 Ligações a ambientes externos

De forma a completar com sucesso o projeto proposto é necessária a conexão a ambientes externos.

4.3.1 Core Bancário - Equation

O Equation é a denominação do sistema central do banco. A utilização de uma integração em tempo real com o core bancário é de extrema importância, para que o cliente possa executar no momento as operações que pretende, tal como acontece quando este executa as ações numa agência.
A ligação com o Equation será realizada utilizando o conceito Enterprise Service Bus (ESB) que está atualmente implementado no BPC. Este conceito caracteriza-se pela disponibilização de funcionalidades como serviços a componentes distintas. Esses serviços são implementados com o intuito de satisfazer determinados requisitos de negócio, sendo facilmente reutilizáveis por outras aplicações.
Desta forma, diversas funcionalidades de negócio estão implementadas em serviços atómicos. Com isto, existe uma forte aposta na generalização das funcionalidades de negócio, por forma a evitar:

1. A replicação de operações;
2. A dependência entre componentes;
3. Ligações ponto-a-ponto entre providers de informação distintos.

Esta arquitetura de referência permite que quaisquer interações entre aplicações distintas passem sempre pela camada de integração do BPC, a qual se encarregará de dar resposta ao pedido solicitado, abstraindo e isolando as aplicações de como essa interação está implementada. Cabe às aplicações que necessitam de aceder a funcionalidades de negócio, interagirem apenas e só com a camada de integração, a qual expõe essas funcionalidades sob a forma de serviços, devendo assim respeitar os contratos das assinaturas dos mesmos.
Este é o alinhamento arquitetural que está implementado no BPC e o qual faz cada vez mais sentido face às crescentes necessidades originadas em canais distintos. Estamos a promover desta forma a utilização duma plataforma de integração que expõe as funcionalidades de negócio, duma forma genérica, reutilizável, unívoca e independente do canal. Existe assim um modelo canónico de comunicação o qual promove o desacoplamento e isolamento de aplicações distintas, com um ponto de

comunicação único e comum a todas, reutilizando funcionalidades de negócio já implementadas.

4.3.2 EMIS

A ligação com a EMIS para execução de operações de pagamentos de serviços terá de ser efetuada utilizando a aplicação PRT disponibilizada pela própria EMIS.
A aplicação PRT tem como objetivo a troca de mensagens em tempo real entre os bancos e o Sistema Central de Processamento da Entidade Gestora da Rede garantindo que não se perde qualquer mensagem.
De modo a cumprir esse objetivo, é utilizada a aplicação PRT, que implementa um protocolo de comunicação *Real-Time*, que se baseia no estabelecimento de sessões entre o sistema central e o banco, possibilitando assim o envio e receção de mensagens, com total garantia de segurança e integridade.
A aplicação baseia-se na utilização da tecnologia de *sockets* sobre o protocolo de comunicação TCP/IP. Dada a natureza do protocolo PRT garante-se a entrega das mensagens entre os intervenientes, e como é uma aplicação java pode ser instalada em todos os sistemas que suportem a *java virtual machine (JVM)*, como sejam Windows ou Unix.
Em termos práticos, nos ambientes de qualidade e de produção será instalado este PRT que permite comunicação entre a EMIS e o banco. Quando um cliente efetua um pedido no IB de uma operação EMIS, a plataforma BPCNet coloca uma mensagem numa *dataqueue* de entrada (IN) com os dados da operação. O PRT instalado no BPC faz a conexão e transmissão da mensagem para o PRT da EMIS que após interpretação devolve ao BPC (de forma síncrona) uma mensagem de resposta. Esta mensagem trás o resultado da operação que será lido e interpretado pelo Internet Banking e consequentemente apresentado ao cliente. A Figura 4.4 representa o esquema de conexão entre o BPCNet e a EMIS.

É ainda importante ter em consideração as seguintes considerações:

- Nas operações efetuadas no contexto de Host2Host de pagamento de serviços, a EMIS não efetua o débito das operações no BPC;

- As operações executadas no Host2Host são retornadas no ficheiro DST5 enviado todos os dias pela EMIS para o BPC;

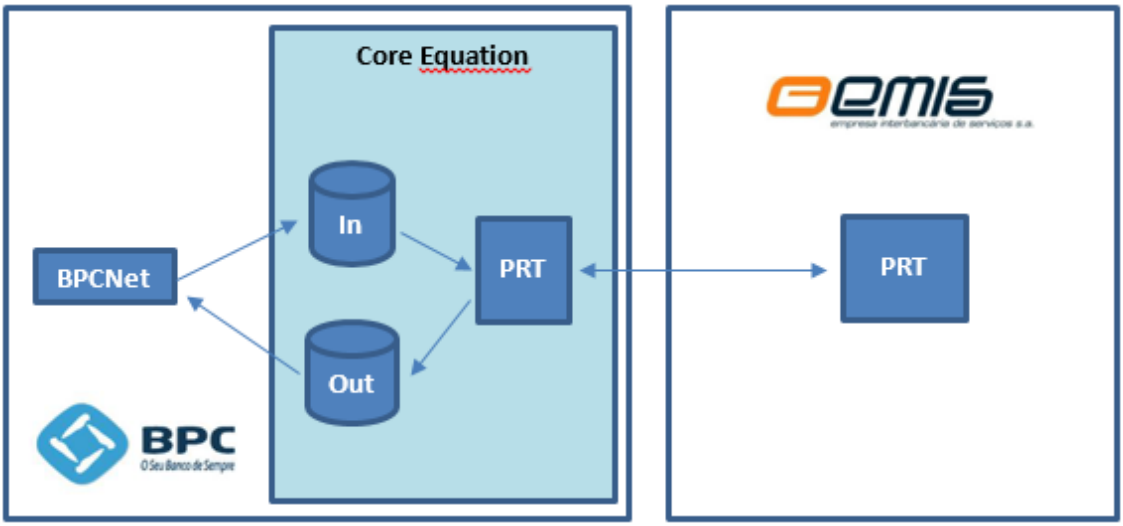


Fig. 4.4: Arquitetura ligação EMIS - BPC

- Quando o ficheiro é processado no Equation o débito da conta é efetuado com base no NIB e valor que foi enviado no serviço para a EMIS.

4.3.3 EMP

A EMP será a entidade responsável pela gestão dos cartões de crédito e débito do cliente. A conexão entre o Internet Banking e a EMP será realizada através da utilização de webservices, disponibilizados pela própria EMP, que permitirão executar todos os request necessários ao bom funcionamento do módulo de cartões de crédito e débito.

Capítulo 5

Implementação da solução

A solução a implementar compromete-se a cumprir vários objetivos traçados pelo banco. O primeiro objetivo é o de apresentar ao público-alvo uma aplicação inovadora, segura e superior às demais existentes no mercado angolano e apresentadas pelos bancos concorrentes, como é o caso da aplicação Atlantico Net do BMA, apresentada na secção 3.4.
Ao longo deste capítulo serão descritas as tecnologias utilizadas assim como a arquitetura montada e quais os principais aspetos de segurança introduzidos nos desenvolvimentos.

5.1 Arquitetura do sistema

Para o correto desenvolvimento do projecto, é necessária a existência de pelo menos 3 ambientes que permitam o desenvolvimento, controlo de qualidade e disponibilização da aplicação. (Figura 5.1)

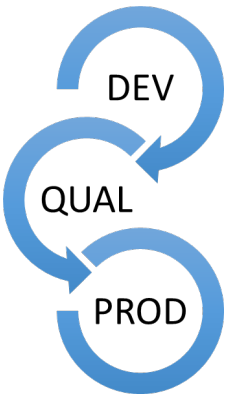


Fig. 5.1: Ambientes disponíveis para o desenvolvimento do projeto

5.1.1 Ambiente de Desenvolvimento

O ambiente de desenvolvimento encontra-se instalado em Portugal, nos escritórios da ITSector, acedendo por VPN ao BPC.
Para complementar o processo de desenvolvimento de software baseado em metodologias ágeis, o ambiente de desenvolvimento usa a técnica de integração contínua. Esta técnica permite que os desenvolvimentos unitários sejam adicionados à aplicação diariamente, permitindo validar a sua integração com toda a aplicação.
A arquitetura expectável do ambiente é está presente na figura 5.2 e compreende 3 servidores distintos, o primeiro para suporte da base de dados, o segundo para suporte da camada de serviços e um terceiro para suportar a camada de apresentação.

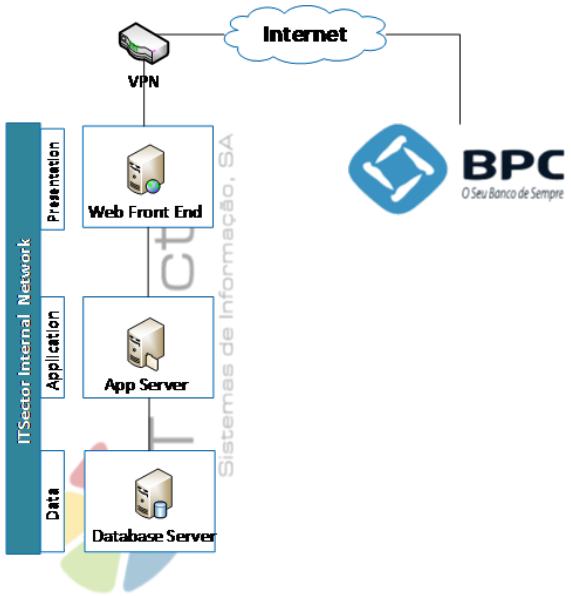


Fig. 5.2: Arquitetura ambiente de desenvolvimento

5.1.2 Ambiente de Qualidade

O ambiente de qualidade (figura 5.3) será instalado nas instalações do BPC em Luanda e apenas será acedido dentro da sua rede interna. Os principais objectivos deste ambiente passam por:

- Instalação das diversas *releases* para que possam ser testadas;
- Controlo de incidentes;
- Certificação dos diversos módulos da aplicação

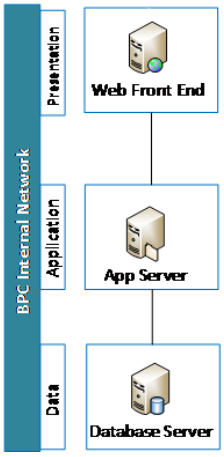
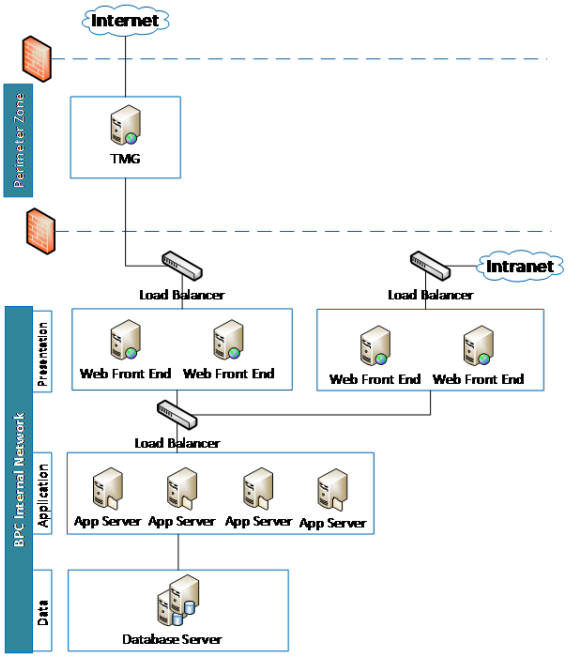


Fig. 5.3: Arquitetura ambiente de qualidade

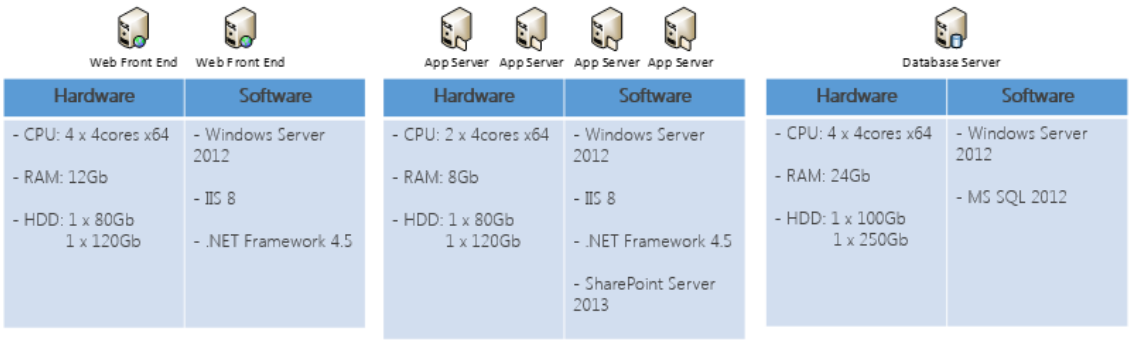
5.1.3 Ambiente de Produção

O objetivo do ambiente de produção será apresentar a solução para os clientes, para que a possam utilizar. É importante que o ambiente garanta nível de serviço, tenha uma boa performance e que seja seguro. Será necessário um servidor de base de dados, vários servidores para a camada de serviços, um conjunto de dois servidores para a camada de apresentação do *frontend* do *Internet banking*, assim como dois servidores para a camada de apresentação do backoffice aplicacional que será apenas acedido através da intranet.

É ainda necessária a criação de uma *perimeter zone* - *DMZ* protegida por duas firewalls, permitindo a segurança de todos os servidores anteriormente falados.



(a)



Hardware	Software
- CPU: 4 x 4cores x64 - RAM: 12Gb - HDD: 1 x 80Gb 1 x 120Gb	- Windows Server 2012 - IIS 8 - .NET Framework 4.5

Hardware	Software
- CPU: 2 x 4cores x64 - RAM: 8Gb - HDD: 1 x 80Gb 1 x 120Gb	- Windows Server 2012 - IIS 8 - .NET Framework 4.5 - SharePoint Server 2013

Hardware	Software
- CPU: 4 x 4cores x64 - RAM: 24Gb - HDD: 1 x 100Gb 1 x 250Gb	- Windows Server 2012 - MS SQL 2012

(b)

Fig. 5.4: Ambiente de produção: (a) Arquitetura; (b) Caraterísticas infraestrutura interna.

5.2 Ferramentas e Tecnologias

Esta aplicação foi idealizada para ser desenvolvida em plataforma Windows, visto que é a utilizada pela empresa. Para o desenvolvimento deste projeto foram então utilizadas ferramentas de desenvolvimento Microsoft. Para cada camada do desenvolvimento foram utilizadas diferentes ferramentas e tecnologias conforme espelhado na figura 5.5.

Software	Linguagens	Tecnologias Ferramentas Metodologias
- SQL Server 2012	SQL	Stores Procedures; Diagramas ER.
- Microsoft Visual Studio	C#	Linq; WCF; REST.
- Microsoft Visual Studio; - Sharepoint	Asp.Net; HTML; CSS; JavaScript	bootstrap; jQuery

Fig. 5.5: Tecnologias utilizadas no desenvolvimento

5.2.1 SQL Server

O Microsoft SQL Server é um Sistema de Gestão de Bases de Dados (SGBD) abrangente que oferece ferramentas de gestão de dados. A gestão é centralizada, o que reduz a necessidade de configurar cada instância separadamente, sendo esta feita no SQL Server Management Studio. Permite, através da redução da complexidade do desenvolvimento e do suporte, maximizar a produtividade das Tecnologias da Informação (TI). Ajuda ainda a resolver problemas de integridade e consistência de dados quando estes provêm de diversos sistemas e estão classificados de formas diferentes (Vale 2012)

O sistema fornece um conjunto de serviços integrados que permitem consultar, pesquisar, sincronizar e analisar os dados. Fornece também desempenho, fiabilidade e escabilidade melhorados, o que permite a redução de tempo e de custo na gestão e desenvolvimento de aplicações. Permite que o controlo seja mais preciso e flexível, oferecendo segurança total para as informações. O SQL Server 2012 suporta ainda dados relacionais e não relacionais, permitindo o armazenamento e gestão de dados não estruturados, como é o caso de documentos e imagens. (Vale 2012)

5.2.2 .Net Framework 4.5

A .Net Framework foi desenvolvida pela Microsoft para uniformizar a programação de aplicações para vários tipos de dispositivos, plataformas e linguagens de programação. Esta possui dois componentes principais, o **Common Language Runtime (CLR)**, responsável pela execução do código e a **Class Library**. Neste projeto foi utilizado a versão 4.5 por ser a mais recentemente disponibilizada pela Microsoft no inicio do projeto. (Microsoft 2012)

5.2.3 Entity Framework

O ADO.NET Entity Framework é a nova plataforma de acesso a dados desenvolvida pela Microsoft e incorporada inicialmente na framework .NET 3.5. Permite criar aplicações em que o acesso a dados é feito com base num modelo concetual e sem utilização de comandos diretos à base de dados. Isto permite que o programador se abstraia totalmente da base de dados (criação de ligações de acesso, comandos, parâmetros, etc.) e utilize apenas objetos durante o desenvolvimento (Souto 2012). A versão do Entity Framework (EF) que está disponível na .NET Framework 4.0, tem um conjunto de novas funcionalidades e melhorias, como é o caso de suporte a POCO - Plain Old CLR Objects (permite criar classes que não herdam, nem implementam nenhuma outra classes ou interface), abordagem Model-First (permite criar primeiro o modelo concetual e, com base nele, criar a base de dados), suporte para o uso de funções em LINQ-to-Entities, Complex Types (criação de tipos de dados complexos), Deferred Loading ou Lazy Loading (capacidade de carregar as propriedades de associação das entidades no momento em que são chamadas). (Souto 2012)

O EDM (Entity Data Model) é um conceito que no EF foi implementado de forma a se obter uma maior produtividade. O modelo de entidades de dados e toda a informação de mapeamento de cada entidade para a sua tabela na base de dados é armazenada num ficheiro de representação XML num ficheiro de extensão *edmx*. Pela descrição do EF constata-se que existem várias vantagens na utilização de um ORM (Object-relational mapping), que tornam a sua adoção quase inevitável. A par deste ORM existem outros com funções semelhantes como o NHibernate pertencente também à Microsoft e o Hibernate escrito em linguagem Java. No entanto, pelas vantagens enunciadas e por um entendimento mais fácil do enquadramento do EF na framework .NET 4.0, optou-se por este ORM no desenvolvimento da solução. (Souto 2012)

5.2.4 LINQ

LINQ (Language Integrated Query) é um componente introduzido na Framework .NET 3.0 com o propósito de colmatar a grande dificuldade em se executarem consultas a bases de dados e unificar o modelo de acesso a dados a diferentes fontes de informação como objetos, documentos XML e estruturas de dados. Utilizando LINQ pode-se programar o código de acesso a dados directamente em C ou Visual Basic e verificar-se a sintaxe em tempo de compilação. Com LINQ não há necessidade de se utilizar diferentes tecnologias para acesso a dados como SQL, XPath, XQuery, entre outras, porque utiliza um modelo unificado de acesso a dados (Souto 2012). A arquitetura da tecnologia LINQ é representada de acordo com a ilustração da Figura 4.5
O LINQ é dividido em várias partes, como LINQ to Objects que permite fazer consultas a objectos em memória como arrays, LINQ to SQL que permite fazer consultas a base de dados, LINQ to Entities que permite fazer consultas a base de dados a partir da mesma linguagem usada para construir a lógica de negócio e LINQ to XML que permite criar, modificar e navegar por ficheiros XML. (Souto 2012)

5.2.5 C#

C é uma linguagem de programação orientada a objetos fortemente tipada, desenvolvida pela Microsoft como parte da framework .NET . A sua sintaxe orientada a objetos foi baseada na linguagem C++ mas inclui muitas influências de outras linguagens de programação como o Java; sendo que uma das vantagens da linguagem Java em relação ao C é possuir compatibilidade com um maior número de plataformas, em que uma aplicação quando desenvolvida na linguagem Java é traduzida pelo seu compilador para os bytecodes, ou seja o código é transformado em código máquina de um processador virtual chamado de Java Virtual Machine (JVM), permitindo a ser executado em qualquer plataforma desde que esteja instalada uma JVM, enquanto que o C além de suportado pela plataforma .NET também o é, por exemplo, no ambiente de Linux. (Souto 2012)

5.2.6 ASP.NET

O ASP.NET é uma tecnologia da Microsoft para desenvolvimento da camada UI (User Interface) de aplicações Web. Os programas em ASP.NET são aplicações centralizadas, residentes num ou mais servidores Web que respondem dinamicamente

aos pedidos dos clientes. Estas respostas são dinâmicas, porque o ASP.NET intercepta pedidos para páginas e encaminha esses pedidos para ficheiros de código compilado just-in-time (JIT) que podem responder no momento. De acordo com o paradigma da programação orientada a objetos, deve-se sempre separar a parte de processamento da aplicação da parte de interface com o utilizador (Souto 2012). Sendo coisas diferentes, não têm necessariamente de estar misturadas. Uma das grandes inovações das ASP.NET é o CodeBehind. Com ele é possível separar o código do servidor (exemplo: Page1.cs) do código HTML (exemplo: Page1.aspx). As páginas Web ASP.NET ou formulários Web são o elemento fulcral da camada UI no desenvolvimento de aplicações Web, estando os formulários integrados nos ficheiros de extensão .aspx .
O ASP.NET lida também com ficheiros de configuração (Web.config e machine.config) que contém iniciação e definições para uma aplicação específica, ou porção de uma aplicação. O servidor ignora pedidos para ficheiros Web, porque servi-los poderia constituir uma quebra de segurança. Relativamente aos pedidos, a grande diferença entre um pedido estático e um pedido dinâmico é que um típico pedido Web referencia um ficheiro estático. O servidor lê o ficheiro e responde com o conteúdo do ficheiro requisitado. Com o ASP.NET, não existe tal limitação. Não é necessário responder a um pedido com um ficheiro, pode-se responder com o que se quiser, incluindo ficheiros HTML criados dinamicamente, XML, gráficos ou dados binários. De se referir que o ASP.NET usa todas as linguagens da plataforma .NET. (Souto 2012)

5.2.7 WCF - Windows Communication Foundation

Windows Communication Foundation (WCF) é uma tecnologia de desenvolvimento de aplicações distribuídas e orientadas a serviços. (Souto 2012)
O WCF surgiu na framework .Net 3.0 com o propósito de unificar tecnologias como COM+, .Net Remoting, Web Services e MSMQ (Microsoft Message Queue), porque antes do WCF, era necessário que no desenvolvimento de aplicações o programador utilizasse tecnologias distintas para cada tipo de aplicação; um exemplo seria a criação de Web Services para disponibilizar na Internet algum serviço. Caso este serviço fosse disponibilizado na intranet, deveria ser criada uma aplicação que utilizasse .Net Remoting, porque esta tecnologia utiliza o protocolo TCP enviando ficheiros binários pela rede o que tornava a aplicação muito mais rápida do que com Web Service (Http/XML). Com a criação do WCF isso deixa de existir, e torna

a tarefa de desenvolvimento aplicacional por parte do programador mais simples e ainda proporciona um considerável ganho de performance em relação às tecnologias que o precedem (Souto 2012). Para que se possa projetar, implantar e hospedar os serviços WCF, deve-se considerar alguns conceitos, nomeadamente os Endpoints que é o que o serviço expõe e seus componentes (Address, Binding e Contract) (Souto 2012)

5.2.8 REST (Representational State Transfer)

O desenvolvimento das apps para dispositivos móveis nunca foi um objetivo do projeto. O principal objetivo era sim o de disponibilizar serviços de forma a que se tornassem consumíveis para um posterior desenvolvimento de uma app móvel. Atualmente existem duas escolas de pensamento no desenvolvimento de Serviços Web: a abordagem tradicional, baseada em padrões (SOAP) e a conceptualmente mais simples e mais recente, REST. (Moreira 2010)
No mundo dos Serviços Web, REST é uma chave que conjuga uma arquitectura cliente-servidor em que os Serviços Web são vistos como recursos e podem ser identificadas pelas suas URLs. Clientes dos Serviços Web que pretendam utilizar estes recursos de acesso a uma representação particular, transferem conteúdos usando um pequeno conjunto de métodos remotos definidos globalmente que descrevem a acção a ser realizada sobre o recurso. REST é uma descrição analítica da atual arquitectura Web, e assim, a interação entre o estilo e o protocolo HTTP resulta sem falhas. Os métodos HTTP, GET e POST são os verbos que o programador usa para descrever as acções necessárias, Criar (Create), Ler (Read), Actualizar (Update) e Eliminar (Delete) (CRUD). (Moreira 2010)
Um desenvolvimento REST pode ser útil quando:

- Os Serviços Web são completamente stateless. Um bom teste é determinar se a interacção pode sobreviver a um restart do servidor.

- Uma infra-estrutura em cache pode ser aproveitada para o desempenho. Se os dados que o Serviço Web devolve não são gerados dinamicamente e podem ser armazenados então, o armazenamento em cache que os servidores Web e outros intermediários intrinsecamente fornecem, podem ser aproveitados para melhorar o desempenho. No entanto, o programador deve ter cuidado, porque estas caches estão limitadas ao método HTTP GET para a maioria dos servidores.

- A largura de banda é particularmente importante e deve ser limitada. REST é particularmente útil para dispositivos como PDAs e telemóveis, para que a sobrecarga de cabeçalhos e camadas adicionais de elementos SOAP e XML seja limitada.

- Disponibilização de Serviços Web ou agregação em sites pode ser facilmente ativado com um estilo RESTful. Os programadores podem utilizar tecnologias como Asynchronous JavaScript com XML (AJAX), JSON (Javascript Object Notation) e ferramentas tais como Direct Web Remoting (DWR) para consumir os serviços nas suas aplicações Web. Os serviços podem ser expostos com XML e consumidos através de HTML sem refazer a arquitetura do actual site.

No caso específico da plataforma desenhada, os serviços desenvolvidos na camada de Middleware estão disponíveis na estrutura interna do banco e foram desenvolvidos com recurso a Serviços Web SOAP. Para prevenir o refazer de serviços, são utilizadas estas referências no desenvolvimento dos serviços REST, que são utilizados pela equipa de desenvolvimento de Apps. Um exemplo de código desenvolvido para a disponibilização de serviços REST é apresentado de seguida:

```
[HttpPost, Route("private/equation/customer/accounts")]
public ServiceResult<EquationAccountCollection> GetCustomerAccounts()
{
var metaInfo = new ResultMetaInfo();
try
{
using (var proxy = new ManagementServiceClientWrapperEquation(configEquation))
{
EquationAccountCollection accountCollection;
var outHeader = proxy.CreateServiceClient().GetCustomerAccounts(
base.ServiceInputHeader, out accountCollection);
if (outHeader.Status == ServiceStatus.Ok)
{
return new ServiceResult<EquationAccountCollection>(accountCollection, metaInfo,
outHeader.HasReturnMessage ? new ServiceMessage(outHeader.ReturnCode,
outHeader.ReturnMessage) : null, outHeader.OperationId, false, outHeader.Progress);
}
return GenerateErrorServiceResult<EquationAccountCollection>(outHeader, metaInfo);
}
}
catch (Exception e)
{
return new ServiceResult<EquationAccountCollection>(e, metaInfo);
```

```
}
}
```

Neste excerto de código é apresentado o serviço REST disponibilizado para o desenvolvimento da funcionalidade de pesquisa de contas de cliente.
Um serviço *HttpPost* é criado, sendo para este definido um recurso (*Route*), que nos permite disponibilizar o mesmo na Internet.
O serviço retorna um objeto (ServiceResult) que devolve:

- Sucesso / Insucesso;
- Em caso de sucesso: Lista de contas (objeto *accountCollection*);
- Em caso de erro: objeto com informação de erro.

Os serviços REST são disponibilizados na camada externa do banco, de forma a serem acessíveis pelas Apps. Existem mecanismos de segurança que permitem assegurar que os serviços não são atacados indevidamente. Estas medidas serão enunciadas na secção 5.4.

5.3 Interfaces

O desenvolvimento tecnológico dos últimos anos, o aumento significativo da banda larga e as inúmeras potencialidades criadas pelas mais recentes ferramentas de desenvolvimento aplicacional, permitiram criar ferramentas de comunicação mais interativas e mais apelativas para os utilizadores finais, tendo sempre como linha orientadora a importância de questões relacionadas com a usabilidade e com a eficácia da comunicação.
De acordo com estes parâmetros é importante desenvolver interfaces mais *user-friendly* que permitam ao utilizador interagir mais intuitivamente com a aplicação, possibilitando que este realize de forma mais eficaz e mais rápida a sua tarefa.
É neste ponto que a imagem da aplicação adquire uma importância vital para o sucesso de qualquer projeto, independentemente do canal de comunicação.
O interface deve acolher o utilizador, de forma a que este se sinta confortável com a aplicação, acompanhando e fornecendo informação necessária para que este sinta total confiança na aplicação e no serviço que esta disponibiliza.
A imagem proposta apresenta um conceito baseado nos seguintes vetores:

- Inovação;

- Facilidade de interação;
- Simplicidade;
- Dinamismo.

Estas linhas de orientação permitiram desenvolver uma proposta de imagem e uma estrutura de navegação simples e intuitiva, adequada a cada canal de comunicação e orientada para a realização eficaz e eficiente das operações disponibilizadas aos utilizadores.
Foram desenvolvidos esboços de alguns ecrãs para o Internet Banking e para o Backoffice da aplicação, de acordo com os requisitos / necessidades do BPC. Os ecrãs estão apresentados nas seguintes figuras.

No login, apresentado na figura 5.6, é requerido o número de contrato e respetiva palavra passe. É ainda informado o cliente de como pode contactar o banco, caso tenha algum problema com o login. Para efeitos de campanha, são disponbilizados conteúdos relativos a produtos do banco.

Fig. 5.6: Internet Banking | Login

O dashboard inicial (figura 5.7) será responsável por dar ao cliente o máximo de informação disponível, de forma a que o cliente fique completamente contextualizado da sua posição integrada. Através de gráficos é possivel analisar os ativos e passivos do cliente no banco.

A execução de operações tem sempre um aspeto semelhante ao apresentado na figura 5.8, ou seja, existe sempre a lista de contas, a operação que estamos a executar, a forma de notificação, e ainda detalhes sobre a operação.

Fig. 5.7: Internet Banking | Dashboard Inicial

Após avançar com a execução da operação surge um ecrã semelhante ao da figura 5.9, que permite ao cliente executar a autenticação para execução da operação.

O Backoffice aplicacional, que permite a gestão de contratos de adesão ao IB foi desenvolvido de forma segmentada, possuindo diferentes funcionalidades para diferentes perfis de acesso. Ao realizar login na aplicação, existem diferentes perfis que podem ser escolhidos como apresenta a figura 5.10.

Realizado o login, o colaborador é enviado para um dashboard que apresenta a lista de processos a tratar. A figura 5.11 apresenta uma lista de processos para o utilizador logado, com os respetivos SLA que permitem de forma mais fácil a perceção de quais os processos mais antigos.

A adesão ao Internet Banking pode ser sumarizada olhando para a figura 5.12. É necessária a introdução de alguns dados pessoais do cliente, como número de telemóvel, endereço de correio eletrónico e ainda os números de envelope de código de acesso e cartão matriz.

A adesão é concluida com a impressão e assinatura do contrato apresentados no anexo A e respetiva aprovação por gerente de balcão e supervisor de backoffice.

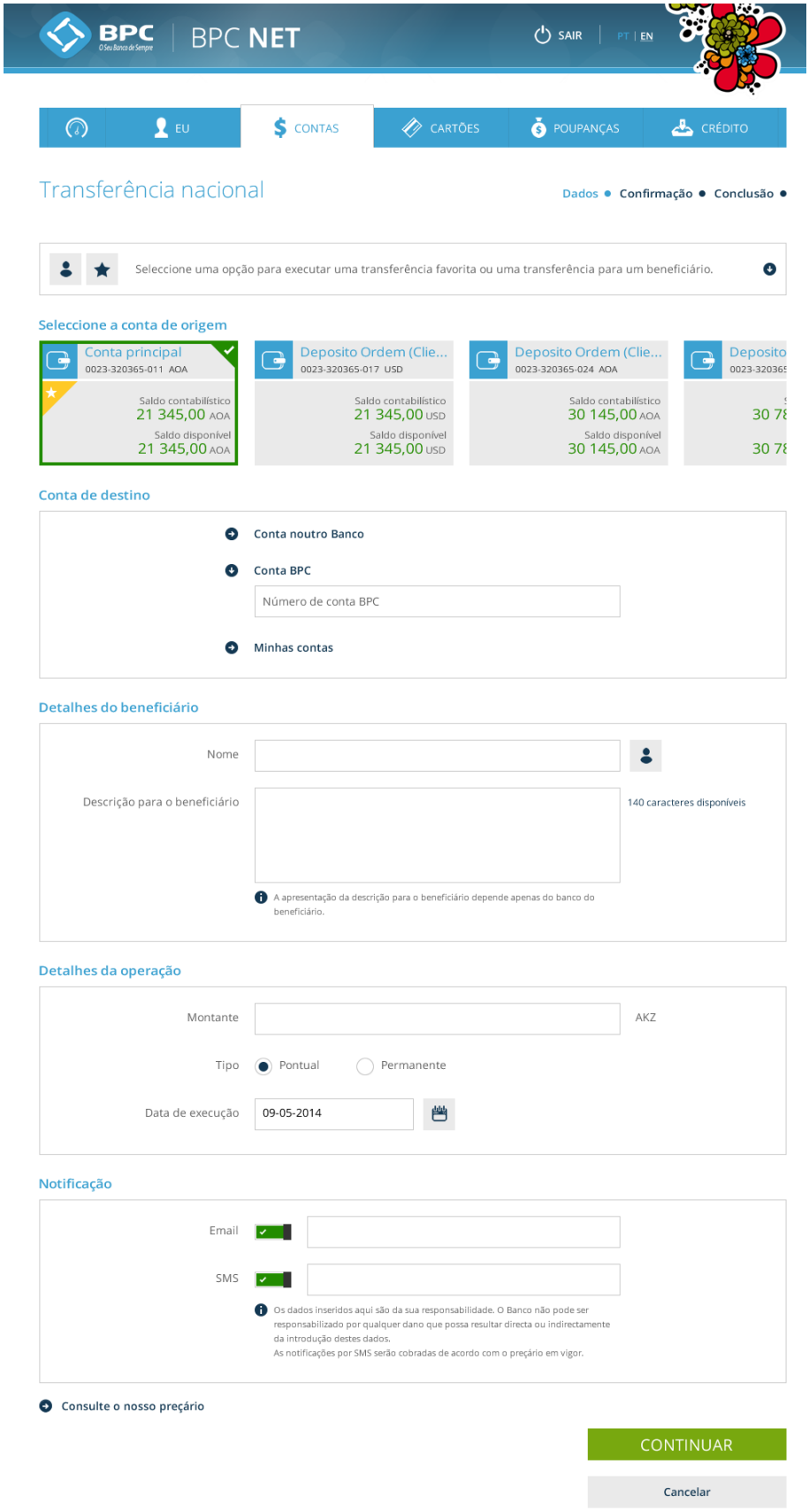


Fig. 5.8: Internet Banking | Transferências

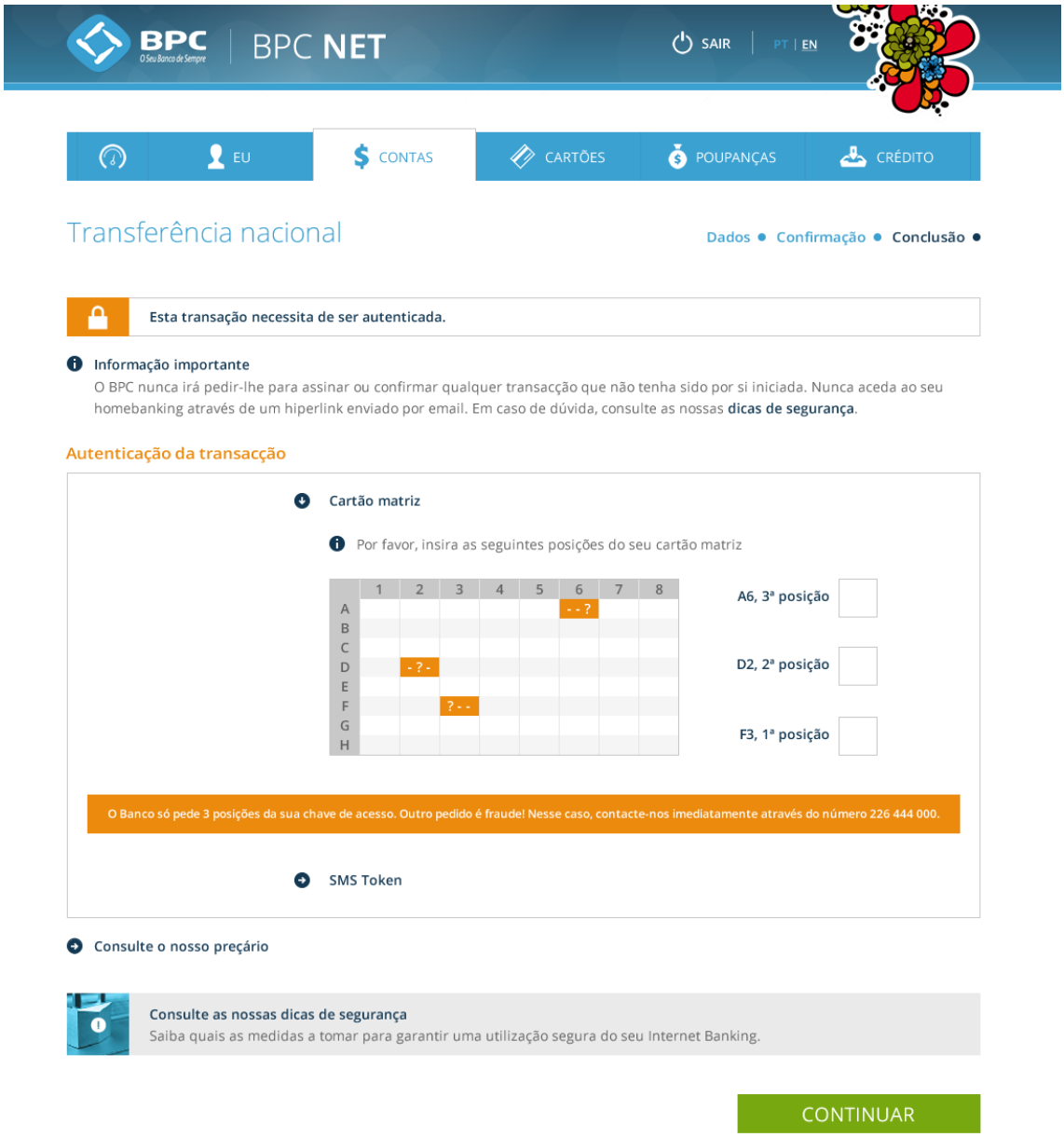


Fig. 5.9: Internet Banking | Autenticação de segundo nível

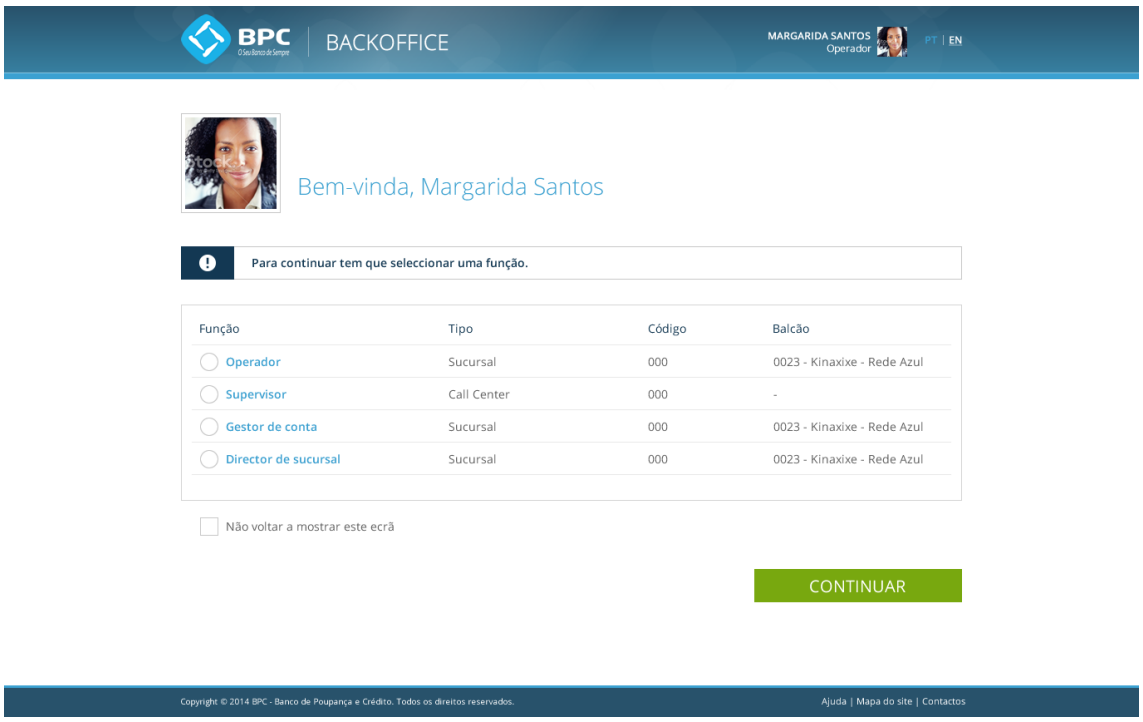


Fig. 5.10: Backoffice | Login

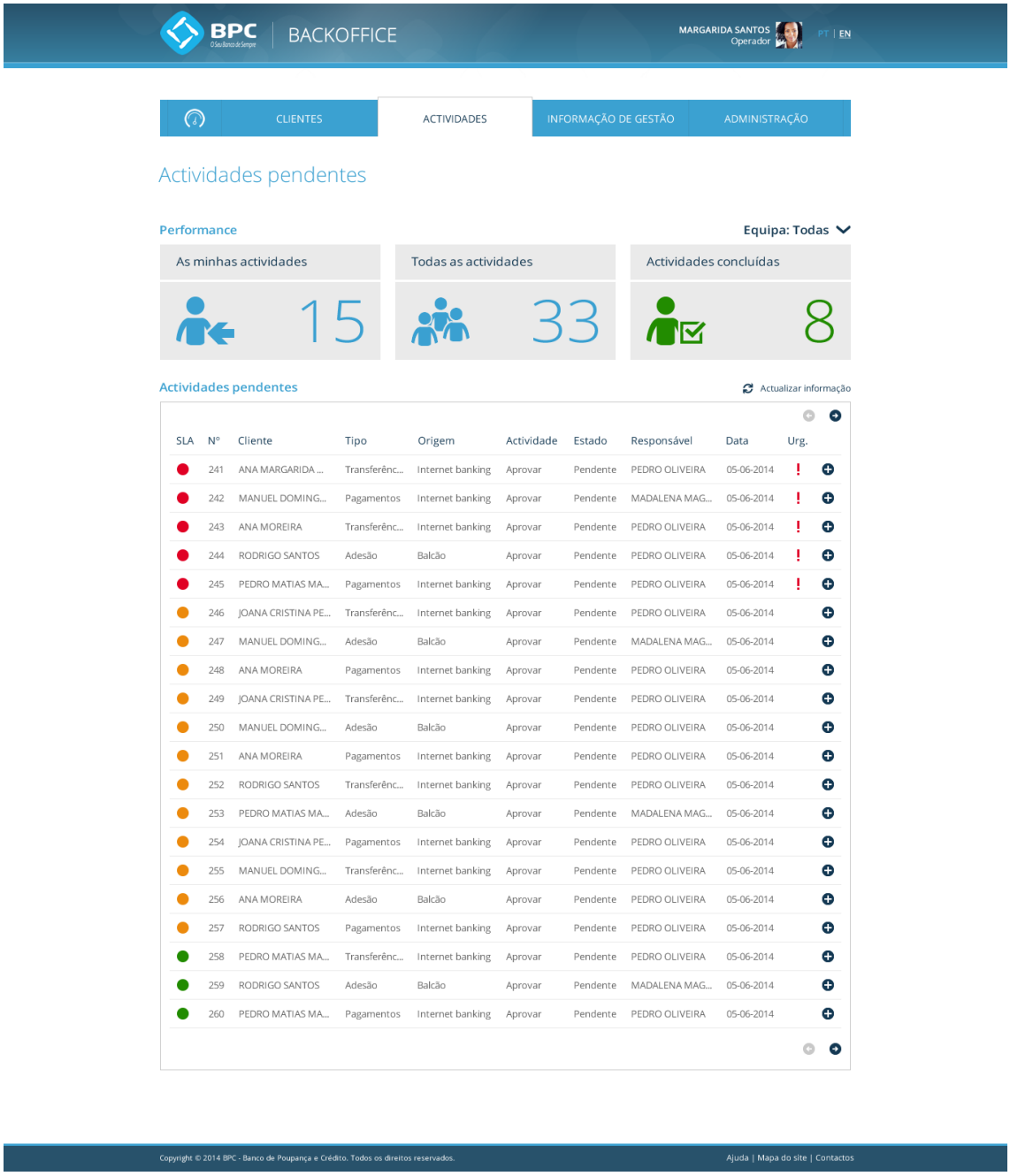


Fig. 5.11: Backoffice | Lista de processos

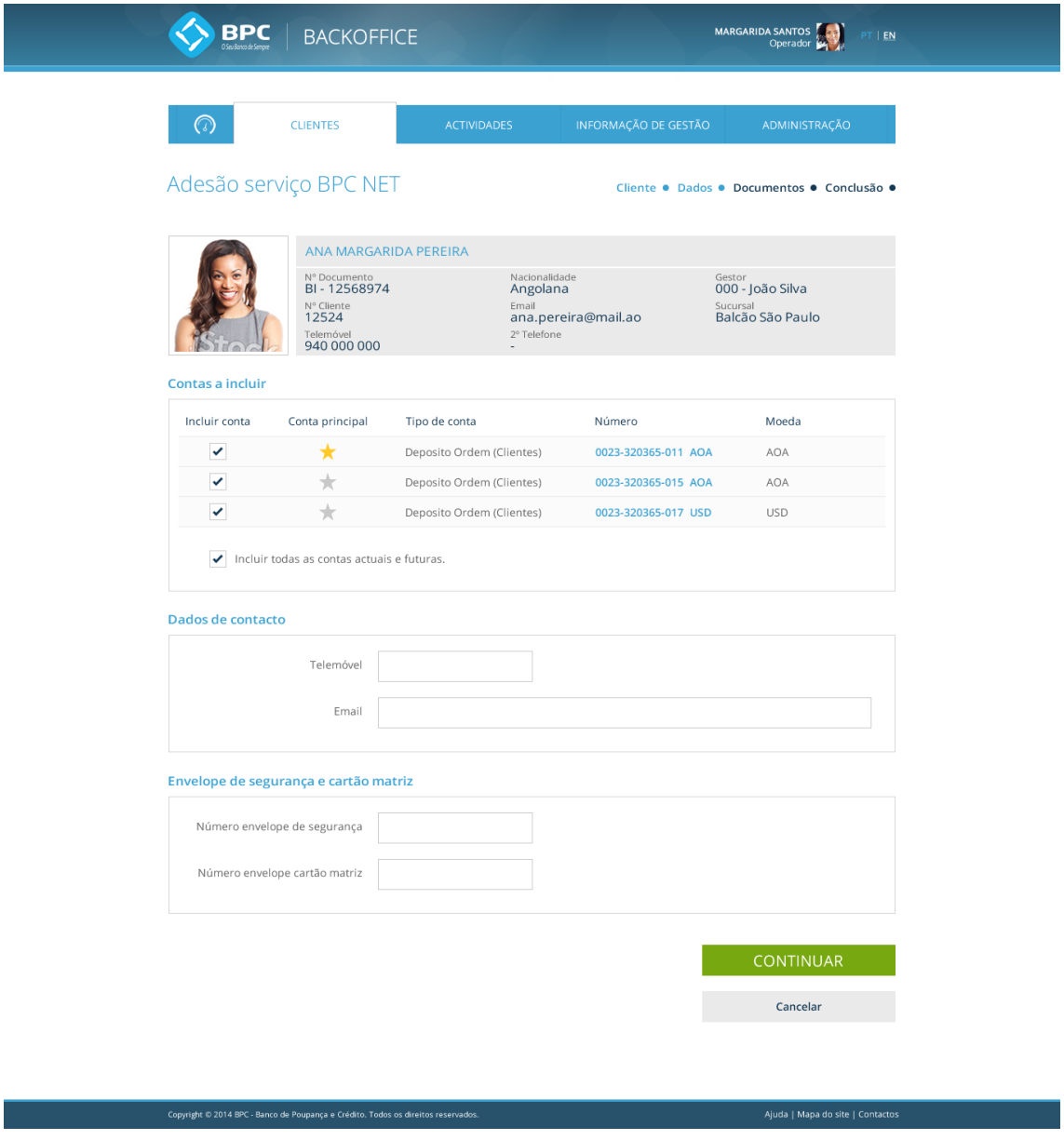


Fig. 5.12: Backoffice | Adesão de Cliente

5.4 Medidas de Segurança implementadas

Tal como apresentado no capítulo 3 no desenvolvimento de um IB é sempre necessário ter em conta determinados aspetos de segurança. Neste projeto foram implementados vários aspetos de segurança, e de várias ordens, que serão apresentados de seguida.

5.4.1 Segurança Aplicacional

De forma a proteger diferente níveis de acesso a informação (consulta, investimentos, movimentação para fora do património, etc. a plataforma tem a capacidade de suportar diversos níveis de autenticação. É então possível a utilização da password de primeiro nível e as opções de matriz e sms token.

Password 1º nível

A password de 1º nível está definida como numérica de 7 dígitos. O objectivo desta password ser numérica é no futuro poder servir como uma autenticação multicanal completa, ou seja, poder ser utilizada pelo canal Contact Center e nomeadamente pelo IVR Interactive Voice Response (que só permite a introdução de caracteres numéricos).

Regras

Esta password é inicialmente entregue em conjunto com o número de contrato/adesão em mãos no momento de adesão.
Após o primeiro login no IB o utilizador será obrigado a alterar esta palavra-chave. Algumas regras básicas devem ser evitadas para a obtenção de uma palavra-chave segura, nomeadamente:

- Palavra-chave com uma repetição de um só caracter. Ex. (1111111)
- Palavra-chave que represente uma data. Ex. (19750324)
- Palavra-chave que repita trios de números. Ex. (12333789)
- Palavra-chave que repita duos de números. Ex. (22770976)

Introdução da Palavra Chave

Os primeiros ataques aos IB eram menos sofisticados e eram baseados na captura

da introdução de dados através dos teclados. Este software era conhecido como keylogger.
Uma das respostas dadas a este tipo de ataques foi a prevenção utilizando teclados virtuais para a inserção de palavras passe.
Com a evolução do nível de ataques esta protecção tornou-se obsoleta, visto que muitos keyloggers podem funcionar em teclados virtuais.
Por sua vez, o teclado virtual tem um inconveniente porque tipicamente a introdução de palavras-chave por meio do rato, deixa exposto em termos visuais ou de gravação de imagem a password introduzida.
Em conclusão, o teclado virtual protege contra um tipo de software malicioso antigo, mas por outro lado deixa exposto o utilizador ao contacto visual com o écran.
Foi então desenvolvida a introdução de palavra passe através de teclado, visto que se o cliente tiver o seu computador devidamente protegido o risco de ver a sua palavra-chave roubada será mínimo.

Armazenamento

As passwords de segurança residem no repositório de dados da plataforma BPCNet. Uma das regras mais importantes para evitar quem tem acesso a base de dados de conhecer as passwords do sistema é a encriptação das mesmas.
As passwords são encriptadas segundo o algoritmo RSA (com base em chave pública e privada) apresentado na figura 5.13. Na criação é utilizada uma chave pública que depois só poderá ser desencriptada com a posse de uma chave privada.

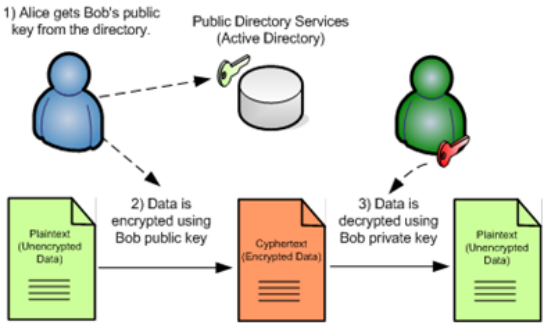


Fig. 5.13: Encriptação RSA para palavras chave

Isto significa que mesmo que algum utilizador tenha acesso aos dados armazenados na base de dados, só conseguirá ler as passwords dos utilizadores, se tiver acesso a chave privada da mesma.

Bloqueio

Em termos externos (Internet) qualquer hacker depois de conhecer o código de utilizador pode utilizar um ataque conhecido como *brute force*, ou seja, tentar diversas vezes a combinação da chave do utilizador até acertar na chave. Este ataque pode demorar algum tempo, mas acaba por ter sucesso.
Para evitar esta situação após o erro consecutivo de 3 vezes da introdução da palavra-chave do cliente, este será bloqueado (este valor pode ser configurado ao nível da plataforma, mas é considerado um valor de referência para este tipo de situações).
Este contador é zerado sempre que o utilizador acerta na palavra chave.

Desbloqueio

Pelo tipo de ataque acima exposto, o desbloqueio da password é uma operação muito sensível. Existem diversas instituições que não permitem o desbloqueio da mesma.
De notar que o desbloqueio, não significa fornecer a password antiga para o utilizador mas sim, efetuar o reset do contador de bloqueio das transações.
Neste caso, optou-se pela solução de disponibilizar uma hipótese de desbloqueio (reset do número de tentativas). Esta situação não está disponível na plataforma online (IB ou Apps). Foi então montada uma funcionalidade que permite ao call center aceder à aplicação de backoffice e executar o desbloqueio da credencial.

Recuperação de palavra chave

Em termos de segurança a recuperação de palavra chave é uma prática completamente reprovada. Desta forma, a plataforma não permite a recuperação de uma palavra-chave perdida.
Se um utilizador não se recordar da password (bloqueada ou não), deverá efetuar no balcão a requisição de um novo envelope com um nova password. A entrega de um novo envelope vai obrigar a impressão de um novo contrato e a assinatura do mesmo.

Validade da palavra chave

UmA das boas práticas de segurança para a password é a sua alteração sistemática. A plataforma com esta funcionalidade. A periodicidade desta alteração pode ser configurada (3 meses, 6 meses, 1 ano, ...)

Coordenadas

De forma a aumentar o número de combinações possíveis para uma chave de 2º nível, a alternativa implementada é a utilização de um cartão de coordenadas. Como o

seu próprio nome indica, o cartão matriz tem um formato de tabela (apresentado na figura 5.14 com várias coordenadas que podem ser pedidas no ato de aprovação de uma operação.

	1	2	3	4	5	6	7	8
A	237	843	633	775	968	733	359	108
B	129	197	417	856	819	507	754	219
C	936	918	150	328	927	974	986	491
D	238	676	466	448	973	602	879	829
E	812	748	993	584	478	269	381	876
F	348	924	171	954	232	237	122	361
G	314	148	660	456	750	648	748	497
H	229	644	647	278	737	937	174	417

Fig. 5.14: Formato de Cartão Matriz

Como exemplo, deste cartão coordenada são requisitadas ao utilizador 3 posições da matriz. Por exemplo para o pedido de coordenada A1 - digito 2, G7 digito 1, F4 digito 3: O utilizador deve introduzir, conforme indicado na figura 5.15, os números 3, 4 e 7.

A interface para requisição de posições do cartão matriz é a indicada na figura 5.16.

	1	2	3	4	5	6	7	8
A	237	843	633	775	968	733	359	108
B	129	197	417	856	819	507	754	219
C	936	918	150	328	927	974	986	491
D	238	676	466	448	973	602	879	829
E	812	748	993	584	478	269	381	876
F	348	924	171	954	232	237	122	361
G	314	148	660	456	750	648	748	497
H	229	644	647	278	737	937	174	417

Fig. 5.15: Resposta ao *challenge* de cartão matriz

As posições do cartão matriz, após inseridas pelo utilizador na interface, são comparadas com o cartão matriz atribuido ao utiulizador através de um método

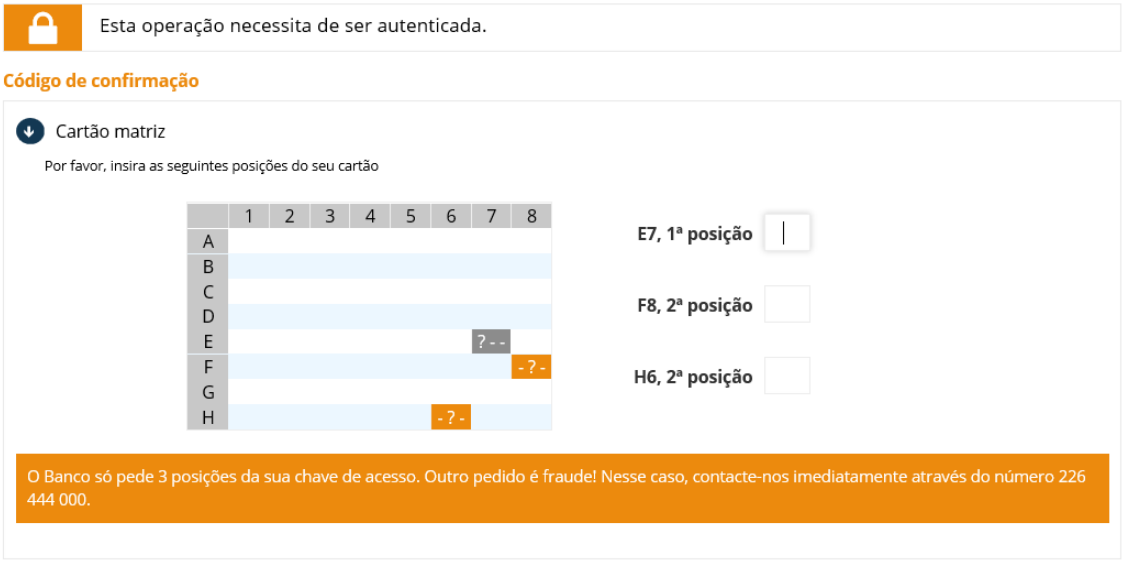


Fig. 5.16: Interface de inserção de posições de cartão matriz

hash, ou seja, não existe uma comparação direta com as posições do cartão.
Se o utilizador se enganar em alguma posição, a próxima tentativa vai sempre gerar a mesma posição. Só quando acertar este pedido é que será gerado um novo.
O pedido de À semelhança da chave de 1º nível esta chave também bloqueia ao fim de 3 tentativas. Derivado a sensibilidade deste tipo de chave (permitir alterações ao património do cliente), para recuperar uma chave perdida o utilizador é obrigatório dirigir-se ao balcão para a sua recuperação.

SMS Token

Outra opção mais dinâmica é a utilização do telefone como recetor da credencial forte. A vantagem desta solução é que a chave enviada é sempre diferente da chave anterior. Sendo assim mesmo que alguém intercete esta chave ou visualize o utilizador a digitar a mesma, não há risco de reutilização porque a chave requisitada na próxima tentativa será sempre diferente da chave atual.
Sempre que o utilizador tentar efetuar uma operação definida para validação como smstoken ser-lhe-á enviada uma mensagem com um número de 7 dígitos para o seu telefone em forma de sms. Para além deste número ser-lhe-á indicada mais alguma informação, tal como a operação que vai ser validada e o montante envolvido.
Este tipo de credencial obriga alguns cuidados na atribuição e visualização do te-

lefone nas plataformas de homebanking, uma vez que este passa a ser considerado uma credencial forte. A interface típica para introdução deste tipo de credencial é apresentada na figura 5.17

Fig. 5.17: Interface de inserção de posições de sms token

Nesta funcionalidade não há bloqueio no envio de SMS por tentativas, uma vez que o número gerado é sempre diferente. É sempre utilizado o último SMS, ou seja, se houver 2 pedidos seguidos o primeiro é ignorado e só será validado o segundo. Em caso de 3 erros seguidos o contrato do cliente é bloqueado e o cliente deverá se dirigir aos balcões para recuperar o acesso do mesmo.

5.4.2 Execução de Operações

A camada transversal do *middleware* é o responsável por correr para todas as operações e efectuar o código comum, não sendo preocupação dos desenvolvedores de transacções estas validações/tarefas para cada uma das operações disponibilizadas. Os primeiros passos do fluxo apresentado na figura 5.18 correspondem a execução de um conjunto de validações:

- Validação da sessão: valida se a sessão do cliente é valida (existe e não expirou);
- Validação da ação: verifica se foi iniciada uma ação pelo método initAction, e se a mesma ação ainda não foi registada como concluída;
- Validação da operação: este passo confronta o identificador de tipo de operação e canal com o catálogo de operações e valida se a operação está activa para o canal;
- Validação da conta base: a validação da conta base é o processo mais complexo e que depende do filtro de contas. Esta filtragem de contas segue dois passos distintos:

  1. Definição da visibilidade global da conta;

2. Validação da conta por operação / canal.

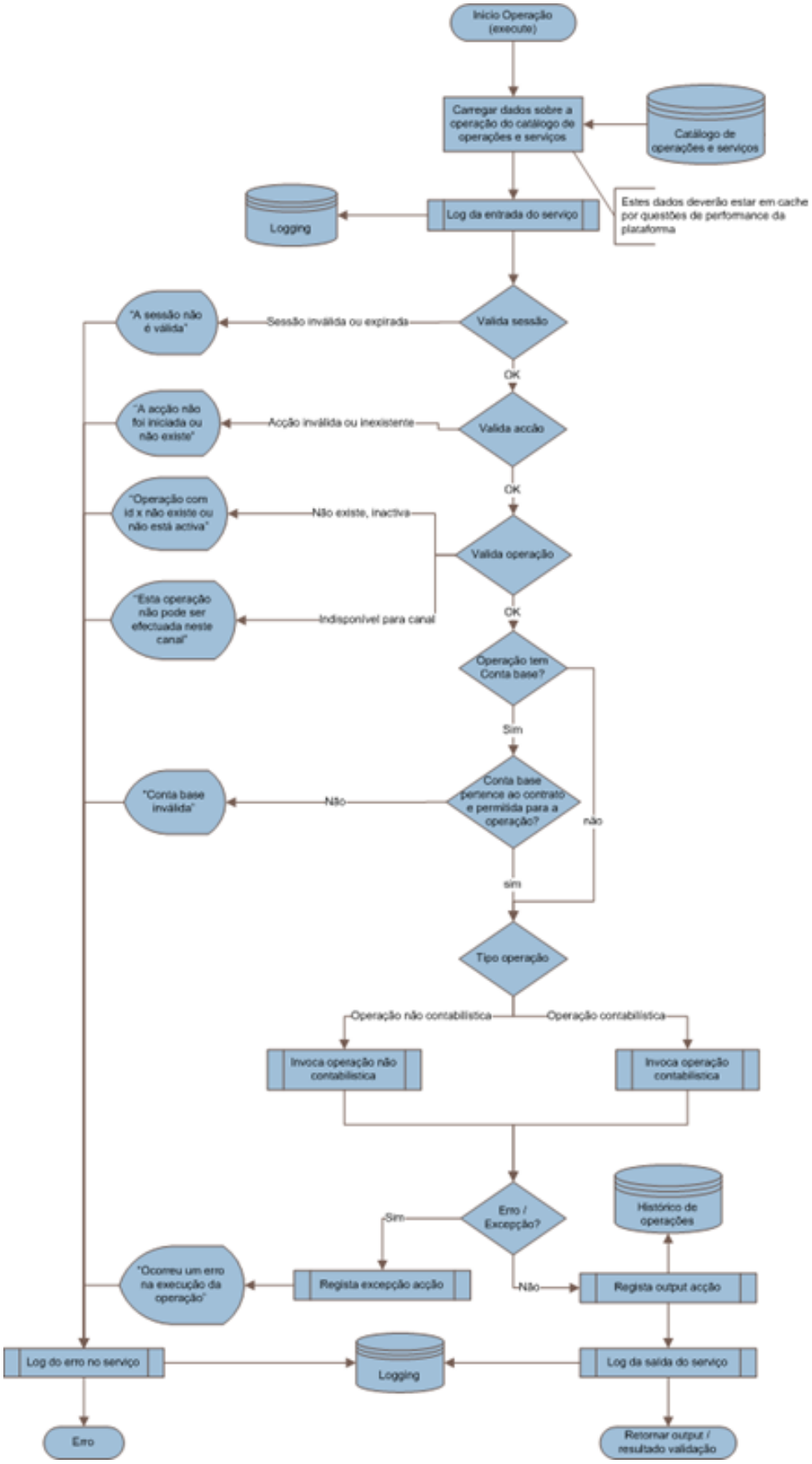


Fig. 5.18: Fluxo de validações de segurança na execução de operações

5.4.3 Data/hora e dispositivo do último acesso

Esta informação é apresentada ao cliente sempre que é efetuado um Login com sucesso. No caso de o utilizador detetar que o último Login não foi efetuado por ele (seja pela data ou pelo dispositivo utilizado) este deve contactar o BPC para reportar o acesso ilícito.

5.4.4 Histórico de Operações

O histórico de operações permite rever o que quais as operações executadas na conta não relacionadas com transações bancárias. Podemos consultar, por exemplo, os últimos logins, mudanças de password, últimos contactos, etc.
O utilizador pode a qualquer altura consultar o seu histórico e reportar qualquer atividade suspeita ao BPC.

5.4.5 Logout Automático

O Logout automático é uma funcionalidade que previne aceder a uma sessão após algum tempo de inatividade.
O Logout automático deve ser realizado em duas camadas:

- A sessão na camada de serviços deve ser terminada, impossibilitando a mesma cookie ou sessionID de realizar pedidos adicionais;
- Uma navegação para a página pública (ou para fora das páginas privadas) no front-end da aplicação.

Este mecanismo ajuda a mitigar o uso ilícito em casos que um utilizador se esquece de terminar a sessão no browser ou nas aplicações.

5.4.6 Análise IP's

Através da análise de IP's é possível adicionar uma camada de segurança. Existem duas validações que se podem realizar:

- Validar se o IP durante uma sessão é sempre o mesmo, permite evitar hijack de sessões.
- Através de geo-referenciação, detectar tentativas de login consideradas suspeitas por serem realizadas num curto espaço de tempo em países separados ou

mesmo primeiras tentativas em países suspeitos (certas gamas de IP atribuídas na Rússia, etc.)

5.4.7 Segurança Serviços REST

Os serviços REST estão, tal como indicado, disponibilizados para a Internet, de forma a serem consumidos pelas Apps. Desta forma, é necessário assegurar que os pedidos de execução destes serviços são fidedignos.
Desta forma, sempre que é efetuado o pedido de execução de um serviço da lista de serviços desenvolvidos, foi desenhado um mecanismo que permite ler diversas informações do contexto HTTP responsável pelo pedido, utilizando estas informações para popular o *Header* do serviço SOAP que executa a operação. As informações obtidas do contexto HTTP são as seguintes:

- Session Id;
- Application;
- Credential Type;
- Token;
- User;
- Language;
- Operation Id;
- Request Id;
- Credential Type;

5.4.8 Segurança Servidores e Ligação

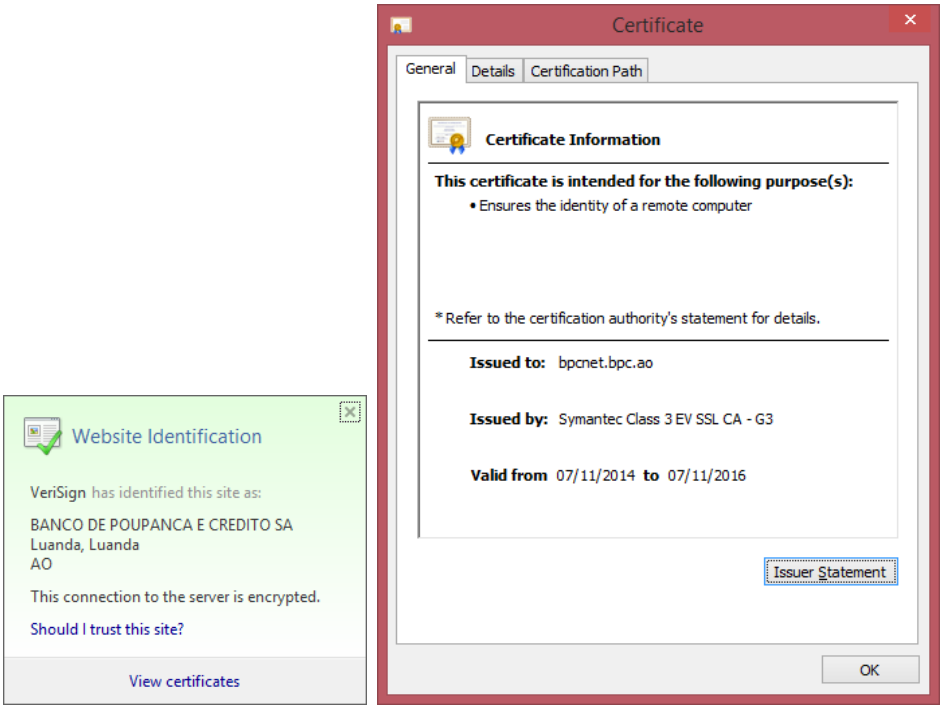
DMZ

Para segurança dos sistemas internos do BPC a ataques, os servidores que expõem o Internet Banking e os serviços REST para utuilização pelas Apps móveis estão protegidos por uma DMZ com uma arquitetura *Multiple Firewall*.
Este tipo de arquitetura permite que os servidores que expõem a camada externa estejam protegidos por uma firewall à entrada e outra firewall na comunicação entre

este servidor exposto na Internet com a intranet do banco.
Desta forma, os servidores de intranet ficarão seguros contra ataques externos.

Certificado Digital

Tal como apresentado na secção 3.2 é importante a instalação de um certificado digital, de forma a atestar a entidade responsável do IB e ainda para ser possível a transmissão segura de informações através de Internet.
No caso do BPC foi instalado um certificado digital SSL EV com protocolo TLS V1.2 com algoritmo RSA 2048-bit para a criação de chaves privadas (figura 5.19.



(a) (b)

Fig. 5.19: Detalhes do certificado digital instalado: a) entidade responsável; b) detalhe de certificado.

Para atestar a segurança do certificado, foi realizado um teste na ferramenta disponibilizada pela Qualys que permite atestar qual o rating do certificado digital numa escala de A a F, sendo estes, respetivamente, o melhor e pior ranking.
Fazendo o teste pelo host https:
bpcnet.bpc.ao verificamos que atualmente o site se encontra no ranking B, conforme apresentado na figura 5.20.

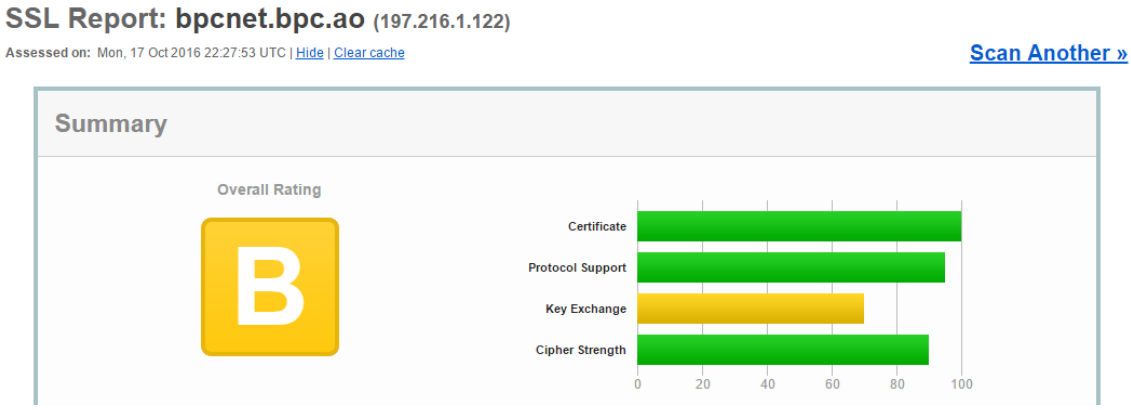


Fig. 5.20: Avaliação do certificado digital instalado na plataforma.

5.4.9 Configuração de conteúdos de segurança

A maior parte das fraudes é causada pelo descuido dos utilizadores quer na disponibilização das suas credenciais, quer na instalação de software de proveniência duvidosa que permite a instalação de malware (software malicioso).
É importante que a plataforma esteja munida de conteúdos que permitam alertar o utilizador de vários comportamentos que deve ter na utilização de um IB. Os conteúdos parametrizados podem ser resumidos da seguinte forma:

- Não utilizar computadores públicos para aceder aos serviços de IB do BPC;
- Memorizar os dados pessoais e não os divulgar;
- Verificar o certificado digital para se certificar que está a aceder aos serviços de IB do BPC;
- Proteger e preservar o cartão matriz;
- Conferir se os dados da operação efetuados no BPC NET, recebidos por SMS Token, estão corretos;
- Verificar as contas regularmente;
- Terminar sempre a sessão BPC NET;
- Limpar a cache (ficheiros temporários) do computador;
- Apagar informação privada do disco do computador;
- Manter-se a par da problemática do Phishing e outras tentativas de fraude.

Para além disto, sempre que o cliente abre a página inicial do IB surge um pop-up de segurança que alerta o utilizador para algumas problemáticas, conforme podemos ver na figura 5.21

Fig. 5.21: Pop-Up de segurança ao abrir página do BPC NET.

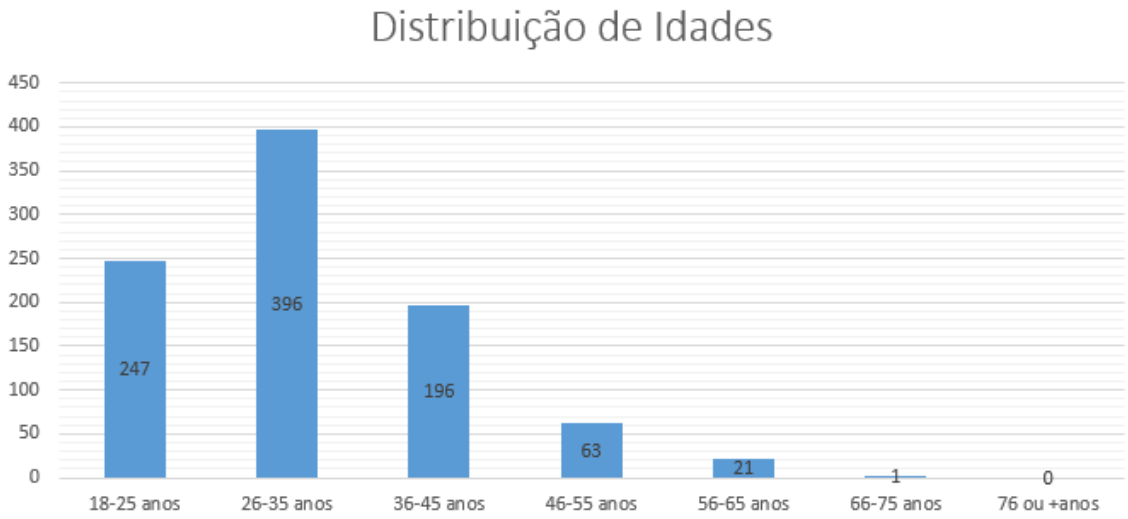
Capítulo 6

Avaliação de Resultados

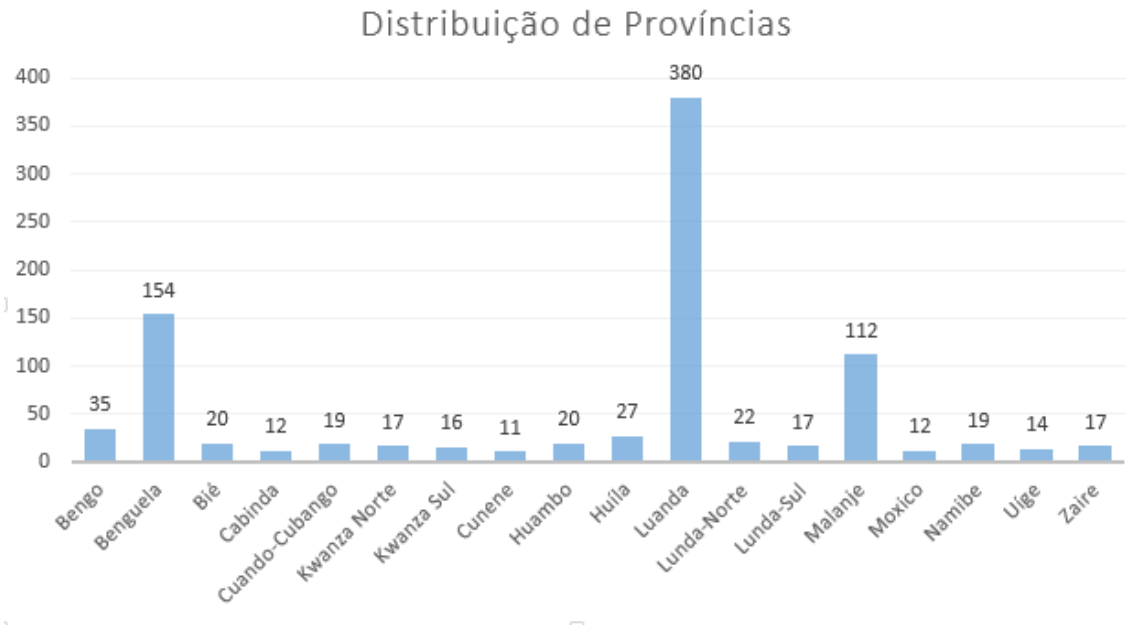
Para avaliação da satisfação dos clientes, em conjunto com o BPC, foi realizado um inquérito de satisfação, com o conteúdo apresentado no Apêndice B.
Para além nisso, com base nos resultados obtidos até ao momento, foi efetuada uma análise estatística do número de operações e adesões. É assim possível efetuar uma análise para vários periodos de tempo, permitindo a geração de uma perspetiva de valores de montante transacionado a atingir a curto prazo assim como uma perspetiva de clientes a aderir ao serviço.

6.1 Análise dos Inquéritos de satisfação

A análise efetuada permitiu, por exemplo, apurar quais os principais aspetos que o cliente realça na nova plataforma assim como quais as principais lacunas do IB, de forma a planear trabalho futuro sobre a plataforma, no âmbito de manutenção evolutiva da aplicação.
Inicialmente e para perceber qual a população envolvida foi efetuada uma média de idades e uma avaliação das províncias onde vivem os clientes que responderam aos inquéritos. Após acompanhar o BPC na distribuição dos envelopes de segurança pelos diversos balcões e conhecendo a realidade do BPC, é expectável que a maioria dos clientes esteja situado em Luanda.
Após análise dos dados, foi então detectado que a maioria de idades situa-se entre os 26 e 35 anos e são habitantes maioritariamente em Luanda. Estas distribuições estão apresentadas na figura 6.1.
As principais vantagens de desenvolver um inquérito de satisfação são perceber se o cliente se encontra satisfeito com o serviço e se tem alguma sugestão de melhoria.



(a)



(b)

Fig. 6.1: Distribuições de: a) idade e b) províncias dos clientes inquiridos

Para além disto, é permitido perceber quais as principais operações realizadas pelos clientes. Neste caso, realizou-se uma distribuição que relacione o tipo de cliente (particular ou empresa) com as operações que mais utilizavam.

Analisando a figura 6.2 conseguimos facilmente perceber que as transferências são a operação mais executada pelos clientes, tanto particulares como empresas. De seguida surgem as recargas que têm maior incidência para clientes particulares do

que para empresas. O mesmo acontece para a maioria das operações, existindo a exceção das DLI's. As DLI's são maioritariamente operadas por empresas, de forma a pagarem ao Ministério das Finanças Angolano os seus impostos.

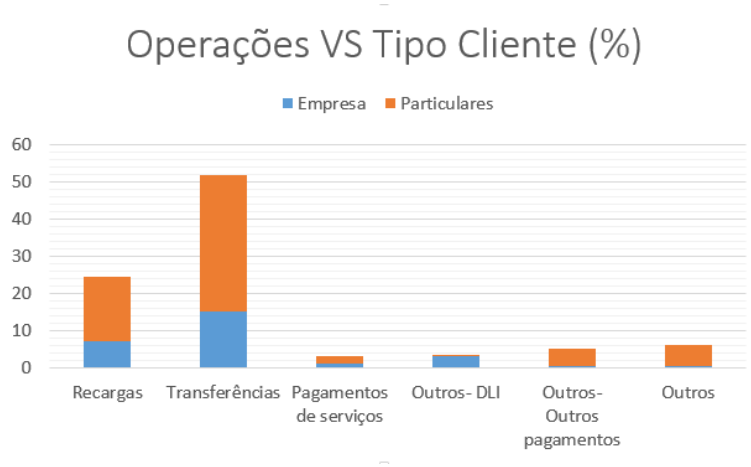


Fig. 6.2: Fluxo de validações de segurança na execução de operações

Relativamente a variáveis de utilização, foi possível analisar os seguintes aspectos:

- Frequência de utilização;
- Aspectos que mais agradam;
- Novas operações;
- Satisfação com plataforma;

Analisando a frequência de utilização (figura 6.3), e analisando o universo de 924 respostas, mais de metade dos clientes diz utilizar a plataforma diariamente ou semanalmente. É necessário ter especial atenção para os clientes que dizem nunca ter utilizado. De referir que os inquéritos foram apenas entregues a clientes que tinham já efetuado uma adesão, ou seja, os clientes efetuaram de facto uma adesão ao serviço, mas ainda não o testaram. Torna-se assim importante que o BPC faça um devido acompanhamento ao cliente, de forma a cativar o cliente para a utilização da ferramenta.

Olhando para os aspectos que mais agradam os clientes, podemos analisar o histograma apresentado figura 6.4. Uma larga maioria dos clientes aprecia o facto de serem disponibilizadas apps para a consulta de contas e execução de operações. Segue-se ainda com alta incidência o gosto pelo aspeto das aplicações, a sua segurança e ainda a lista de operações disponibilizadas. Ao analisarmos o capítulo 2

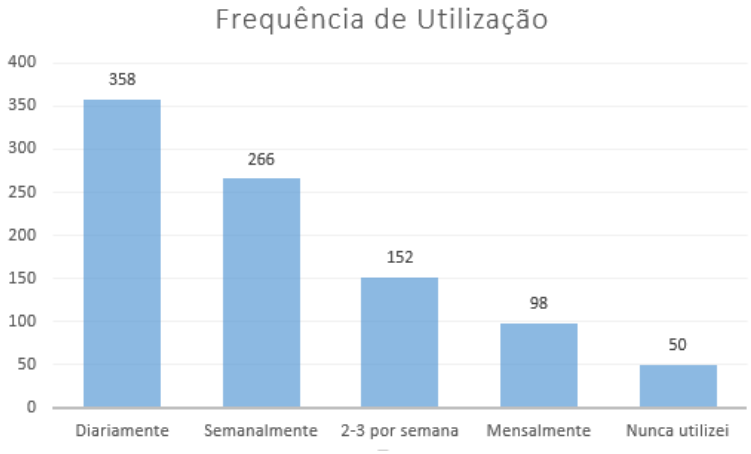


Fig. 6.3: Histograma de Utilização da Plataforma

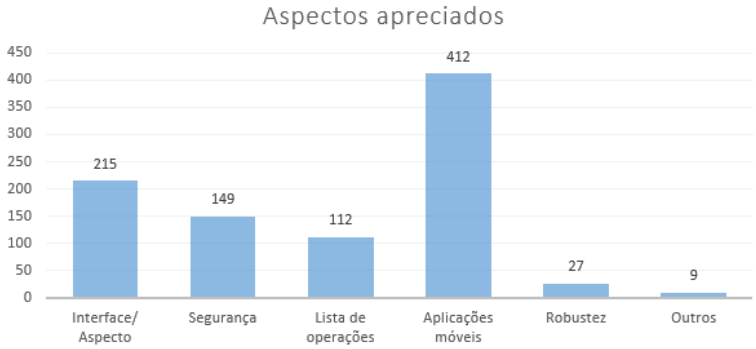
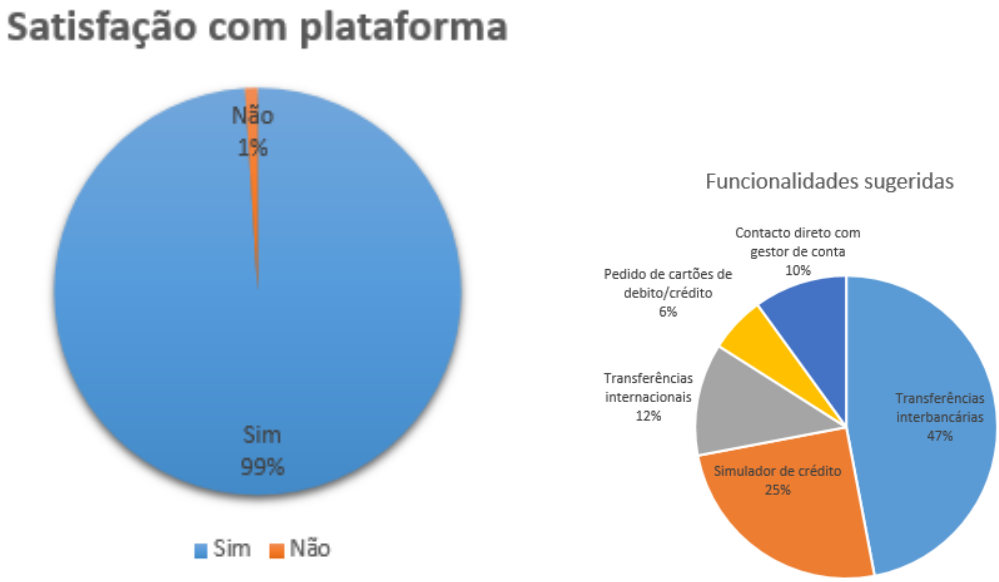


Fig. 6.4: Histograma de Aspectos mais apreciados pelos clientes

conseguimos verificar que estas são as premissas que fazem com que o cliente aumente a sua fidelidade a uma entidade bancária, por exemplo.

Por fim, pode fazer-se uma análise à satisfação geral dos clientes e ainda outra análise a possíveis melhorias na plataforma, incidindo esta melhoria maioritariamente em operações que possam ser adicionadas à plataforma.
Interpretando a figura 6.5, é possível concluir que 99% dos clientes está satisfeito com a plataforma e que a grande sugestão de melhorias está na inclusão de transferências interbancárias no IB (aproximadamente 47%).



(a) (b)

Fig. 6.5: Distribuições de satisfação dos clientes: a) Satisfação e b) Funcionalidades sugeridas

6.2 Análise estatística

Ao efetuar consultas no ambiente de produção, é permitido apurar alguns dados estatísticos, sendo estes dados principalmente relativos a número de adesões efetuadas e a número e montante de transações efetuadas.

6.2.1 Adesões

As primeiras adesões ao serviço ocorreram durante o mês de Janeiro de 2016, onde foram registados a grande maioria dos colaboradores do banco de forma a colocar a solução em piloto interno, isto é, a solução encontrava-se online, mas apenas para utilização por parte dos colaboradores. Desta forma, foi possível perceber qual o impacto que a solução teria para os restantes clientes do banco. No final de Janeiro de 2016, estavam realizadas um total de 2909 adesões, dividindo-se estas em 2450 particulares e 459 empresas.

A partir daqui, o número de adesões foi crescendo de forma gradual, o que indica que os clientes estão a aderir com facilidade à solução. Isto pode dever-se não só pelo "passa a palavra"sobre as plataformas criadas mas também pelas ações de Marketing criadas pelo BPC, de forma a divulgar a nova solução de IB. A tabela 6.1 demonstra a evolução de adesões desde o mês de Janeiro até à data atual (Outubro 2016).

Tab. 6.1: Evolução de adesões

Mês - 2016	Adesões		
	Particulares	Empresas	Total
Janeiro	2450	459	2909
Fevereiro	3781	628	4409
Março	4316	732	5048
Abril	4895	820	5715
Maio	5380	907	6287
Junho	6077	990	7067
Julho	6705	1101	7806
Agosto	7194	1193	8387
Setembro	8327	1343	9670
Outubro	9212	1416	10628

Pode-se ainda, através dos dados indicados, construir uma perspetiva gráfica que permita fazer uma estimativa relativamente a dados futuros.
Analisando a figura 6.6 podemos aferir que o crescimento das adesões tem sido linear, nesta fase inicial.
Apesar das tendências nestes primeiros meses se apresentarem lineares, é estimado que o universo de clientes a aderir ao serviço estagne, visto que a adesão está limitada ao número de clientes do banco. Assim sendo, se fosse analisada a evolução de adesões a um período longo, a distribuição de adesões deveria apresentar-se mais próxima de uma função logarítmica, indicando que o universo de clientes a aderir estagna ao final de determinado tempo. É importante perceber o impacto que a solução está a ter no mercado angolado. Em média, têm sido feitas 750 novas adesões particulares e 106 novas adesões de empresas mensalmente. Estes números comprovam, novamente a importância que os clientes do BPC dão ao novo canal criado para gestão de contas e estão, portanto a aderir em massa ao serviço.

6.2.2 Operações realizadas

O principal retorno do projeto pode ser avaliado, não só através do número de adesões executadas, mas também através do número de operações executadas.
Para os períodos de Janeiro 2016 até Outubro, foram analisados os valores de montante transacionado para uma das operações mais executadas: transferências nacio-

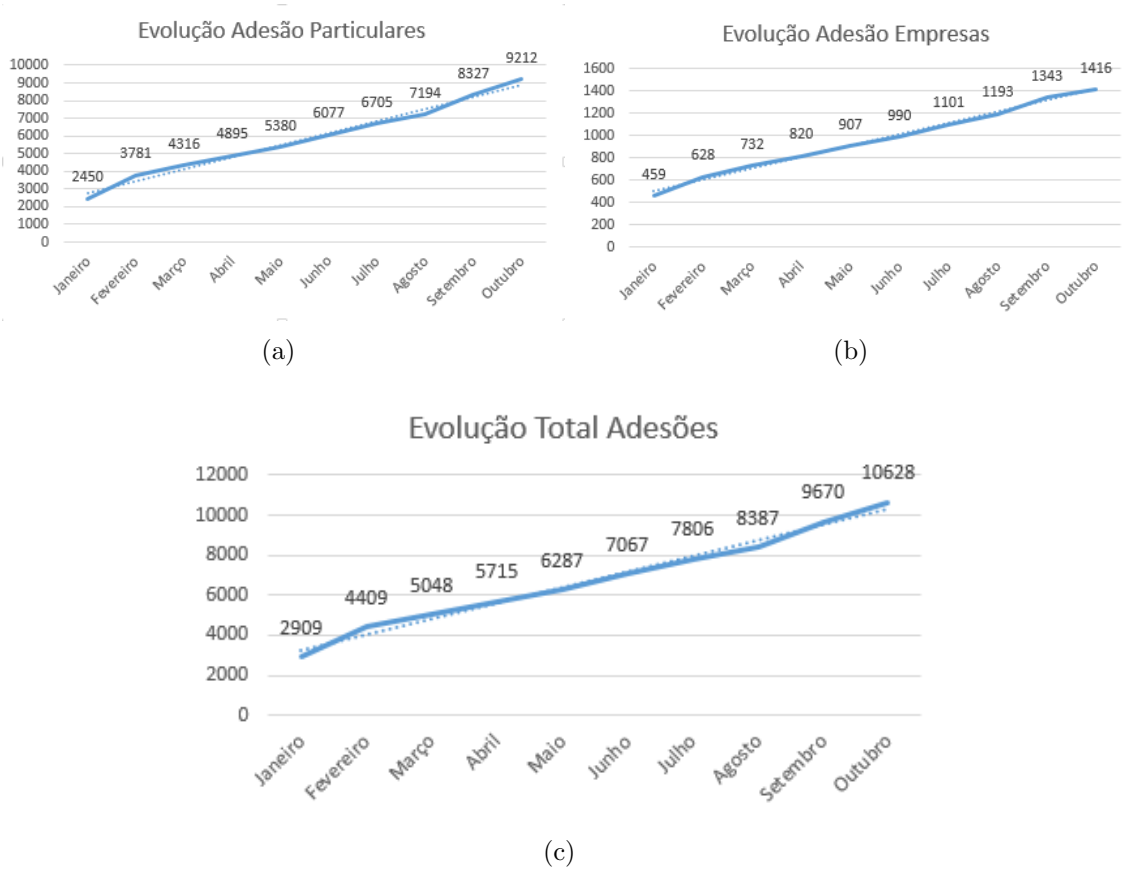


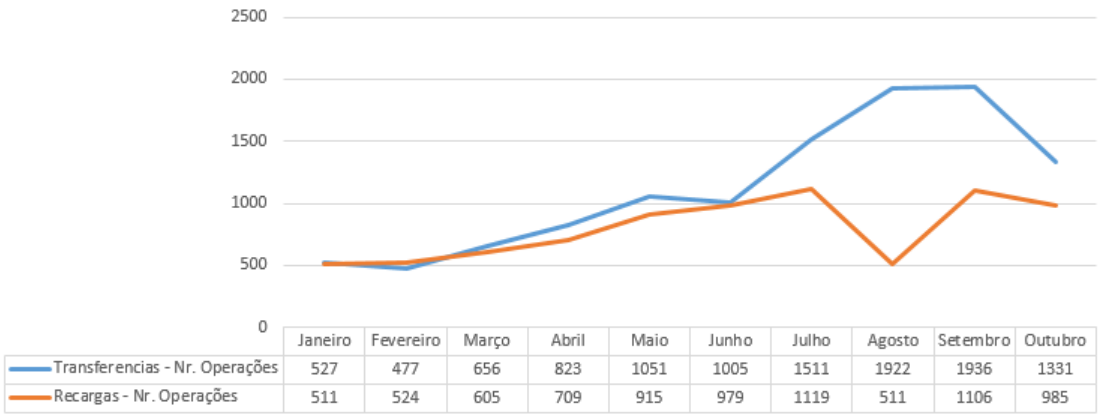
Fig. 6.6: Evolução de Adesões: a) Adesões Particulares; b) Adesões Empresas; c) Total de Adesões

nais e recargas.

Analisando novamente os resultados apresentados na secção 6.1, podemos aferir que as transferências que os clientes mais utilizam são as transferências nacionais e as recargas.

As transferências são de facto uma mais valia, qualquer que seja o mercado em que se esteja inserido. As recargas, no contexto do mercado angolado, são de facto a maior novidade no BPCNet. Até há muito pouco tempo, as recargas em angola funcionavam como um cartão que é vendido em quiosques, onde está digitado um código que permite ao cliente carregar o seu telemóvel.

A inserção desta funcionalidade no BPCNet, transforma-a numa das mais utilizadas, precisamente por ter revolucionado a forma de proceder a um carregamento de telemóvel. Analisando os dados desde Janeiro até Agosto, podemos apurar que, à semelhança do número de adesões, o número de operações executadas tem aumentado substancialmente. (Figura 6.7) Estima-se que, à medida que o universo de clientes



	Janeiro	Fevereiro	Março	Abril	Maio	Junho	Julho	Agosto	Setembro	Outubro
Transferencias - Nr. Operações	527	477	656	823	1051	1005	1511	1922	1936	1331
Recargas - Nr. Operações	511	524	605	709	915	979	1119	511	1106	985

Fig. 6.7: Número de operações realizadas: Transferências Nacionais e Recargas

do BPCNet vai aumentando, a relação entre o número de adesões e o número de operações realizadas seja diretamente proporcional, isto é, aumentando o número de adesões, aumentará também o número de operações executadas e consequentemente o montante transacionado pelo novo canal.

De realçar que existe uma quebra na execução de recargas. Esta quebra deve-se ao facto de ter existido, durante a ultima quinzena do mês de Agosto, uma falha na comunicação EMIS - BPC, que impossibilitou a execução de todo o tipo de pagamentos através do BPCNet.

Capítulo 7

Conclusão

Com o aumento do número de pessoas que têm acesso a serviços de Internet, torna-se importante, qualquer que seja o negócio em que estamos envolvidos, que haja uma adaptação dos serviços disponibilizados de forma a que se acompanhe as tendências do mercado. Desta forma, é de uma importância extrema que o mercado evolua de forma a disponibilizar serviços de Internet que permitam aos clientes executares todas as suas ações através deste meio.

A área da banca não é diferente. Cada vez mais os bancos optam por soluções inovadoras de forma a agilizar operações bancárias sem recurso a agências. Podemos enumerar várias solução, como por exemplo, ATM's, TPA's para pagamento de compras, quiosques e ainda a disponibilização de plataformas na Internet que permitem ao cliente fazerem a sua própria gestão das suas contas.

Um IB é de facto uma ferramenta que se pode tornar uma mais valia, qualquer que seja o mercado em que está inserido. Por norma, os clientes sentem-se satisfeitos ao utilizar este tipo de ferramentas, pois permite-lhes a execução de quase todo o tipo de operações sem deslocações até agências físicas.

No caso do BPC, a plataforma que tinham disponível era demasiado antiga e apresentava muito poucas funcionalidades. Para além disto, apresentava uma enorme dependência do administrador da plataforma, de forma a que funcionasse corretamente.

Analisando os objetivos apresentados na secção 1.2, podemos admitir que todos estes foram cumpridos.

Numa fase inicial, foram identificadas todas as ameaças que podem comprometer a segurança financeira dos clientes. Conceitos como *phishing*, *SQL Injection*, *malwares*, etc. foram devidamente analisados. Para todos os conceitos, foram analisadas

formas de anular estas ameaças.
A solução desenvolvida, tal como indicado num dos objetivos, tem como principal preocupação a seua segurança. Era extremamente importante realizar um projeto capaz de dotar o BPC com uma plataforma segura. As medidas de segurança aplicadas foram variadas mas podem-se resumir em:

- Segurança aplicacional (p.e. utilização de stored procedures para prevenção de *SQL Injection*);
- Validação de execução de operações (p.e. validação de sessões antes de executar uma operação que afete o património do cliente;
- Segurança de servidores (para segurança das infraestruturas);
- onfiguração de conteúdos de segurança (sensibilização dos clientes para aspetos de segurança);

O desenvolvimento do IB era um dos principais objetivos do projeto, pois o BPC encontrava uma enorme lacuna nesta vertente de negócio, possuindo apenas a ferramenta de BPCNet-IFM, que se percebeu ser muito limitada relativamente ao mercado atual. Para além disto, conseguiu ainda perceber-se, após reuniões de análise, que a preocupação sobre a segurança da ferramenta não estava instalada.
Este objetivo, após uma análise cuidada de soluções apresentadas no mercado angolano, foi concluido com sucesso, tendo sido desenvolvida uma plataforma fiável, segura, com um aspeto moderno e inovador. Foram assim disponibilizadas inúmeras funcionalidades que permitem ao cliente ter um controlo perfeito das suas contas bancárias.
Numa comparação com as funcionalidades disponibilizadas na plataforma que os clientes BPC utilizavam, podemos enumerar muitas funcionalidades com as quais estes não tinham tido contacto.

- Gestão de contas poupanças (liquidação, constituição; detalhe);
- Gestão de cartões de crédito / débito (detalhe, cancelamento, movimentos);
- Gestão de créditos (detalhe, plano de pagamentos, movimentos);
- Gestão de perfil (fotografia de perfil, chave de acesso, contactos, favoritos);
- Pagamentos (serviços, carregamentos, outros, recargas);

A plataforma desenvolvida foi disponibilizada em Janeiro de 2016, a partir de quando começaram a ser angariados novos clientes.
Para além do desenvolvimento desta plataforma, e como foi enunciado inicialmente, um dos maiores objetivos era também tornar a plataforma multicanal, isto é: permitir que o desenvolvimento da plataforma forneça os recursos necessários para que, em resposta à proliferação de equipamentos móveis, seja concedida a possibilidade de um futuro desenvolvimento de apps. Desta forma, e através do desenvolvimento de serviços REST, pode dar-se como atingido o objetivo.
Desde então, os serviços desenvolvidos já começaram a ser utilizados e estão já disponibilizadas apps para os diferentes sistemas operativos existentes no mercado (iOS, Android, Windows).
Outro grande objetivos era fornecer à DSE uma plataforma intranet que lhes permita executar a correta gestão de todos os contratos de adesão gerados. Foi para isso gerado o Backoffice da aplicação. É através desta aplicação que os colaboradores do banco aprovam contratos de adesão ao IB. Funcionalidades como adesões, gestão de contratos, resposta a mensagens seguras provenientes do IB passaram a ser possíveis através desta ferramenta. A ferramenta torna-se importante em todo o projeto pois permite fornecer ao cliente um suporte mais rigoroso na utilização do IB, assim como um serviço mais organizado e mais rápido quando é recebido um pedido de adesão.
A análise de estatísticas e a análise dos inquéritos realizados permitem-nos perceber que os clientes se encontram satisfeitos com a aplicação e que o número de clientes a aderir continuará a crescer temporalmente, tendo o projeto, mais uma vez, sido bem sucedido.

Futuramente, é necessário ter em conta as necessidades dos clientes, as suas reclamações e sugestões.
É assim importante apostar na manutenção corretiva e evolutiva das plataformas criadas, pois só assim estaremos na presença de uma solução em constante evolução.
Relativamente à manutenção evolutiva, é muito importante, como já foi referido, ter em atenção as necessidades e sugestões dos clientes. O resultado do inquérito pode então mostrar que estes pretendem ver disponibilizadas as transferências entre diferentes bancos e ainda um simulador de crédito.
Para além destes aspectos, é importante fazer uma análise cuidada a novos ataques que possam surgir, que podem comprometer a segurança dos utilizadores e do seu património.

Na insurgência de um novo tipo de ataque, é necessário estudar a sua prevenção e deve ser realizada, no âmbito de manutenção evolutiva, uma nova intervenção na solução.

Bibliografia

Albertin, A. L. (1999), 'Comércio eletrônico: um estudo no setor bancário', *Revista de Administração Contemporânea* **3**(1), 47–70.

Angola, K. (2012), Análise ao Sector Bancário Angolano, Technical report.

Blatz, J. (2011), 'CSRF: Attack and Defense', *McAfee* .

Diniz, E. H. (2000), 'Evolução do uso da web pelos bancos', *Revista de Administração Contemporânea* **4**, 29–50.

Freitas, J. P. J. (2007), 'Como evitar ataques de engenharia social'.

Gadgil, S. (2013), 'SQL Injection Prevention in Banking', *International Journal of Computer Science and Information Technologies* **4**(2), 345–349.

International, T. (2016), *Transparency International | the global coalition against corruption*, http://www.transparency.org/cpi2015results-table.

Klein, A. (2002), 'Cross Site Scripting Explained', *Sanctum Security Group* .

Lau, M. (2006), Análise das fraudes aplicadas sobre o ambiente internet banking, Master's thesis, Curso de Engenharia da Escola Politécnica da Universidade de São Paulo.

Lau, M. (2010), 'Técnicas utilizadas para efetivação e contenção das fraudes sobre Internet Banking no Brasil e no mundo'.

Meuter, M. L. e. a. (2000), 'Self-service technologies: understanding customer satisfaction with technology-base services encounters', *Journal of Marketing* **64**, 50–64.

Microsoft (2012), Framework .net 4.0, Technical report, https://msdn.microsoft.com/en-us/library/ms171868(v=vs.100).aspx.

Moreira, F. (2010), Evolução de software e serviços web, Master's thesis, Instituto Superior de Engenharia do Porto.

O'Donnell, G. (2002), 'Secure DMZ Infrastructure Management', *MetaGroup* .

Oliver, R. L. (1999), 'Whence consumer loyalty', *Journal of Marketing, New York* pp. 33–44.

Parasuraman, A. & Grewal, D. (2000), 'The impact of technology on the quality-value-loyalty chain: a research agenda.', *Journal of the Academy of Marketing Science* **28**(1), 168–174.

Porter, M. E. (2001), 'Strategy and the Internet', *Harvard Business Review OnPoint* pp. 61–78.

Ramos, A. S. M. & Costa, F. S. P. H. A. R. (2000), 'Serviços bancários pela Internet: um estudo de caso integrando a visão de competidores e clientes', *Revista de Administração Contemporânea* **4**(3), 133–154.

Ristic, I. (2014), 'SSL/TLS Deployment Best Practices', *Qualys SSL Labs* .

Souto, J. H. (2012), Aplicação sig: Gestão de pontos de interesse de entidades, Master's thesis, Instituto Politécnico de Bragança: Escola Superior de Tecnologia e Gestão.

Spett, K. (2005), 'Cross-Site Scripting: Are your web applications vulnerable?', *SPI Dynamics* .

Szymanski, D. & Hise, R. T. (2000), 'E-satisfaction: an initial examination', *Journal of Retailing* **76**(3), 309–322.

Tomiuk, D. & Pinsonneault, A. (2001), 'Customer loyalty and electronic -banking: a conceptual framework', *Journal of Global Information Management* **9**(3), 4–14.

Turban, E. e. a. (2000), 'Electronic commerce : a managerial perspective'.

Vale, C. K. G. (2012), Gestão de crédito, Master's thesis, Escola Superior de Saúde de Viseu.

Wendel, G. H. (2011), 'Malwares VS Antivirus', *H2HC Fourth Edition* .

Zilber, M. A. & Caçador, M. F. (2003), 'O Internet Banking como fator de fidelização na estratégia de relacionamento com clientes no setor bancário', *Universidade Mackenzie* pp. 1–3.

Apêndice A

Contrato de Adesão

A concretização de uma adesão é dada quando é gerado automaticamente pela plataforma de backoffice um contrato de adesão apresentado ao cliente para respetiva validação e assinatura.
O contrato apresentado seguidamente é semelhante ao gerado.

Contrato de adesão ao serviço BPC NET - Particulares

Conta	Nº Cliente	Balcão	Data	Nº Contrato
			/ /	

Dados Cliente

Nome:

Email:

Telemóvel:

Conta Principal

Tipo de conta	Número	Moeda
	- -	
	- -	
	- -	
	- -	
	- -	

Declaro serem verdadeiras as informações prestadas, tomo conhecimento e aceito as Condições Gerais de Utilização do BPC NET. Autorizo o débito de todas as despesas inerentes a utilização dos serviços do BPC NET. Declaro, igualmente, consentir o tratamento informático pelo BPC de todos os dados pessoais constantes no presente pedido de adesão, mediante sua inclusão na base de dados do Banco. O BPC assegura aos titulares dos dados pessoais os direitos de acesso, correcção, supressão, sempre que legitimamente o solicitem.

Assinatura do Cliente (conforme B.I.)

Assinatura da Gerência

i) O Conferente deverá assegurar o correcto preenchimento do presente impresso e conferir a assinatura do Cliente.

Envelope de segurança e cartão matriz

Número envelope de segurança:

Número envelope cartão matriz:

BPC – O seu Banco de sempre

BPC – Banco de Poupança e Crédito, Largo Saydi Mingas, Luanda – Angola

Caixa Postal nº 1343 | SWIFT Code: BPCLAOLU | Tel: +244 222 390141 | Fax: +244 222 393 790

CONDIÇÕES GERAIS DE UTILIZAÇÃO DO BPC NET – PARTICULARES

Entre o Banco de Poupança e Crédito S.A.R.L, com Sede no Largo Saydi Mingas, na cidade de Luanda, com nº de Identificação Fiscal 5410000552, matriculada na competente Conservatória do Registo Comercial de Luanda sob os números 2129, doravante designado abreviadamente Banco e, o Cliente supra identificado que o subscreve, doravante designado abreviadamente por Cliente.

CONSIDERANDO QUE:

(i) O Cliente é Titular de uma Conta D.O. junto do Banco;

(ii) O Banco pretende disponibilizar aos seus Clientes um serviço que consiste na possibilidade de manter relações com o Banco por via Internet e por outras formas de acesso remoto que venham a ser criadas, para que os Clientes possam:

• Aceder a informação sobre produtos e serviços do Banco;

• Obter informações e realizar operações bancárias sobre Contas de que o Cliente seja Titular;

• Transmitir instruções de cancelamento a todo o Serviço ou individualmente a algum tipo de acesso.

As partes celebram o presente Contrato, que se rege pelas disposições seguintes e subsidiariamente, pelas "Condições Gerais do Contrato de Abertura de Conta".

1. Noções

Para efeito do presente Contrato a palavra:

a) **SERVIÇO –** Significa que o BANCO prestará ao CLIENTE, nos termos deste contrato, o serviço de *Internet Banking* para pessoas singulares, por meio do sistema denominado BPC NET PARTICULARES, com a possibilidade conferida ao Cliente de manter relações com o Banco através do acesso a canais remotos, possibilitando-lhe por este meio o acesso a informações sobre produtos e serviços do Banco, bem como a realização de ordens de transferência, compra, venda, subscrição ou resgate sobre os produtos ou serviços disponibilizados;

b) **CANAIS REMOTOS –** Significa o acesso ao serviço por via Internet, ou outras formas de acesso remoto que venham a ser definidas pelo Banco;

c) **NÚMERO DE ADESÃO –** Compreende um número de identificação do Cliente, constituído por dez (10) dígitos, único, pessoal e intransmissível, que lhe permite aceder ao Serviço;

d) **CÓDIGO SECRETO –** Compreende um número secreto, único, pessoal e intransmissível, definido pelo Banco no momento da Adesão ao serviço e alterado obrigatoriamente pelo Cliente após o primeiro acesso ao Serviço;

e) **CHAVE DE CONFIRMAÇÃO** – Compreende um elemento de identificação, secreto, pessoal e intransmissível, emitido pelo Banco e passível de alteração pelo Cliente sobre a forma de um conjunto de dez (10) caracteres alfanuméricos que são exigidos ao Cliente para a realização de determinadas transacções a efectuar através do serviço.

2. Objecto

Em resultado da celebração do presente contrato, o Cliente passa a poder aceder através do Serviço a todas as Contas de que seja Titular único ou solidário e sem condições particulares de movimentação.

3. Condições de utilização do Serviço

3.1. O Cliente poderá em qualquer altura alterar as Contas a que tem acesso bem como a natureza das operações a que pretende ter acesso através do Serviço.

3.2. O Cliente autoriza o banco a preencher e validar todos os documentos necessários à efectiva realização e liquidação das operações dadas através do Serviço.

3.3. Independentemente de outras regras que sejam definidas no futuro, a identificação do Cliente para acesso ao Serviço processa-se através da indicação pelo mesmo de um Número de Adesão, bem como de um Código Secreto definido pelo Banco no momento da Adesão e alterado obrigatoriamente pelo Cliente após o primeiro acesso efectuado através do Serviço.

3.4. O Banco pode, ainda, a todo o tempo, condicionar a realização de operações através do serviço à indicação pelo Cliente de dados constantes de uma chave (Chave de Confirmação) especialmente concebida para o efeito, que lhe será enviada pelo Banco.

3.5. O Banco poderá, ainda:

3.5.1) Não executar ordens quando não sejam facultados correctamente os dados de validação do Cliente;

3.5.2) Não executar ordens quando existam dúvidas razoáveis sobre a identidade da pessoa que está a transmitir a ordem;

3.5.3) Não executar ordens após um número de tentativas de acesso falhadas a definir pelo Banco; 3.5.3.1Requerer ao Titular que no caso de movimentos de elevado valor as ordens sejam dadas por escrito.

3.5.4) Impedir ou introduzir limitações à realização de determinado tipo de operações através do Serviço, sempre que tal seja imposto ou recomendado em virtude da aplicação das disposições legais vigentes no território ou Estado de residência/nacionalidade do Cliente.

4. Suspensão do Serviço

4.1. O Banco reserva-se o direito de suspender ou fazer cessar o acesso ao Serviço sempre que razões de segurança o justifiquem.

4.2. Ainda por razões de segurança, o Banco pode suspender o acesso ao Serviço global ou parcialmente, caso o Cliente não utilize até 45 dias após a adesão.

4.3. Caso o acesso ao Serviço seja suspenso nos termos do disposto no número anterior, o Cliente poderá solicitar a sua activação mediante pedido dirigido ao Banco.

5. Confidencialidade

5.1. O Banco compromete-se a manter sob rigorosa confidencialidade os Códigos Secretos e a informação constante da Chave de Confirmação atribuídos ao Cliente.

5.2. O Cliente obriga-se a guardar sob segredo o seu Código Secreto e, bem assim, prevenir o seu uso abusivo por parte de terceiros.

5.3. O Cliente é responsável e suportará todos os prejuízos resultantes de uma utilização abusiva do Serviço por terceiros.

6. Responsabilidade

O Banco não será, em caso algum, responsável pelos prejuízos derivados de erros de transmissão, deficiências técnicas, interferências ou desconexões ocorridas.

7. Custos

Independentemente dos custos associados aos meios de comunicação utilizados, o Banco poderá estabelecer um preço pelo Serviço, de acordo com o preçário em vigor no banco.

8. Confirmação de transacções

8.1. A realização de operações através do Serviço é confirmada pelo Banco através do extracto de conta.

8.2. O Cliente poderá solicitar um comprovativo específico para uma transacção, reservando-se o Banco o direito de cobrar uma comissão de acordo com o preçário em vigor.

9. Autorizações

O Cliente autoriza de forma irrevogável o Banco a, sempre que este o considere necessário:

a) Utilizar os registos informáticos como meio de prova para qualquer procedimento judicial que venha a existir directa ou indirectamente entre as partes, podendo o Cliente solicitar ao Banco que lhe forneça cópia ou transcrição escrita do conteúdo das conversações que se tiverem realizado entre ambos;

b) Não executar ordens quando não sejam facultados correctamente os dados de validação do Cliente;

c) Não executar ordens quando existam dúvidas razoáveis sobre a identidade da pessoa que está a transmitir a ordem;

d) Não executar ordens após um número de tentativas de acesso falhadas a definir pelo Banco;

e) Requerer ao Titular que no caso de movimentos de elevado valor as ordens sejam dadas por escrito.

10. Utilização dos dados

10.1. O Cliente autoriza expressamente o banco a proceder ao tratamento informático dos dados fornecidos, bem como a cruzar essa informação com a restante informação por si facultada ao Banco em virtude da abertura de Contas ou de celebração de quaisquer contratos, designadamente para fins de natureza estatística, de crédito, ou para identificação de produtos bancários e financeiros do Banco ou de Empresas do BPC, sem prejuízo do cumprimento do dever do sigilo bancário.

10.2. O Cliente tem o direito de aceder aos elementos a si referentes constantes das bases de dados a que se refere a presente cláusula, de exigir a sua actualização e/ou rectificação, bem como exigir a eliminação do seu nome das mesmas uma vez extinto o contrato.

11. Eficácia Jurídica

11.1. As relações entre o Cliente e o Banco serão regidas por este contrato e pelas condições particulares de cada produto ou operação e, subsidiariamente pelas "Condições Gerais de Abertura e Movimentação de Conta".

11.2. O Banco reserva-se o direito de, a qualquer momento, proceder a alterações às presentes condições, comunicando-as ao Cliente no mais breve período de tempo possível.

11.3. A validade do presente contrato fica condicionada à recepção pelo Banco de um exemplar do contrato devidamente assinado pelo Cliente. 11.4. O Banco reserva-se o direito de autorizar ao Cliente, caso as condições técnicas assim o permitam, o acesso à consulta dos dados constantes da sua conta antes de recepcionado o contrato devidamente assinado.

11.5. As consultas efectuadas nos termos do número anterior presumem-se efectuadas pelo Cliente, declinando o Banco desde já qualquer responsabilidade decorrente da utilização abusiva ou fraudulenta da informação constante da Conta.

11.6. As ordens transmitidas pelo Cliente e executadas pelo Banco através dos meios deste contrato, gozarão de plenos efeitos jurídicos, não podendo o Cliente alegar a falta de assinatura para o cumprimento das obrigações assumidas nessas ordens.

12. **Modificação de Dados**

O Cliente compromete-se a informar o Banco de qualquer alteração de morada, ou de quaisquer outros dados que tenham sido transmitidos anteriormente.

13. Informação Financeira

13.1. A informação financeira disponibilizada através do Serviço, designadamente, cotações, índices, notícias, estudos ou outra informação financeira é obtida através de outras entidades, não podendo o Banco e as entidades que a prestam ser responsabilizados pela eventual incorrecção dos dados fornecidos ou pela má percepção, interpretação ou utilização da informação transmitida. 13.2. A informação é propriedade das entidades que a prestam, comprometendo-se o Cliente a não a transmitir ou reproduzir, quaisquer que sejam os meios empregues.

14. Duração

O presente contrato durará por prazo indeterminado. Podendo qualquer das partes pôr-lhe termo mediante simples comunicação à outra parte.

15. Jurisdição Competente

15.1. Este contrato será regido pela Lei Angolana. 15.2. Para a resolução de eventuais questões emergentes do presente contrato é estipulado o Foro no Tribunal da Província competente, com expressa renúncia a qualquer outro.

Assinatura do Cliente (conforme B.I.)

Assinatura da Gerência

Data: «Data»

BPC – O seu Banco de sempre

BPC – Banco de Poupança e Crédito, Largo Saydi Mingas, Luanda – Angola
Caixa Postal nº 1343 | SWIFT Code: BPCLAOLU | Tel: +244 222 390141 | Fax: +244 222 393 790

Apêndice B

Inquéritos de Satisfação

No sentido de averiguar a satisfação dos clientes, em conjunto com o departamento de Marketing do BPC, foi efectuado o inquérito apresentado nas páginas seguintes.

BPC | BPC - NET

Inquérito de satisfação

De forma a avaliar a sastifação do cliente com a nova plataforma de *internet banking* – BPC NET, solicitamos que preencha o seguinte inquérito. A sua avaliação é importante na melhoria deste serviço.

1. Idade

☐ 18-25 ☐ 26-35 ☐ 36-45 ☐ 46-55 ☐ 56-65 ☐ 66-75 ☐ 76+

2. Genéro

☐ Masculino ☐ Feminino

3. Tipo de cliente

☐ Particular ☐ Empresa

4. Província

_____

5. Agência

_____

6. Com que frequência costuma utilizar o *internet banking*- BPC NET?

☐ Diariamente ☐ Semanalmente ☐ 2-3 por semana ☐ Mensalmente
☐ Nunca utilizei

7. Qual a funcionalidade que mais utiliza?

Selecione o máximo de 3 funcionalidades:
☐ Recargas ☐ Transferências ☐ Pagamento de serviços
☐ Constituição de poupança ☐ Liquidação de poupança
☐ Requisição de cheques ☐ Outro: _____

8. Quais os aspectos que mais aprecia no BPC NET?

Selecione apenas 1 funcionalidade
☐ Interface/Aspecto ☐ Segurança ☐ Lista de operações
☐ Aplicações móveis ☐ Robustez ☐ Outro: _____

9. Que operações gostava de ver adicionadas ao BPC NET?

Selecione apenas 1 funcionalidade

☐ Transferências interbancárias ☐ Simulador de crédito
☐ Transferências internacionais ☐ Pedido de cartões de debito/crédito
☐ Contacto direto com gestor de conta

10. Está satisfeito com a nova plataforma de *internet banking*-BPC NET?

☐ Sim ☐ Não