MESTRADO EM
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO

TRABALHO DE PROJETO

GESTÃO DE IDENTIDADES CORPORATIVAS NUMA EMPRESA DE TELECOMUNICAÇÕES

BRUNO MANUEL ROSAS MARQUES

ORIENTAÇÃO:

PROFª ENGª ANA MARIA MARQUES RIBEIRO DOS SANTOS LUCAS

09 - 2012

Agradecimentos

À Guida, pelo apoio, paciência e compreensão durante todo este tempo.

Ao Pedro Tenreiro, que me encorajou a voltar aos estudos e foi um fantástico colega.

Aos restantes amigos e colegas de turma e de trabalho que me apoiaram.

Aos meus pais e irmã.

E finalmente, um agradecimento especial à professora Engª Ana Lucas, pelo incentivo que me deu para continuar estudos para além da Pós-Graduação, pela confiança depositada, pela sua preciosa ajuda e pelos conselhos e orientações durante este ano – fez-me sentir que de facto valeu a pena.

Resumo

A Gestão de Identidades Corporativas (identificada na literatura como *Identity and Access Management* ou pelas siglas IAM, I&AM ou ainda IdM) é, para muitas empresas, um tema difícil de endereçar devido à complexidade dos seus múltiplos sistemas de informação. Muitas vezes colocam-se questões relativas às funções de negócio que cada colaborador executa na organização, acerca de quais os acessos e permissões a sistemas de que realmente necessita para o seu trabalho e quais as permissões que atualmente possui. Dar uma resposta precisa a estas questões num determinado instante do tempo é muitas vezes impossível, devido à mobilidade entre empresas, à rotatividade dos colaboradores e à própria evolução temporal dos sistemas.

Este trabalho apresenta o desenvolvimento de um projeto de IAM numa grande empresa de Telecomunicações, designado por GIU – Gestão Integrada de Utilizadores, no qual o autor desempenhou o papel de investigador utilizando a metodologia de *Action Research*. O objetivo da investigação consistiu em, para além de colaborar na implementação do projeto, refletir sobre os aspetos positivos e negativos das decisões tomadas e produzir um conjunto de fatores críticos de sucesso e boas práticas para a implementação de projetos deste tipo. Além disto, procura-se ainda indicar caminhos futuros para a melhoria da plataforma, em interligação com a área de Qualidade de Dados, que permitam que o GIU seja uma fonte de verdade ainda mais credível no que diz respeito à informação de utilizadores e perfis que reside em cada um dos seus sistemas-alvo.

Palavras-chave: *Action Research*, Gestão de Identidades Corporativas, Provisão de Acessos, Segurança

Abstract

Corporate Identity Management (identified in the literature as Identity and Access Management or the acronyms IAM, I&AM or IdM) is, for a fair amount of companies, a hard issue to address due to the complexity and diversity of their information systems. Questions often arise about which business roles are performed by the organization's employees, what permissions they truly require in order to perform their jobs, and what permissions are currently assigned to them. A precise answer to these questions is often impossible to obtain for several reasons, such as, employee turnover, software integration issues and the rapid evolution of corporate systems.

This work presents the development of an IAM project named GIU. The project is currently taking place in a large telecommunications company, in which the author played the researcher role using the Action Research methodology. During a direct collaboration in the implementation process, several observations on the positive and negative aspects of project decisions were made, in an effort to provide a set of critical success factors and best practices for the implementation of future projects of the same kind. Moreover, future additions to the platform are recommended, such as connecting it with Data Quality tools, an improvement that would allow GIU to be an even more reliable source of truth concerning the permissions currently provisioned in each of the enterprise systems.

Keywords: *Action Research*, Identity and Access Management, Access Provisioning, Security

Índice

1 Introdução 8

1.1 Estrutura do relatório 8

2 Revisão de literatura 9

3 Metodologia de Investigação 16

3.1 Action Research 16

4 O projeto GIU – Gestão Integrada de Utilizadores 20

4.1 Motivação e objetivos (*Business drivers*) 20

4.2 Visão geral do GIU 22

4.3 Ciclos de *Action Research* do projeto GIU 24

4.3.1 1º Ciclo 24

4.3.2 2º Ciclo 29

4.3.3 3º Ciclo 33

5 Conclusões 37

5.1 Recomendações de boas práticas 37

5.2 Fatores críticos de sucesso identificados 39

5.3 Considerações finais 41

6 Limitações do estudo 41

7 Trabalho futuro 42

Anexo I - Processo de negócio - provisão 49

Anexo II – Requisitos de aplicações SOX 50

Anexo III – Gestão de funções de negócio 52

Lista de Figuras

Figura 1 – RBAC, versão mais completa (UML), adaptado de Ferraiolo *et al*.(2001) e Ray *et al.* (2004) 9

Figura 2 – Ciclo de *Action Research* (Adaptado de Susman & Evered, 1978)..... 17

Figura 3 - Visão geral do GIU 22

Figura 4 – Provisão de aplicações *Call Center* e FFM..... 24

Figura 5 – Gestão de Funções de Negócio – Dados genéricos da função 52

Figura 6 – Escolha da direção empresarial da função de negócio..... 52

Figura 7 – Escolha das aplicações para a função de negócio 53

Figura 8 – Escolha de perfis para a aplicação CTI (determinam posições CRM pré-selecionadas)..... 53

Figura 9 – Escolha de Posições Siebel (CRM) – algumas só para quem tiver acesso à aplicação CTI..... 54

Figura 10 – Outras características da função de negócio por aplicação (algumas podem ficar por definir)..... 55

Lista de Abreviaturas

ACD – Automatic Call Distributor

AD – Microsoft Active Directory

CCF – Customer Care Framework

CRM – Customer Relationship Management

CTI – Computer Telephony Integration

EAI – Enterprise Application Integration

eSSO – Enterprise Single Sign-On

FFM – Field Force Management

GEL – Gestão Eletrónica de *Logins*

GIU – Gestão Integrada de Utilizadores

IAM – Identity and Access Management

MDM – Master Data Management

NSOM – Novo Sistema de Order Management

OIM – Oracle Identity Manager

RBAC – Role Based Access Control

Siebel – Sistema CRM da Oracle

SoD – Segregation of Duty

SOX – Sarbannes-Oxley Act

1 Introdução

A gestão das autenticações e permissões de utilizadores nos sistemas corporativos não é obviamente um problema novo, remontando aos primórdios da disciplina de Sistemas de Informação. No entanto, a complexidade deste problema é atualmente muito elevada, devido às exigências de negócio e ao grande número de sistemas existentes em muitas empresas de grande dimensão.

Este trabalho de projeto foca-se nesta problemática, usando a metodologia A*ction Research* no âmbito de um projeto de Gestão de Identidades Corporativas, designado por GIU e desenvolvido para uma empresa de Telecomunicações, com o objetivo de identificar os principais problemas associados à sua implementação, bem como um conjunto de boas práticas e fatores críticos de sucesso que poderão ser úteis em futuros projetos desta natureza.

1.1 Estrutura do relatório

Este trabalho de projeto visa ajudar uma empresa de telecomunicações a agilizar e automatizar os seus processos de Gestão de Identidades e torná-los conformes com novas exigências de segurança e auditoria. Além deste objetivo, durante o seu acompanhamento é também efetuado o levantamento de um conjunto de fatores críticos de sucesso e de boas práticas a seguir.

Este documento encontra-se organizado em sete partes. Após um capítulo introdutório, é apresentada a revisão de literatura sobre os conceitos associados à Gestão de Identidades. Neste capítulo são também apresentadas as problemáticas com as quais as empresas se deparam neste tipo de projetos. Seguidamente, apresenta-se a metodologia *Action Research* e o GIU, através de um panorama geral do projeto, os principais *drivers* que estiveram na base da sua criação, e os ciclos de *Action Research* que tiveram lugar durante o seu acompanhamento, que decorreu de julho de 2011 a agosto de 2012.

Por último, apresentam-se as conclusões e as limitações do estudo, assim como algumas indicações para possível trabalho futuro.

2 Revisão de literatura

O tema do controlo de acessos baseado em papéis, adiante designado por RBAC (*Role Based Access Control*), foi abordado inicialmente por Ferraiolo & Kuhn (1992). A proposta original foi alvo de sucessivas extensões, melhorias e procura de um modelo padrão por parte de Ferraiolo *et al.* (1995) e Sandhu *et al.* (2000), nomeadamente a inclusão de hierarquias de perfis e a possibilidade de definição de restrições à sua atribuição. Esta versão mais complexa cujos conceitos são a seguir ilustrados em UML é hoje um *standard*, inicialmente proposto como tal por Ferraiolo *et al.* (2001).

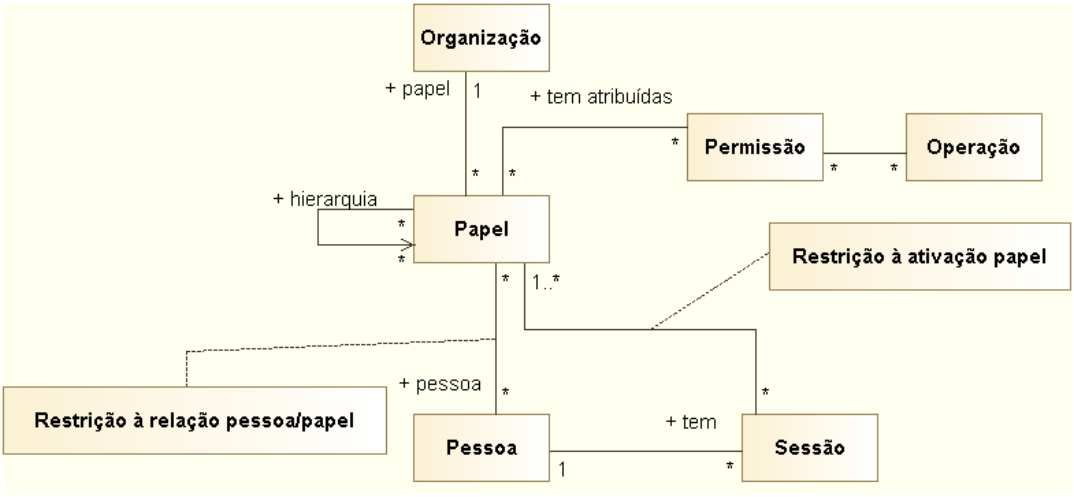


Figura 1 – RBAC, versão mais completa (UML), adaptado de Ferraiolo *et al.*(2001) e Ray *et al.* (2004)

De um ponto de vista conceptual, o modelo RBAC prevê a existência das seguintes entidades:

- Pessoa – o elemento que assume um dado papel numa organização – tipicamente representa um funcionário dessa organização;

- Papel – conjunto de permissões de acesso a operações necessário para exercer determinada função numa organização. É um conceito hierárquico (Sandhu *et al.*, 2000, p. 3) e totalmente abstrato pois não faz referência a nenhum sistema de informação em particular, sendo estas duas das grandes vantagens deste método de controlo de acessos face a outros possíveis, como o *Discretionary Access*

Control (Toelen, 2008, p. 16), que consiste numa gestão de *access control lists*, ou uma atribuição direta de permissões, método também conhecido por *Mandatory Access Control* (Toelen, 2008);

- Relação entre pessoa e papel – Pode impor-se pelo modelo que determinada relação entre uma pessoa e um papel só é válida em determinados dias da semana, ou outro tipo de restrições, como o princípio de segregação de funções, proposto por Kuhn (1997), que implica que, por exemplo, um utilizador não pode ter permissão para solicitar a criação de *logins* e para autorizar essa mesma criação;

- Operação – aquilo que é possível efetuar em concreto num determinado sistema;

- Permissão – relação entre papéis e operações, que especifica que operações podem ser executadas por quem tem determinado papel na organização;

- Sessão – corresponde à instanciação do papel (ou papéis) de uma determinada pessoa, existindo num contexto temporal. Uma pessoa está associada a zero ou mais sessões em cada instante, e tanto a sessão como a pessoa ficam associadas aos papéis a elas atribuídos. Isto corresponde tipicamente ao *login* em um ou mais sistemas de forma explícita ou transparente (*single sign-on*);

- Relação entre sessão e papel – O modelo permite a imposição de que só seja possível criar sessões para alguns dos papéis se determinadas condições forem válidas. Diversas restrições podem ser impostas, e existem propostas de modelos para as representar, como o de Ray *et al*. (2004).

Como podemos inferir, trata-se de um modelo bastante flexível para a gestão de permissões, pois não é necessário existir um administrador central (os utilizadores associados a determinadas funções podem também ter permissões para atribuir permissões dentro de âmbitos pré-definidos) e a associação de papéis a utilizadores é feita de forma abstrata e totalmente independente dos sistemas. O modelo facilita ainda a administração dos sistemas, pois qualquer alteração é automaticamente propagada ao domínio que está a ser administrado e é possível definir papéis à custa de outros já existentes de forma hierárquica, graças a uma extensão à proposta original de Ferraiolo

& Kuhn, apresentada por Sandhu *et al.* (2000) e incorporada no diagrama UML apresentado.

A maioria das empresas de média e grande dimensão adotaram, há já alguns anos, diretórios corporativos, tais como o *Active Directory* (AD), sistemas de bases de dados ou outros, que podem ser usados para implementar o modelo RBAC por intermédio do conceito de grupos. No entanto, continua muitas vezes a não existir uma gestão unificada e centralizada de utilizadores, sessões e papéis com caráter transversal, existindo em vez disso diversas implementações de autorizações independentes e incompatíveis entre si, bem como diversos acessos independentes a cada um dos sistemas necessários ao negócio. Com efeito, vários fatores impediram que esse objetivo se concretizasse em todo o seu potencial:

- Disparidade tecnológica, com sistemas heterogéneos ou ultrapassados, e com custos de adaptação difíceis de justificar;
- Adoção de sistemas fechados que não permitem integração;
- Dificuldade em manter registo das necessidades de cada aplicação ao nível geral, porque são muitas e geridas por muitos departamentos distintos;
- Elevado custo e dificuldade técnica de implementação global de processos de *single sign-on* (um único login / password para acesso a todas as aplicações da empresa), que permita uma noção de sessão global e transparente, devido à já referida heterogeneidade tecnológica;
- Reestruturações / reorganizações / aquisições / alterações de *software*;
- Dificuldade na migração de dados de utilizadores para um sistema centralizado, muitas vezes devido a problemas de qualidade de dados nos sistemas existentes ou a diferentes representações desses dados. Segundo Lucas (2010), o impacto da falta de qualidade de dados na economia foi estimado por Eckerson (2002) em cerca de 600.000 milhões de dólares por ano só nos Estados Unidos. Ainda de acordo com Eckerson (2002, p. 10), a perda de credibilidade dos sistemas e as dificuldades de reconciliação de informação surgem como as duas maiores

consequências de uma fraca qualidade de dados. Sendo estes dois aspetos tão importantes num sistema de IAM, que necessita de migrar e reconciliar dados de múltiplas proveniências, bem como atuar como uma fonte de verdade na empresa, é natural esperar que este problema possa ter impacto elevado (IBM, 2007, p. 9). Xie *et al.* (2010, p. 3) e Dejager *et al.* (2010, p. 3) apresentam-nos quadros ilustrativos das muitas dimensões que caracterizam a qualidade dos dados, sendo aqui cruciais para efeitos de reconciliação a consistência, fiabilidade e integridade dos dados pré-existentes nos sistemas-alvo, existindo também considerações análogas para os dados de referência.

Em conclusão, o que se observa na prática é que a mera existência de diretórios centralizados como, por exemplo, a *Microsoft Active Directory* (AD) e a gestão de perfis ao nível de cada aplicação não resolvem completamente o problema da provisão de papéis organizacionais que envolvam, em simultâneo, diversos sistemas tecnologicamente díspares. Torna-se assim necessário definir papéis agregadores de permissões em sistemas heterogéneos, que exigem a criação de um complexo sistema de provisão, capaz de implementar os conceitos abstratos do modelo RBAC de um modo transversal e extravasar as fronteiras de cada sistema ou conjunto limitado de sistemas. Este conceito é designado na empresa em análise por função de negócio, e pode ser definido como:

- Uma agregação de um ou mais papéis, relacionando cada um dos respetivos perfis (relação 1:N) com um sistema e a operação que é necessário efetuar nesse sistema para efetuar a sua provisão;

- Uma lista de parâmetros adicionais, pré-definidos ou deixados ao critério do utilizador no ato da provisão, como proposto por Kuhn *et al.* (2010) e Hitachi ID Systems, Inc. (2012, p. 5).

A definição destas funções de negócio é já em si um desafio – por exemplo, Jaferian *et al.* (2009) usaram ferramentas de *mining* dos acessos criados nos vários sistemas de uma organização de modo a procurarem utilizadores com acessos similares, inferindo assim os papéis a criar em IAM. Para além disto, sem IAM, é muito difícil ter-se a certeza de que as permissões dos utilizadores são de facto as necessárias (e apenas essas), bem

como gerir o seu ciclo de vida (Toelen, 2008, p. 24), exceto em casos triviais, bem como criar a ilusão de uma sessão coerente entre sistemas heterogéneos.

Além das questões já referidas, a gestão corrente dos acessos, com a implementação do conceito de função de negócio, acarreta outras dificuldades que devem ser mitigadas:

- Os já referidos problemas com a qualidade de dados nos sistemas existentes;
- Um grande aumento dos custos de exploração devido às múltiplas combinações possíveis de função de negócio / sistema / funcionalidade (muitas vezes são milhares…), e à sua frequente mutação (Jaferian *et al*., 2009; Hitachi ID Systems, Inc., 2012, p. 4);
- Um aumento da possibilidade de múltiplos erros, decorrente do ponto anterior;
- Acumulação de privilégios e acessos – quando um elemento muda de projeto ou de funções, por vezes pode não existir a preocupação de lhe retirar todos os acessos que deixaram de ser necessários, pois sem IAM não é possível manter um mapa centralizado das funções de negócio dos colaboradores na empresa, papéis do modelo RBAC que lhes correspondem e as permissões de acesso em cada sistema a eles associadas. Jaferian *et al*. (2009) ilustram o caos que pode ser gerado ao longo dos anos por estas situações, inaceitáveis quando existem auditorias (Hitachi Systems, Inc., 2012, p. 12);
- Acessos poderem continuar a existir mesmo após a saída de um colaborador da empresa, com os óbvios problemas de segurança que isso acarreta; particularmente preocupante no caso de funções que lidam com sistemas que contém informação de negócio de nível operacional ou estratégico, e que por isso é de acesso reservado;
- Possibilidade de existirem equipas externas (parceiros, fornecedores) com acessos ou permissões indevidas;
- A criação e integração constante de novos sistemas e funcionalidades, que obrigam a atualizar os perfis existentes nas aplicações.

- O dinamismo do negócio, que obriga à manutenção, criação e extinção frequente das funções de negócio, com periodicidade quinzenal, ou mesmo semanal.

Numa primeira abordagem à criação de uma solução de IAM, poder-se-á começar por criar o mapeamento entre funções de negócio, papéis e permissões necessárias para os desempenhar – tarefa certamente possível, mas de elevada complexidade. Mesmo dedicando-se uma equipa inteira a mantê-la atualizada, como garantir que a imagem existente nos sistemas reflete esta matriz em permanente mutação, com novas funcionalidades, novos negócios, novos sistemas, e obsolescência de outros?

Os fatores já referidos acima dificultam esta tarefa, tornando-a um desafio permanente, que obriga à interação frequente entre múltiplas equipas de negócio, responsáveis por comunicar as novas necessidades, e equipas de desenvolvimento e operações que efetuam a atualização das matrizes de funções de negócio no sistema de IAM sempre que necessário. Além disto, no caso de se tratar de alterações de funções de negócio já existentes, é necessário ainda alterar de forma retroativa as permissões dos utilizadores atuais, para que estas passem a refletir a nova realidade. Sendo assim, o sistema de IAM terá de disponibilizar processos expeditos para a execução desses mecanismos sempre que estas alterações ocorram.

Uma vez exposto este problema de gestão com o qual muitas organizações se deparam, é de esperar que empresas com alguma dimensão a nível de sistemas de informação que tentem atacá-lo na sua globalidade se deparem com um grande desafio, que pode obrigar por vezes a reformulações desses mesmos sistemas, envolvendo ao mesmo tempo vários quadrantes da organização. Numa empresa de média ou grande dimensão tipicamente existem dezenas ou mesmo centenas de sistemas, pelo que se impõe uma abordagem gradual ao problema, por intermédio da implementação de IAM aplicado primeiramente a um conjunto limitado de sistemas-alvo, progressivamente estendida e adaptada a outros de forma gradual.

No grupo empresarial em análise, assiste-se atualmente à consolidação de diversas empresas, numa ótica de procura de maior eficiência – nesse contexto, houve lugar a uma uniformização de sistemas que antes pertenciam apenas a uma empresa ou estavam replicados por várias empresas. Citam-se como exemplos a criação de uma AD única e

um projeto de unificação dos sistemas de *Customer Relationship Management* (CRM), que teve precisamente por objetivo criar uma visão única dos dados dos clientes da empresa.

Neste contexto de uniformização e consolidação, a iniciativa de IAM está a assumir grande relevância ao nível da organização, em virtude das suas implicações não apenas ao nível da segurança dos sistemas de informação, mas também ao nível da cada vez maior exigência de controlo de acessos aos sistemas, impostas pelo *Sarbannes-Oxley Act* na sua secção 404 (Kaur, 2011, p.3-5). Esta norma, além das políticas rigorosas de gestão e controlo de acessos, obriga ainda as empresas a sujeitar o processo de provisão a auditorias periódicas. Existem no mercado ferramentas de apoio à criação de sistemas de IAM, assim como estudos comparativos recentes das mesmas, como o de Kumar & Rodrigues (2010). Tipicamente estas ferramentas permitem controlar todo o processo de provisão e registar todos os passos efetuados. Ao tornar a provisão obrigatória a partir do sistema de IAM (proibindo-se expressamente a criação de utilizadores e atribuição de permissões diretamente nos sistemas alvo), consegue-se ter um sistema auditável e processos de gestão de utilizadores definidos e geridos a partir de um único ponto na empresa.

Além do acima exposto, ao ser eleito um conjunto restrito de interlocutores na organização para efetuar as tarefas de provisão de acessos, impondo-se um *worlflow* de autorizações com interlocutores distintos (respeitando a segregação de funções), consegue-se ainda reduzir a probabilidade de fraude (Koelewijn, 2009, p. 23).

A implantação de IAM nas empresas apresenta, muitas vezes devido ao elevado número de sistemas, complexidade e investimento inicial associado elevados. Com efeito, trata-se de um custo agregado à operação dos sistemas que existirá daqui para a frente – cada sistema introduzido ou alterado na empresa pode implicar alterações no sistema de IAM – mas, por outro lado, automatizará processos até aqui manuais. Não é, assim, possível ter garantias de redução de custos (Koelewijn, 2009, p. 23; Toelen, 2008, p. 49; IBM, 2007, p. 9).

3 Metodologia de Investigação

Sendo este um trabalho efetuado no contexto real de um projeto, com o objetivo de resolução de um problema organizacional concreto, com fortes sinergias entre a teoria e a prática (Avison *et al.*, 1999, p. 94), a metodologia selecionada foi a *Action Research*.

3.1 Action Research

A metodologia *Action Research* foi apresentada pela primeira vez por Lewin (1946). Trata-se de um processo interativo de resolução de problemas organizacionais levado a cabo por investigadores que aperfeiçoam progressivamente a sua capacidade de resolução por meio de um ciclo iterativo de planeamento, ação, reflexão e aprendizagem.

De acordo com Baburoglu & Ravn (1992), citados por Baskerville (2004), o objetivo da metodologia é estudar as mudanças que ocorrem numa organização, ao mesmo tempo que se participa e contribui ativamente para essas mesmas mudanças. A importância da colaboração entre todos os participantes no processo e o investigador é sublinhada em Peters & Robinson (1984), citados por Baskerville (1999, p. 9). Sobre o papel do investigador em *Action Research*, podemos encontrar uma descrição bastante clara e sucinta em Clark (1972, p. 65): *"For convenience it is useful to think of the practitioner as part of a set of actors who are oriented to solution of practical problems, who are essentially organizational scientists rather than academic scientists."*

Segundo Mårtensson & Lee (2004, p. 509), tradicionalmente os investigadores procuram sempre colocar rigor extremo nos seus estudos, mas esta situação leva a que se perca por vezes aplicabilidade do estudo. Ainda de acordo com os mesmos autores, muitas vezes investigação que poderia ser considerada relevante por pessoas fora do meio académico acaba por ser rejeitada por falta de rigor científico, por não ser validável ou replicável.

A metodologia de *Action Research* procura assim encontrar um compromisso entre o rigor e a relevância, indo de encontro aos apelos de Keen (1991) e Robey & Marcus (1998). Estes últimos, citados por Mårtensson & Lee (2004, p. 509), referem que «é possível e desejável cumprir as exigências de rigor e relevância simultaneamente,

produzindo investigação académica rigorosa e ao mesmo tempo considerada útil e relevante por parte dos praticantes no exercício das suas atividades de Gestão».

Deste modo, procura-se melhorar as práticas, estratégias e conhecimento, de forma a melhorar a capacidade de resolução de problemas práticos de forma iterativa.

O modelo de *Action Research* usado foi proposto por Susman & Evered (1978), e é composto por cinco fases:

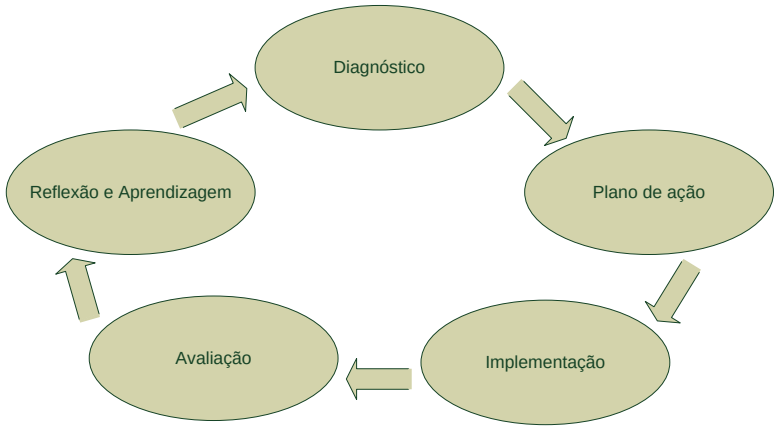


Figura 2 – Ciclo de *Action Research* (Adaptado de Susman & Evered, 1978)

De acordo com Baskerville & Wood-Harper (1996, p. 238), a fase de diagnóstico consiste na identificação e interpretação do problema organizacional que está na base da necessidade de mudanças na empresa. São aqui formuladas hipóteses de trabalho que suportarão as fases seguintes.

Segue-se uma fase de planeamento, que envolve o investigador e os restantes participantes no processo, que identifica um alvo de mudança e um conjunto de ações a tomar para chegar a um determinado estado de evolução. Várias abordagens podem aqui ser consideradas, mas só uma deverá emergir desta fase (Susman, 1983).

A fase de implementação corresponde a colocar em prática as ações planeadas. Nesta metodologia, o investigador é forçosamente parte integrante do processo, não sendo apenas um observador – nem sempre terá total poder de decisão, mas estará sempre diretamente envolvido na mudança. São aqui recolhidos os dados necessários à investigação, por intermédio de métodos como entrevistas, observações e consulta de

documentação (Lau, 1999). Espera-se que o investigador seja capaz de ter esta atitude participante e ao mesmo tempo crítica face à realidade envolvente – Lee & Dennis (2012) e Markus (1994), citados por Davison *et al.* (2012, p. 770), sublinham a importância de um envolvimento profundo do investigador no ambiente de trabalho, através da análise de conteúdo de *e-mails, chats*, e, naturalmente, conversando sempre que possível com os elementos da equipa e clientes, para que seja possível uma recolha de informação completa e fidedigna.

A informação recolhida na fase de implementação deve em seguida ser alvo de avaliação e reflexão crítica para uma interpretação e compreensão do sucesso ou insucesso das ações tomadas. A importância desta última fase é assinalada por Baskerville & Wood-Harper (1996). É importante que as lições aprendidas nesta fase sejam bem assimiladas, para que possam ser usadas no ciclo seguinte.

Geralmente um estudo de *Action Research* incorpora vários ciclos como os acima descritos. Lindgren & Henfridsson (2004, p. 444) apresentam um exemplo de como pode ser apresentada uma investigação deste tipo de forma sintética.

No que diz respeito às abordagens filosóficas, existem diferentes perspetivas nas quais se pode basear um estudo, sendo as mais correntes o positivismo e o interpretativismo.

O positivismo tem correspondência com a abordagem científica tradicional, que procura uma realidade objetiva, partindo de pressupostos iniciais, tais como o estabelecimento de determinadas variáveis dependentes e independentes, e aplicando métodos totalmente independentes do meio envolvente, tais como equações ou testes estatísticos, para procurar estudar a relação entre estas variáveis (Lee, 1999) e confirmar ou infirmar hipóteses de partida. Existe assim total isenção e independência do investigador e replicabilidade do estudo, não havendo lugar para interpretação subjetiva dos factos observados (Caldeira, 2000).

Em contraste com o positivismo, num estudo de tipo interpretativista procura-se aumentar conhecimentos sobre uma determinada área de estudo, tendo em conta o contexto social e cultural envolvente, dinâmico por natureza (Klein & Myers, 1999, p. 73). Dada a constante mutação destes contextos, não é de esperar a replicabilidade de

um estudo positivista, dado que as organizações não são estáticas e as relações entre pessoas, organizações e tecnologias estão em constante mutação (Klein & Myers, 1999, p. 73). Além disto, numa abordagem interpretativista não é exigida total isenção ao investigador, pois este procura interpretar uma determinada realidade da qual muitas vezes é parte integrante, e essas observações podem ser influenciadas pelos seus interesses, crenças e valores (Orlikowski & Baroudi, 1991).

Este trabalho usa a abordagem interpretativista, pois o investigador é um membro da equipa do projeto em estudo, sendo assim o registo de observações, bem como as conclusões obtidas influenciadas pela sua perceção pessoal (Machado, 2004, p. 24). Dada a proximidade entre investigador e restante equipa, tendem a ficar simplificados os passos de recolha da informação, pois reduzem-se eventuais resistências a essa recolha, especialmente no que diz respeito à génese e historial do projeto.

A abordagem interpretativista aqui seguida parece ser particularmente adequada à metodologia *Action Research*. Com efeito, Lee (1999, p. 33) faz um apelo à comunidade de investigadores para a aceitação e reconhecimento de estudos relevantes para a prática que não usem a abordagem positivista mais tradicional, e o positivismo é mesmo visto por alguns autores como uma antítese dos princípios do método de *Action Research* (Susman & Evered, 1978; Winter, 1989).

Além disto, segue-se uma abordagem qualitativa, dado que, como refere Machado (2004, p. 26), os dados obtidos num contexto de projeto, como o relatado neste trabalho, tipicamente não possuem características que possam suportar uma análise quantitativa precisa.

Importa ainda, neste contexto, referir algumas das limitações do processo de *Action Research*. De acordo com Klein & Myers (1999, p. 69), pode ser usada uma abordagem positivista (Clark, 1972), crítica (Carr & Kemmis, 1986) ou interpretativista (Elden & Chisholm, 1993), sendo que o uso desta última, segundo Baskerville (1999), dificulta o processo usual de publicação em revistas da especialidade por não existir um consenso quanto ao processo de revisão. Isto deve-se ao facto de a investigação em *Action Research* obedecer ao princípio filosófico de que a realidade é subjetiva e é influenciada por fatores sociais, culturais e históricos. Checkland *et al.* (1998, p. 16) referem também

que um estudo de *Action Research* não é geralmente replicável, pois variáveis como o local, o tempo e o próprio investigador têm influência nas conclusões.

Outras limitações referidas por Baskerville (1999) resultam do facto de a investigação ter lugar num ambiente de projeto, no qual podem surgir conflitos éticos entre a atividade de consultoria, paga por um cliente que tem determinado objetivo de negócio, cujas orientações podem mudar no decorrer do processo, e a investigação a levar a cabo, que se pretende focada numa temática de interesse do investigador. Caso estes dois aspetos divirjam, poderá ter de existir uma elevada capacidade de adaptação por parte dos participantes.

4 O projeto GIU – Gestão Integrada de Utilizadores

4.1 Motivação e objetivos (*Business drivers*)

Um estudo da Forrester Research de 2011, citado por Al-Khouri (2011, p. 464), mostra que os projetos de IAM têm sido priorizados como críticos pelas empresas nas suas estratégias de segurança corporativa. Este estudo identificou em múltiplas empresas os *drivers* genericamente considerados como mais importantes, tais como a introdução de melhorias operacionais significativas nos processos de negócio associados à provisão de utilizadores, assim como a resolução do problema da rastreabilidade dos sistemas de provisão (que se impõe dada a entrada do controlo SOX). Este último ponto foi identificado como um dos principais *drivers* em estudos como o da KPMG (2009), que cita ainda como outros *drivers* de topo, por ordem decrescente de importância, a agilidade na gestão do negócio, a redução de custos operacionais e as melhorias operacionais. Koelewijn (2009, p.8) identifica também a segurança, conformidade com SOX e outras diretivas, melhoria da qualidade de serviço e redução de custos.

A empresa em que se realizou este projeto foi criada na sequência da fusão entre empresas do mesmo grupo, e atravessa uma fase de consolidação dos seus sistemas de informação, que representa um desafio de larga escala e de médio-longo prazo. Neste âmbito, foi criado um mapa estratégico das plataformas-chave de suporte aos Sistemas de Informação da empresa, que entre outras aplicações, envolve um novo sistema de *Order Management* (NSOM) destinado a substituir o atual (de elevadíssima

complexidade e criticidade, mas assente em tecnologia obsoleta), um sistema unificado de *Customer Relationship Management* (CRM) – Siebel Único, uma ferramenta de *Enterprise Application Integration* (EAI corporativo) – TIBCO, uma nova plataforma única de *Computer Telephony Integration* (CTI) – *CTI One*, entre diversos outros.

Paralelamente, é necessário, para dezenas de outras aplicações legadas, criar um sistema de provisão que obedeça a normas mais estritas, pois estas estão suportadas por um sistema de provisão antiquado (Gestão Eletrónica de *Logins*, ou GEL) que não é adaptável às atuais exigências e tem de ser descontinuado.

Além disto, a recentemente criada Política de Segurança de Sistemas de Informação da empresa proíbe a existência de *interfaces* de provisão direta (sem passar por IAM) para um conjunto de aplicações-chave (especialmente as que estão sujeitas a controlos SOX), sendo que para as restantes está também já decidida a sua migração para o GIU.

Obviamente, tudo isto obrigará a uma alteração profunda nos processos de gestão, dado que estas alterações são transversais e por isso revestem-se de elevada criticidade, sendo o GIU uma peça fundamental nesta visão para os Sistemas de Informação da empresa nos próximos anos.

O investimento nesta plataforma é portanto altamente estratégico, pois, de acordo com a sua equipa de gestão, os objetivos são bem claros – impor o cumprimento das normas resumidas no Anexo II - Requisitos de aplicações SOX (objetivo que a empresa está obrigada a cumprir), conseguindo ao mesmo tempo poupanças significativas com a automatização, e uma elevada qualidade e rapidez de resposta a pedidos de provisão.

4.2 Visão geral do GIU

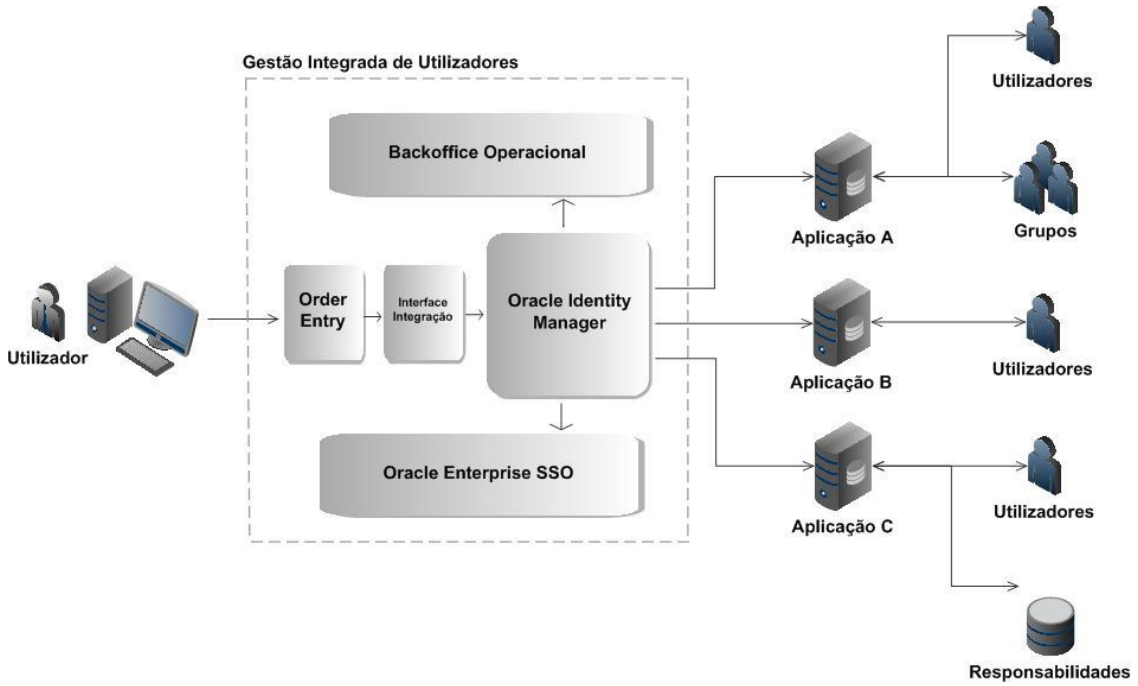


Figura 3 - Visão geral do GIU

Em termos gerais, o GIU disponibiliza os seguintes serviços de segurança:

- Provisão de Acessos – o GIU assegura a provisão de contas de utilizador e respetivos acessos nas aplicações de negócio tendo como principais funcionalidades:
    - Ponto único de contacto para a solicitação de acessos aplicacionais;
    - Recolha e gestão de pedidos de acesso (*order-entry*), implementando regras de negócio na recolha de informação necessária à provisão de acessos;
    - Aprovação de pedidos de acesso, automatizando o *workflow* de aprovação e possibilitando vários níveis de aprovação;
    - Automatização do processo de provisão, através de *interfaces* com as aplicações;
    - *Single Sign-on.*

As funcionalidades anteriores são suportadas pelas seguintes componentes:

- O*rder Entry*, cuja responsabilidade é o processamento de pedidos e suporte aos fluxos e *workflows* de aprovação dos acessos dos utilizadores;

- *Oracle Identity Manager* (OIM), que após aprovação de um pedido em *Order Entry* inicia o aprovisionamento dos utilizadores junto das aplicações, gerindo também o seu ciclo de vida. Esta componente é também usualmente designada por GIU-OIM;

- *Oracle Enterprise Single Sign-on*, que opcionalmente gere a criação automática de sessões entre certas aplicações. O objetivo a médio prazo é criar um projeto paralelo de unificação das autenticações perante o maior número de aplicações possível, evitando a utilização de múltiplos tipos de acesso para um conjunto de aplicações de negócio. O seu grau de sucesso depende do tipo de aplicações que estão implementadas na empresa, pois é esta componente que tem de ter flexibilidade para se adaptar ao que existe com as limitações inerentes – raramente é efetuado o processo inverso, por questões de custos ou mesmo impossibilidade técnica (pacotes de *software* fechados); no entanto, produtos deste tipo permitem um bom grau de abrangência, por intermédio de esquemas de captura de páginas *web* de *login* ou de ecrãs das aplicações, com submissão da informação de autenticação às várias aplicações, criando assim de forma razoavelmente satisfatória a noção de sessão unificada prevista pelo modelo RBAC;

- *Backoffice* operacional – toda a gestão corrente da plataforma e da criação de utilizadores é efetuada a partir de ferramentas de *backoffice*. O OIM traz de base um extenso conjunto de funcionalidades (*web site* de gestão de provisão), e disponibiliza *interfaces* de programação para os implementadores, para que seja possível a criação de funcionalidades adicionais. Com base nestas *interfaces* é possível estender o OIM e suportar necessidades operacionais específicas, relacionadas com operações de provisão, revogação ou atualização em massa, carregamento de dados e execução de retroatividades, entre outros.

4.3 Ciclos de *Action Research* do projeto GIU

Descrevem-se em seguida os ciclos de *Action Research* que correspondem às principais fases de acompanhamento do projeto.

4.3.1 1º Ciclo

Os primeiros sistemas integrados no GIU foram os que dizem respeito às equipas de *Call Centers* e equipas no terreno (*Field Force Management* – FFM). Esta priorização fez sentido, na medida em que o elevado número de pessoas abrangidas por estes sistemas e a sua elevada rotatividade representavam uma fatia bastante significativa dos custos de provisão com processos tradicionais e não automáticos (através de *tickets* ou *e-mail*). Foi neste âmbito inicial que se idealizou o conceito de função de negócio, central ao seu funcionamento e já explanado anteriormente, e foi com estes sistemas que o projeto teve o seu arranque. No entanto, dada a urgência nesse arranque, efetuado num contexto de passagem de conhecimento por parte de uma equipa externa anterior, com os constrangimentos técnicos, políticos e temporais inerentes, não foi possível implementar desde logo uma gestão eficaz da provisão de funções de negócio, sendo esta, nesta fase, ainda efetuada de forma *ad-hoc*, sistema a sistema.

Eis uma panorâmica da versão inicial do GIU:

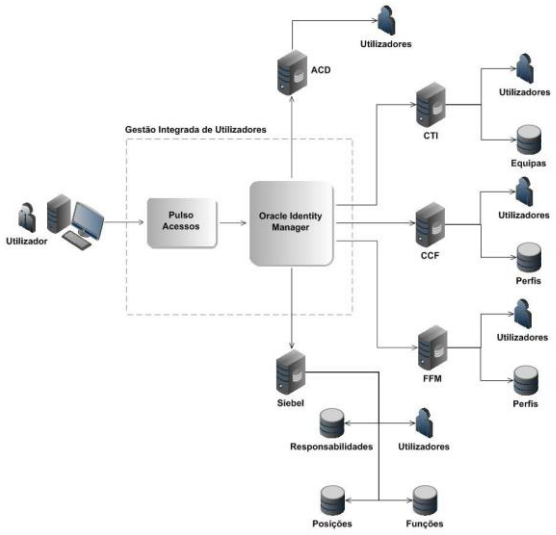


Figura 4 – Provisão de aplicações *Call Center* e FFM

4.3.1.1 Diagnóstico inicial

A participação neste ciclo deu-se sobretudo ao nível da recolha de informação sobre o projeto, em reuniões com a equipa anterior e com o cliente, existindo a expetativa de que a nova equipa GIU-OIM passasse a dominar a plataforma num espaço de tempo relativamente curto.

Existindo já um conjunto importante de aplicações suportadas nesta primeira versão (especialmente o CRM), esta tarefa revelou-se morosa, existindo necessidade de várias semanas de levantamento do sistema existente, problemáticas e limitações existentes em detalhe, procurando-se compreender as abordagens que foram seguidas numa ótica de melhoria futura.

Foi neste ciclo identificado um conjunto de necessidades de ações a tomar, algumas para o imediato e com caráter urgente, outras para futuro. Dado que era essencial gerir o tempo de permanência da equipa anterior, pertencente a outra empresa de serviços, e procurar extrair o máximo de informação possível, neste ciclo houve apenas concentração na documentação e correção a pedido de problemas identificados no *software*, não havendo lugar a quaisquer evoluções do mesmo em termos funcionais. Além disto, por meio de entrevistas e reuniões com o cliente e a equipa cessante, foi possível obter informações acerca de um conjunto de problemáticas com as quais o projeto se debateu até aí e que iriam muito provavelmente continuar a manifestar-se ao longo do projeto.

4.3.1.1.1 Problemáticas da implementação

4.3.1.1.1.1 Organizacionais

A migração para o GIU é, por experiência no terreno, um processo delicado e por vezes moroso. Com efeito existem desafios organizacionais com os quais nos debatemos para procurar colocar um projeto como este em marcha sempre que surge a necessidade de uma nova fase de integração, tais como:

- Pressão para implementar IAM num curto espaço de tempo;

- Saber quem dá suporte a determinadas aplicações desenvolvidas há vários anos, visto que o conhecimento sobre as mesmas é muitas vezes incompleto;

- Tentar ter uma visão global das aplicações e suas interdependências muitas vezes não óbvias – constata-se, por exemplo, que uma determinada função de negócio necessita de quase todas as aplicações para poder efetuar o seu trabalho, pelo que não é possível migrar a provisão para o GIU de algumas, deixando outras por migrar, e se torna necessária uma migração de várias aplicações em simultâneo, com os riscos inerentes;

- A informação sobre funções de negócio e processos de provisão anteriores ao GIU nem sempre se encontra estruturada, pelo que se torna necessário efetuar o seu levantamento;

- Dificuldade em tirar um *snapshot* da informação que se encontra nos sistemas atuais para a migrar para o GIU – esta informação não está centralizada e está em constante mutação, não sendo viável parar a provisão para efetuar esta recolha;

- Dificuldades na geração de relatórios exigidos pelo SOX – esta norma exige a realização de auditorias periódicas com informação dos acessos criados ou revogados para cada colaborador da empresa, incluindo as datas destas operações de provisão e informações que não estão todas centralizadas no sistema IAM. Por esse motivo existe a necessidade de consulta de diversas fontes de dados dispersas. Para mais informação ver Anexo II – Requisitos de aplicações SOX.

4.3.1.1.1.2 Técnicas

Historicamente, existiram já no passado, em empresas do grupo, iniciativas que procuraram centralizar a criação de utilizadores, desenvolvidas ao longo dos anos, mas que hoje se encontram em processo de descontinuação, em virtude de terem sido desenvolvidas em tecnologias que se tornaram obsoletas, de não existir suporte nem documentação adequados para as mesmas, e de não serem adaptáveis à plataforma escolhida para suportar IAM no novo mapa estratégico de aplicações corporativas.

4.3.1.1.1.3 Políticas de Segurança

A Política de Segurança da empresa é um extenso documento publicado em 2010, que tem como objetivo implementar e divulgar um enorme conjunto de critérios e preocupações a ter em matéria de segurança. Em alguns capítulos são especificados requisitos aos quais todos os sistemas terão de passar a obedecer, especialmente no que diz respeito à gestão de *passwords* e outros aspetos definidos no Anexo II – Requisitos de aplicações SOX. Além do que é estritamente exigido pelo SOX, opta-se ainda por:

- Evitar usar *passwords* sequenciais;
- Proibir a transmissão das mesmas por qualquer meio eletrónico (por exemplo *e-mail*), a não ser em casos muito particulares;
- Obrigar à alteração no primeiro *login.*

No que diz respeito ao suporte por parte da plataforma GIU, é pré-requisito uma aplicação adaptar-se às normas, se ainda não o fez.

Na implementação do GIU há a preocupação constante em garantir que são salvaguardadas estas medidas; no entanto, algumas questões de teor organizacional e não técnico, têm também de ser garantidas pela política de segurança, e extravasam o âmbito de qualquer solução IAM, tais como controlar acessos a edifícios, penalizar usos fraudulentos de cartões de acesso ou partilha de *passwords*, e outros aspetos que os próprios sistemas não têm possibilidade de endereçar. A elevada rotatividade de equipas e sistemas obriga a um apertado controlo destas situações, para evitar, por exemplo, situações de partilha ou divulgação indevida de *passwords*.

4.3.1.2 Plano de ação

Dados os constrangimentos existentes, houve lugar ao seguinte plano de ação:

- Melhorar a documentação do sistema e processos existentes;
- Desenvolver processos de *backoffice* para automatizar tarefas que não estavam devidamente operacionalizadas nem entregues a equipas de suporte, consumindo excessivo tempo à equipa GIU-OIM (próxima fase);

- Estabilizar alguns componentes do *software* existente, que, devido aos prazos de implementação da fase inicial, ainda apresentava falhas por tratar;

- Compreender e melhorar *interface* entre *Order Entry* e OIM, abandonando a então existente, desenvolvida sob pressão e com graves problemas relacionados com a sua manutenção (gradualmente).

4.3.1.3 Implementação

Não sendo ainda possível desenvolver novas funcionalidades, tiveram lugar as seguintes atividades:

- Ciclo intensivo de reuniões com equipa anterior durante a sua fase de saída, de modo a documentar os módulos e o seu funcionamento;

- Identificação de documentação a fornecer por parte da equipa cessante;

- Elaboração da documentação de levantamento e acompanhamento da equipa cessante para garantir a passagem do conhecimento;

- Apoio e acompanhamento na correção de problemas do *software* de modo a ganhar familiarização com o mesmo.

4.3.1.4 Avaliação

De acordo com uma entrevista aos elementos da equipa envolvidos neste ciclo, verificou-se que, apesar de terem existido resistências à passagem de conhecimento para uma outra empresa por parte da equipa anterior, o processo foi avaliado pela equipa como um sucesso, graças à preocupação com o detalhe na documentação, e às reuniões exaustivas que procuraram extrair o máximo de informação possível no tempo disponível. A opção de acompanhamento diário permitiu uma familiarização progressiva com o sistema e com as questões a ter em conta na sua expansão futura.

4.3.1.5 Reflexão e aprendizagem

Neste ciclo, houve a tomada de consciência, por parte da nova equipa, da complexidade do GIU, assim como dos problemas organizacionais inerentes. Muitos dos aspetos referidos na literatura, como as constantes mutações dos dados de referência do sistema

(Hitachi ID Systems, Inc., 2012, p. 4) e a dificuldade de acompanhamento devido à ainda pobre automatização dos processos (Jaferian *et al*., 2009) fizeram-se sentir desde o início da entrada do projeto em ambiente produtivo, com a consequente dificuldade em garantir novos desenvolvimentos e dar suporte aos existentes. A qualidade dos dados de referência que migravam para GIU, nem sempre perfeitamente congruentes com os existentes nos sistemas-alvo, foi outro problema também esperado, originando erros de provisão e causando pressão na equipa, devido ao facto de ser necessário analisá-los caso a caso, com o correspondente consumo de tempo. Houve, pois, desde logo, a necessidade de começar a desenvolver ferramentas para automatizar diversos processos até aqui manuais, à medida que a equipa se familiarizava com o OIM.

4.3.2 2º Ciclo

Neste ciclo houve lugar à melhoria e estabilização do *software* legado pela equipa anterior, assim como ao desenvolvimento de módulos que permitissem a operacionalização eficiente da plataforma.

4.3.2.1 Diagnóstico

Existindo necessidades constantes de criação e revogação de acessos em grande quantidade e com elevada frequência, era urgente neste ciclo a criação de processos que automatizassem estas tarefas. Era também urgente concretizar melhorias em vários componentes de *software*, já identificados no 1º ciclo, bem como a melhoria dos processos de *backoffice* para apoio às operações.

4.3.2.2 Plano de ação

1) Automatização de processos de provisão em massa

Criação de um utilitário para permitir criações, atualizações e revogações massivas de utilizadores.

Era necessário, por exemplo, criar os seguintes mecanismos:

- Provisão, atualização, reconciliação e revogação de acessos em massa, para cada sistema-alvo;

- Criação de processos automáticos de atualização de dados de referência sem intervenção humana;

- Gestão de dados de referência e configuração da plataforma sem intervenção da equipa de desenvolvimento;

- Processamento em massa de retroatividades através da deteção automática de alterações entre versões dos dados de referência.

2) Gestão de funções de negócio – versão inicial

O desenvolvimento deste módulo tinha por objetivo que as funções de negócio existentes ficassem parametrizadas em GIU-OIM, sendo uma das componentes da informação de referência. Cada função de negócio determina:

- O conjunto de aplicações às quais o utilizador tem acesso quando essa função lhe está atribuída;

- Para cada aplicação, quais as permissões de acesso e módulos que são visíveis (especialmente importante para o sistema CRM, que tem milhares de opções deste tipo); aqui, sempre que possível, e especialmente para o CRM Siebel, são criados perfis neste sistema-alvo que abrangem outros de forma hierárquica, para se evitar ter de efetuar a provisão de centenas de perfis por utilizador em certas funções de negócio;

A matriz das funções de negócio pode ser pensada, numa primeira abordagem, como uma lista do tipo (função negócio, sistema-alvo, perfil no sistema-alvo). No entanto, como já foi referido, isto apresenta um potencial problema de explosão do número de funções de negócio, que tornaria o problema intratável – segundo Kuhn *et al.* (2010, p.80), sendo N o número de perfis distintos, o número de funções de negócio que pode ser criado é de 2^N. Existem duas formas de mitigar este problema, bem conhecido pelos criadores do modelo RBAC, sendo em Kuhn *et al.* (2010) proposta uma solução usada no GIU – em vez de deixar a função completamente definida, deixar apenas uma parte dos perfis fixa, ficando a escolha dos restantes, bem como a escolha de determinadas configurações específicas de alguns sistemas, ao critério do requisitante no ato da

provisão. Deste modo, é possível reduzir consideravelmente o número de entradas na matriz, pois não é necessário especificar todas as combinações possíveis para os perfis de escolha livre. Outra proposta do modelo RBAC, também aqui utilizada, consiste na criação de hierarquias de papéis, não sendo necessário especificar que uma função de negócio necessita dos papéis A, B e C se o papel C já herdar as características de A e B (Sandhu *et al.*, 2000).

Tendo em conta estas premissas, é possível tornar a gestão da referida matriz um problema tratável, criando-se apenas algumas centenas de funções de negócio, ao invés de muitos milhares.

3) Gestão de informação de referência

Neste ciclo do projeto havia a necessidade de criar processos automáticos de gestão de informação de referência, que até aqui era atualizada de forma manual.

Pretendia-se criar processos de gestão em duas vertentes:

- Importação periódica de dados para o GIU a partir de fontes diversas (cada sistema-alvo disponibiliza os seus dados de referência de formas distintas, não existindo muitas vezes um ponto único de contacto para este fim, ou uma gestão de dados mestre centralizada que permita a consulta dos mesmos num único ponto);

- Importação manual a partir de ferramentas de *backoffice*, quando não é possível a importação automática.

4) Implementação de nova *interface* de comunicação entre *Order Entry* e OIM

Tendo em vista simplificar a comunicação entre os dois módulos principais do GIU e torná-la mais independente da tecnologia de cada um deles, foi criada uma *interface* de comunicação consistindo num *Web service* genérico para envio de formulários e receção dos resultados das operações, bem como todo o tipo de consultas ao sistema IAM e à sua informação de referência. Esta *interface* de comunicação é responsável por:

- Aprovisionar, atualizar ou revogar acessos *ad-hoc* em sistemas-alvo, validando a coerência dos dados submetidos;

- Associar, alterar ou revogar funções de negócio, garantindo a propagação para os diversos sistemas, pela ordem de precedência correta, da informação de provisão a adicionar ou a remover em cada caso;

- Dar acesso de consulta à informação de referência.

4.3.2.3 Implementação

Foram efetuadas todas as ações planeadas neste ciclo.

4.3.2.4 Avaliação

De acordo com entrevista efetuada a um elemento da equipa de suporte técnico, este tipo de abordagem simplificou de forma drástica o trabalho diário desta equipa no que diz respeito ao apoio às operações. Ao mesmo tempo, observou-se ainda uma redução significativa do tempo diário dedicado a este tipo de tarefas por parte da equipa de desenvolvimento GIU-OIM, com os evidentes ganhos em termos de foco e produtividade.

A sensibilização da equipa de *Order Entry* para a necessidade de readaptação do sistema de provisão para utilizar a nova *interface* começou também aqui a dar frutos, pois, apesar de continuar ainda a ser necessária a coexistência da *interface* legada com a nova, existiram num curto espaço de tempo diversas adaptações que, com algumas poucas exceções, permitiram uma migração sem sobressaltos.

Ao nível da gestão de funções de negócio, verifica-se que, ao contrário do que ocorria antes do GIU, esta informação está estruturada e suportada desde a raiz, como um agregador de acessos a um conjunto de sistemas. Além disto, ao eleger-se uma única equipa na empresa para ficar com a responsabilidade de administrar a matriz, esta passou a ser vista como *focal point* para estas questões, minimizando-se incoerências ou conflitos na gestão desta informação.

Subsistiram no entanto problemas com a qualidade dos dados provenientes dos sistemas integrados no GIU – nem sempre é possível uma sincronização perfeita dos mesmos, e

nem sempre estes respeitam as restrições de integridade. Muitos destes problemas fogem ao controlo direto da equipa, mas o sucesso do GIU como agregador e integrador de informação depende da qualidade desses dados, o que obriga muitas vezes a múltiplas interações com equipas dos sistemas-alvo para despistes e correções de informação de referência.

4.3.2.5 Reflexão e aprendizagem

Neste ciclo, foram mais uma vez notórias as dificuldades existentes com a qualidade de dados, especialmente ao nível da gestão da informação de referência, o que mostra a importância que teria a pré-validação destes dados com auxílio de ferramentas especializadas, prevenindo-se assim os problemas em vez de os corrigir. Quando isto ocorre, é esperado elevado impacto na credibilidade do IAM (IBM, 2007), pelo que é fundamental otimizar estes procedimentos.

Apesar do problema acima, a automatização de processos de importação de dados e adição de validações permitiu em parte colmatar algumas destas dificuldades, reduzindo a possibilidade de erro humano.

A abstração tecnológica da separação das componentes *Order Entry* e OIM por um *Web service* revelou-se uma aposta acertada, simplificando e desacoplando estas componentes do sistema, tal como preconizado na literatura (Li & Karp, 2007, p. 9), e simplificando as interações entre as equipas.

Ao nível das funções de negócio, a abordagem seguida permitiu reduzi-las a cerca de 200, um número considerado aceitável – no entanto, este tenderá a aumentar com a adição de mais sistemas à noção de função de negócio, pois para já apenas estão abrangidos os 4 sistemas associados aos *Call Centers*.

4.3.3 3º Ciclo

Este ciclo consistiu na preparação do GIU para receber as aplicações legadas suportadas pelo sistema de provisão GEL (Gestão Eletrónica de *Logins*) – sendo uma das grandes motivações iniciais do projeto GIU, o GEL2GIU é assim um projeto estratégico, uma vez que visa fazer a empresa abandonar uma plataforma de provisão considerada obsoleta. Apesar de existir elevado interesse na implantação do GEL2GIU num curto

espaço de tempo, constatou-se ao longo do tempo que se tratava de uma tarefa de elevada complexidade, cujo diagnóstico de ações a tomar não foi trivial.

4.3.3.1 Diagnóstico

O sistema GEL é responsável pela provisão num conjunto de aplicações legadas, que são apenas uma parte deste novo universo abrangido pelo GIU. Apesar das suas limitações ao nível de gestão de *workflows* – na sua maioria artesanais, por intermédio de *trouble tickets*, *e-mail* ou outro tipo de processos que não garantem uma adequada integração e uma fácil rastreabilidade, o GEL continua ainda hoje a dar suporte à criação de utilizadores num universo de cerca de 15 sistemas. Um dos projetos do GIU que tem vindo a ser desenvolvido pela equipa de trabalho tem sido precisamente esta migração, e designa-se por GEL2GIU.

Eis as principais dificuldades com as quais a equipa se deparou ao estudar o sistema GEL:

- Falta de documentação clara do sistema a nível técnico e processual, e inexistência de interlocutores formalmente responsáveis pelo suporte da aplicação, com disponibilidade para ajudar a equipa no levantamento de informação;

- Problemas de qualidade dos dados existentes no GEL (incongruências), potencialmente conduzindo a uma difícil migração, e a uma possível integração de erros no novo sistema, perpetuando-os; só uma validação caso a caso iria permitir minimizar este problema.

4.3.3.2 Plano de ação

Foram identificadas as seguintes ações, neste ciclo:

1) Identificar sistemas geridos pelo GEL e processo de provisão;

2) Procurar replicar o GEL de forma faseada, começando pelos sistemas mais utilizados.

4.3.3.3 Implementação

Começou-se por solicitar informação sobre as aplicações geridas pelo GEL, a sua criticidade, e o seu peso relativo em termos operacionais, no que diz respeito à provisão – com esse objetivo, foi pedida uma lista dos pedidos de provisão efetuados ao GEL no espaço de um ano. Optou-se por uma abordagem faseada, pois verificou-se que de entre cerca de 15 sistemas, um conjunto de apenas 3 – *Active Directory*, *Xamix* e *IX* absorviam mais de 70% dos pedidos.

Posteriormente, foi necessário obter informação de referência necessária à provisão em cada um destes sistemas, especialmente para o sistema *IX*, que representa por si um vasto conjunto de aplicações suportadas em bases de dados *Informix* e servidores *Unix*. O GEL utiliza mapeamentos para a provisão em cada uma destas aplicações, para cada tipo de perfil de utilizador (em certo sentido um conceito semelhante ao de função de negócio já aqui abordado, mas limitado aos sistemas suportados pelo GEL e a aplicações *Informix*). De acordo com elemento da equipa GIU-OIM, foi necessário criar de raiz um motor de provisão no GIU para replicar este comportamento do GEL, tendo sido esta uma das componentes mais complexas e desafiantes do projeto.

Durante o desenvolvimento desta componente houve ainda um constrangimento adicional relacionado com a saída de alguns elementos da equipa, com a consequente passagem de informação, respeitante à especificação funcional criada na fase de análise e a uma parte bastante significativa da solução até aí desenvolvida.

4.3.3.4 Avaliação

Numa primeira tentativa de colocação da aplicação em produção, constatou-se que a análise efetuada era demasiado simplista – com efeito, verificou-se que apesar de a provisão nestes sistemas ter sido migrada com sucesso, surgiam queixas de equipas que não conseguiam efetuar a provisão de certas aplicações em GEL, fundamentais para o negócio. Na verdade, nenhum destes problemas foi levantado na fase de análise pelos interlocutores, pois estas dependências eram conhecidas apenas por equipas técnicas que já não estavam no projeto GEL e não estavam documentadas.

Além disto, o impacto da qualidade de dados existente no GEL não foi totalmente estimado à partida como tendo um potencial efeito tão nefasto no projeto. Cita-se apenas a título exemplificativo alguns dos muitos problemas encontrados:

- Informação de referência por vezes incorreta face à existente nos sistemas-alvo;
- Utilizadores inexistentes ou inválidos mas cadastrados;
- Utilizadores com determinados campos de informação inválidos;
- Incongruências entre sistemas com *soft links* (existe informação no sistema A que devia refletir informação existente no sistema B mas tal não está a ocorrer);
- Utilizadores duplicados;
- Utilizadores que deviam existir nos sistemas A e B mas só existiam num deles;
- Informação importada de um sistema A que apresenta informação referente a um sistema-alvo B em estado incoerente com o que se encontra nesse sistema-alvo.

Foi assim necessário cancelar a provisão feita em GEL2GIU, e voltar ao sistema GEL até se encontrar um novo plano de ação.

É importante ainda referir o impacto significativo da substituição de alguns elementos da equipa GIU-OIM no desenvolvimento do GEL2GIU – tendo a mesma tido lugar já numa fase adiantada do desenvolvimento, a passagem de conhecimento implica sempre um esforço adicional na equipa de projeto e pode originar lacunas no domínio da solução.

4.3.3.5 Reflexão e aprendizagem

Após este ciclo, a equipa ficou com uma melhor noção do funcionamento do GEL, bem como do facto de que existia muita informação de negócio que não ficou esclarecida na fase de análise, pois não se encontrava documentada e não existia por parte dos interlocutores contactados no processo uma visão global dos processos de provisão relacionados com as aplicações afetadas. Esta visão surgiu apenas quando outras equipas verificaram que não estavam a ter acessos em sistemas que ainda estavam a ser

aprovisionados por GEL, pois a provisão destes dependia em GEL de outros que entretanto tinham sido migrados para o GEL2GIU (*Active Directory*).

Na posse destes novos dados, foi possível criar novo plano de ação, consistindo na passagem destas aplicações dependentes para a componente *Order Entry* (descontinuando-se o GEL), e levantamento das interdependências existentes. Este processo ainda decorre, dado o elevado número de aplicações a integrar e a evolução paralela do GEL, mas evitou-se nesta fase a complexidade adicional da introdução da componente OIM.

Dada a antiguidade do GEL e as dificuldades da sua governação, foram aqui notórias, mais do que em qualquer dos outros ciclos, as limitações decorrentes da fraca qualidade de dados existente, pelo que a futura migração para OIM deverá começar pela depuração de dados na fonte, em conformidade com IBM (2007, p. 9).

5 Conclusões

Durante este trabalho, foi possível, durante os meses de evolução aqui documentados, acompanhar a criação das estruturas de base do GIU e um conjunto de módulos considerados estruturais, em virtude da sua abrangência em termos de empresas e pessoas envolvidas.

As lições aprendidas neste processo dizem sobretudo respeito à abordagem que deve ser seguida neste tipo de projeto: como deve ser implementado e operacionalizado, qual a abordagem a seguir em termos de migração para uma nova plataforma de provisão, e a importância que a manutenção de dados de elevada qualidade tem para este tipo de iniciativas, podendo mesmo considerar-se um fator fulcral – se isto não for acautelado antes de se avançar para a solução de IAM, deve aproveitar-se a sua implementação para introduzir esse tipo de controlo de qualidade na arquitetura da empresa.

5.1 Recomendações de boas práticas

A intervenção pronta e adequada das equipas técnicas perante problemas dos utilizadores é um fator fulcral para que exista confiança na plataforma. Neste contexto, a criação de utilitários para a automatização de tarefas por parte das equipas de

operações revelou-se uma boa prática a ter em conta, pois foi altamente benéfica, mesmo com o custo de alguns desenvolvimentos inicialmente não previstos. Recomenda-se, assim, reservar tempo no planeamento de um projeto deste tipo para implementar estas automatizações desde o início e para cada novo sistema a integrar.

Ao nível tecnológico, o OIM revelou ser uma ferramenta adequada aos objetivos, se bem que por vezes a sua curva de aprendizagem possa ser um entrave à entrada de novos elementos na equipa. Verifica-se ainda que a ferramenta não está totalmente explorada, pelo que poderá permitir construir futuramente processos e *worflows* mais robustos que os atuais, se for possível compreender melhor o seu funcionamento. Por estes motivos, em futuros projetos com esta ferramenta, é recomendável que seja ministrada formação aprofundada a dois ou mais elementos da equipa, antes do início do projeto.

Observou-se ainda que a aposta em tecnologias abertas como *Web services* para abstração dos sistemas-alvo das comunicações permitiu uma mais rápida operacionalização, e uma mais rápida integração de sistemas. Este benefício foi observado em projetos similares como o de Oliveira & Rehem (2010), e é referido por Li & Karp (2007, p. 9). A separação da componente de O*rder Entry* da componente de provisão teve também um impacto significativo, ao permitir que as equipas de desenvolvimento separadas se concentrassem mais nas suas respetivas componentes, escondendo assim a complexidade do OIM. Recomenda-se, assim, a utilização deste tipo de abordagem tanto na comunicação com os sistemas externos como entre os módulos do IAM, dadas as melhorias na modularização e desacoplamento do *software*.

Ao nível da qualidade de dados, verificou-se que a informação que a empresa possui sobre os acessos dos seus colaboradores aos seus próprios sistemas apresentava diversas falhas, especialmente no GEL. Efetivamente, surgiram dificuldades acrescidas na migração dos utilizadores dos atuais sistemas para o OIM – muitas vezes observou-se que a extração de dados dos sistemas atuais e sua reconciliação no OIM apresentava erros, tendo estes de ser validados e corrigidos caso a caso, contribuindo assim para situações de perda de confiança no projeto e aumentos significativos de custos, em conformidade com Eckerson (2002). É, pois, recomendável a utilização de ferramentas

de *Data Cleansing*, bem como a pré-validação dos dados inseridos por reconciliação na plataforma IAM para que a mesma seja credível.

5.2 Fatores críticos de sucesso identificados

A partir da experiência de contacto com o projeto, foram identificados os seguintes fatores críticos de sucesso para que iniciativas deste género tenham continuidade no longo prazo:

- Apoio da gestão e disponibilização dos recursos humanos e materiais necessários – importantíssima ajuda na identificação dos interlocutores para cada sistema e garantia da sua disponibilidade, bem como no levantamento de requisitos;
- Existência de recursos altamente qualificados para levar a cabo o projeto, com baixa rotatividade nas equipas – as situações vividas durante o *handover* inicial respeitante ao 1º ciclo (substituição integral da equipa do GIU, com as dificuldades na passagem de conhecimento e as alterações de processos de trabalho daí resultantes), bem como no âmbito do GEL2GIU, mostraram como este aspeto é importante;
- Investimento forte desde o início na automatização de processos – sem este investimento efetuado no 2º ciclo, não teria sido possível ter a equipa disponível para fazer evoluir a plataforma;
- Capacidade de comunicação interdepartamental e interempresarial para que seja possível efetuar o levantamento dos sistemas existentes, os seus formatos de mensagens e os fluxos de dados existentes – um projeto transversal como este requer uma equipa de gestão bastante ágil, dada a dimensão do grupo empresarial em estudo;
- Nomeação de núcleo de competência que fique responsável por fazer novos projetos aderir ao sistema IAM e promover as boas práticas no âmbito da sua exploração – para cada novo sistema a integrar, é necessário esclarecer os responsáveis dos sistemas-alvo sobre as regras em vigor – provisão obrigatória através do GIU e nunca diretamente nos sistemas-alvo, para serem evitadas

incongruências de dados, trabalho desnecessário de correção de erros ou mesmo não-conformidades em auditorias de segurança;

- Não querer fazer tudo de imediato («*big bang*») – na adesão de novos sistemas ao IAM, começar por um piloto de âmbito limitado, aprendendo com a experiência e ir estendendo progressivamente o IAM a um maior número de utilizadores e a um cada vez maior número de sistemas – com efeito, a versão inicial do GIU permitiu ao projeto ganhar aceitação, apesar de ser bastante mais limitada e de mais difícil utilização comparativamente à atual;
- Definição clara do modelo de governação da provisão de utilizadores à partida – antes da implementação deve ficar bem claro quem é responsável por gerir a plataforma, explorá-la e garantir o seu correto funcionamento numa base diária. Esta questão implica garantir a alocação de equipas de exploração dedicadas ao sistema, que prestem célere apoio a problemas técnicos, garantindo assim que a introdução da plataforma de IAM não causa impacto negativo no negócio – esta separação bem clara revelou-se crucial no caso do GIU, pois permitiu à equipa de desenvolvimento focar-se nas suas tarefas e intervir em questões de exploração apenas pontualmente para esclarecimentos ou problemas no *software*;
- Efetuar ações de sensibilização, clarificando as mais-valias de IAM aos responsáveis por cada sistema da empresa, e não assumindo que todos as conhecerão à partida – o IAM não é apenas mais um projeto de Tecnologias de Informação (TI) – é algo transversal à empresa, e todos têm a beneficiar com a sua implementação – se isto não ficar claro para todos à partida, poderão existir diversos tipos de resistências à integração de alguns sistemas na plataforma de IAM («porque é que não posso ser eu a controlar os meus utilizadores?», «para que serve esta burocracia?», «vão ter acesso aos dados do meu sistema?»); é pois importante clarificar os benefícios desta abordagem de gestão centralizada, e também a obrigatoriedade do uso de IAM, devido às cada vez mais rigorosas normas de auditoria e segurança em vigor.

5.3 Considerações finais

Podemos afirmar que o GIU, apesar de estar já com uma arquitetura sólida e a suportar alguns sistemas bastante importantes da empresa, tem ainda um longo caminho a percorrer.

Como já foi referido, o GIU faz parte do mapa de aplicações estratégicas para os próximos anos. Assim sendo, trata-se de uma iniciativa que não é vista como uma "moda do momento", e que terá forçosamente de ter continuidade até estar totalmente embebida na arquitetura da empresa. A conformidade com o SOX é também um impulsionador do sucesso do projeto, pois garante a continuidade do seu financiamento. Ainda assim, tem sempre de existir a consciência de que poderão não ser visíveis no imediato resultados financeiros diretos decorrentes desta atividade, apesar das poupanças induzidas pela automatização de processos.

Em conclusão, trata-se sem dúvida de um projeto desafiante, abrangente e com bastantes evoluções previstas para os próximos anos, que poderá vir a tornar-se na plataforma geral de provisão de utilizadores da empresa.

6 Limitações do estudo

Tratando-se de um estudo efetuado no contexto do desenvolvimento de um projeto, é natural que as conclusões sobre os fatores mais influenciadores do sucesso, os maiores problemas com os quais uma equipa se debate num projeto deste tipo, ou mesmo as recomendações que podemos dar a futuros implementadores, possam não ser as mesmas num projeto efetuado num contexto empresarial distinto, relativo à área de atuação, historial, dimensão da empresa, ou mesmo aos recursos humanos e materiais envolvidos, mesmo tratando-se de um projeto do mesmo teor. Aliás, esta é a principal limitação do método de *Action Research*. As conclusões apresentadas são, pois, fruto da experiência de projeto e da interpretação pessoal da informação recolhida e ocorrências observadas. Ainda assim, dada a complexidade do GIU, pensamos que será possível extrapolar para outros contextos, tendo em conta as experiências aqui relatadas, antes de se iniciar um projeto similar.

7 Trabalho futuro

Apesar de o GIU apresentar já alguma maturidade, durante o desenvolvimento dos vários módulos foram observados problemas recorrentes que podem ser endereçados. Efetivamente, em consequência do facto de terem existido problemas relacionados com qualidade de dados com os quais as equipas de desenvolvimento e de operações se debateram durante o projeto, somos levados a pensar que uma direção futura para a plataforma, para além das previsíveis expansões e integrações para provisão num maior número de sistemas, poderá passar pela interligação do GIU com uma plataforma de *Master Data Management* / *Data Quality*.

O módulo de *Master Data Management* (MDM), ao fornecer uma visão única dos dados de referência da empresa e possibilitar a sua gestão de forma mais eficiente e controlada, poderia teria um papel importante instalado a montante do GIU, atuando assim como filtro da informação de referência, e permitindo que esta seja validada e testada, com gestão de alterações e de versões, antes de chegar ao GIU. Acreditamos que a melhoria da qualidade dos dados de referência daí resultante iria refletir-se numa melhor qualidade do serviço prestado pela plataforma, com as consequentes poupanças e melhorias operacionais (redução de número de *tickets* e atrasos causados por informação de referência incorreta).

O módulo de *Data Quality* teria a sua maior utilidade quando aplicado ao *Data Cleansing* dos dados já existentes em sistemas da empresa, à medida que forem sendo migrados para o GIU. Estamos em crer que, com a ajuda deste tipo de ferramentas, conseguir-se-á que o GIU seja uma fonte de verdade sobre a provisão de utilizadores melhor do que todas as que existiam até à data da sua criação.

REFERÊNCIAS

Al-Khouri, Ali M. (2011). Optimizing Identity and Access Management Frameworks. *Journal of Engineering Research and Applications (IJERA). ISSN: 2248-9622 www.ijera.com. Vol. 1, Issue 3,* 461-477.

Avison, D.; Lau, F.; Myers, M.; Nielsen, P (1999). Action Research, *Communications of the ACM*, Vol. 42, No. 1, January 1999, 94-97

Baburoglu, O. N.; Ravn, I. (1992). Normative Action Research. *Organization Studies (13:1),* 19-34.

Baskerville, R.; Wood-Harper, A. (1996). A critical perspective on action research as a method for information systems research. *Journal of Information Technology, 11*, 235-246.

Baskerville, R. (2004). Special Issue on Action Research in Information Systems: making IS research relevant to practice – foreword. *MIS Quarterly Vol. 28 No. 3*, 329-335.

Baskerville, R. (1999). Investigating Information Systems with Action Research. *Communications of the Association for Information Systems, Vol. 2*, Article 19.

Caldeira, M. (2000). Critical Realism: A philosophical perspective for case study research in social sciences, *Episteme, Ano II*, 5-6, pp. 73-78.

Carr, W.; Kemmis, S. (1986). Becoming Critical: Education, Knowledge and Action Research, *Falmer Press*, London.

Checkland, P; Holwell, S. (1998). Action Research: Its Nature and Validity. Systemic Practice and Action Research, Vol. 11, No.1, 9-21.

Clark, P. (1972). Action Research and Organizational Change. *London: Harper & Row*.

Davison, R.M.; Martinsons, M.G.; Ou, Carol X.J. (2012). The roles of theory in canonical action research. *MIS Quarterly Vol. 36 No. 3*, 763-786.

Dejager, Karel; Hamers, Bart; Poelmans, Jonas; Baesens, Bart (2010). A Novel Approach to the Evaluation and Improvement of Data Quality in the Financial Sector. *Proceedings of the 15th International Conference on Information Quality (ICIQ2010), Little Rock, Arkansas*, 12-14 Nov. 2010.

Eckerson, W.W. (2002). Data Quality and the Bottom Line: Achieving Business Success Through a Commitment to High Quality Data. *The Data Warehousing Institute Report Series, No.101*, Chatsworth, USA.

Elden, M., Chisholm, R. F. (1993). Emerging Varieties of Action Research: Introduction to the Special Issue, *Human Relations* (46:2), pp. 121–142.

Ferraiolo, David F., Kuhn, D. Richard (1992). Role-Based Access Controls. *15th National Computer Security Conference (1992)*, Baltimore MD, USA, 554 – 563.

Ferraiolo, David F., Cugini, J., Kuhn, R. (1995). Role Based Access Control: Features and Motivations, *Proceedings, Annual Computer Security Applications Conference*, IEEE Computer Society Press, 1995.

Ferraiolo, David F, Sandhu R, Gavrila S, Kuhn, R., Chandramouli R. (2001). Proposed NIST Standard for Role-Based Access Control, 2001.

Forrester Report, Twelve Recommendations For Your 2011 Security Strategy. *Forrester Research* [em linha]. Disponível em http://www.forrester.com (Acedido em 22 de junho de 2012).

Hitachi ID Systems, Inc. (2012). Beyond Roles: A Practical Approach to Enterprise User Provisioning. [em linha]. Disponível em http://hitachi-id.com/identity-manager/docs/beyond-roles.pdf (Acedido em 25 de agosto de 2011).

IBM. (2007). Identity and access management: Uncovering the secrets to successful implementations. IBM Corporation. [em linha]. Disponível em ftp://public.dhe.ibm.com/common/ssi/ecm/en/sew03002usen/SEW03002USEN.PDF (Acedido em 25 de agosto de 2012).

Jaferian, P., D. Botta, *et al*. (2009). A case study of enterprise identity management system adoption in an insurance organization. *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology*, Baltimore, MD, USA — Nov. 07 - 08, 2009.

Kaur, Harmeet (2011). Identity and Access Management—Its Role in Sarbanes-Oxley Compliance. *JOnline*.

Keen, P. G. W. (1991). Relevance and Rigor in Information Systems Research: Improving Quality, Confidence, Cohesion and Impact. *Information Systems Research: Contemporary Approaches and Emergent Traditions*, H-E. Nissen, H. K. Klein, and R. Hirschheim (eds.), Elsevier Science Publishers (North-Holland), Amsterdam, 1991, 27-49.

Klein, H. K., Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretative Field Studies in Information Systems. *MIS Quarterly, 23, 1*, 67-93.

Koelewijn, G (2009). Identity & Access Management – Get in control: IT Governance, people, permission and technical challenges. *Master: Computer Science, Faculty Electrical Engineering, Mathematics and Computer Science, Delft University of Technology*.

KPMG (2009). KPMG's 2009 European Identity & Access Management Survey – Status and maturity of identity and access management projects in European organizations [em linha]. Disponível em http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/European-identityaccess-management-survey.pdf (Acedido em 22 de junho de 2012).

Krishnan, J., D. Rama, *et al*. (2007). Costs to comply with SOX Section 404. *Auditing: A Journal of Practice & Theory, Vol. 27, No. 1*, May 2008, 169-186.

Kuhn, D. Richard. (1997). Mutual Exclusion of Roles as Means of Implementing Separation of Duty in Role-Based Access Control Systems. *Second ACM Workshop on Role-Based Access Control.*

Kuhn, D. Richard, Coyne, E.J., Weil, T.R (2010). Adding Attributes to Role-Based Access Control, *IEEE Computer Magazine*, Vol. 43 Issue 6, June 2010, pp. 79-81.

Kumar, S.M., Rodrigues, P. (2010). A Roadmap for the Comparison of Identity Management Solutions Based on State-of-the-Art IdM Taxonomies. *Proceedings of CNSA'2010*, 349-358.

Lau, F. (1999). Toward a Framework for Action Research in Information Systems Studies. Information Technology & People, Vol. 12 Issue 2, pp.148 - 176

Lee, A. S. (1999). Rigor and Relevance in MIS Research: Beyond the Approach of Positivism Alone. *MIS Quarterly, 23; 1*, 29-34.

Lee, A. S., e Dennis, A. R. (2012). A Hermeneutic Interpretation of a Controlled Laboratory Experiment: A Case Study of Decision Making with a Group Support System, *Information Systems Journal (22:1)*, 3-27

Lewin, Kurt (1946). Action Research and Minority Problems. *Journal of Social Issues Volume 2, Issue 4*, 34–46.

Li, Jun; Karp, Alan H. (2007). Access control for the services oriented architecture. *Workshop On Secure Web Services*, 2007, Fairfax. New York: ACM, 2007. p. 9–17. ISBN: 978-1-59593-892-3.

Lucas, Ana (2010). Corporate Data Quality Management in context. *Proceedings of the 15th International Conference on Information Quality (ICIQ2010),* Little Rock, Arkansas, 12-14 Nov.2010.

Lindgren, Rikard; Henfridsson, Ola (2004). Design Principles for Competence Management Systems: A Synthesis of an Action Research Study. *MIS Quarterly Vol. 28 No. 3*, 435-472.

Machado, Ricardo J. (2004). Investigação em Metodologias de Desenvolvimento: o *Action Research.* SEDES04, Coimbra, 2004

Markus, M. L. (1994). Electronic Mail as the Medium of Managerial Choice, *Organization Science (5:4)*, pp. 502-537.

Mårtensson, P.; Lee, A. (2004). Dialogical Action Research at Omega Corporation. *MIS Quarterly Vol. 28 No. 3*, 507-536.

Object Management Group, *OMG/Business Process Management Initiative* [em linha]. Disponível em http://www.bpmn.org/ (Acedido em 1 de dezembro de 2011).

Oliveira, C.S; Rehem, S. (2010). RASEA – Uma Solução Unificada para Controle de Acesso Multiplataforma de Aplicações, *ConSerpro – Congresso de Tecnologia e Gestão Aplicadas a Serviços Públicos*, 24-26 Nov. 2010, Recife, Brasil.

Orlikowski, W. J., e Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions, *Information Systems Research*, 2, 1, pp. 1-28.

Peters, M.; Robinson, V. (1984). The Origins and Status of Action Research. *Journal of Applied Behavioral Science, (20) 2,* 113-124.

Ray, I.; Li, N.; France, R.; Kim, D. (2004). Using UML To Visualize Role-Based Access Control Constraints. *Proceedings, ACM Symposium on Access Control Models and Technologies - SACMAT'04*, June 2-4, 2004, Yorktown Heights, NY, USA.

Robey, D.; Markus, M. L. (1998). Beyond Rigor and Relevance: Producing Consumable Research about Information Systems. *Information Resources Management Journal (11:1)*, 1998, 7-15.

Sandhu R., Ferraiolo D., Kuhn R. (2000). The NIST Model for Role Based Access Control: Towards a Unified Standard. *Proceedings, 5th ACM Workshop on Role Based Access Control*, July 26-27, 2000, Berlin, 47-63.

Susman, G.; Evered, R. (1978). An assessment of the scientific merits of action research. *Administrative Science Quarterly, 23*, 582-603.

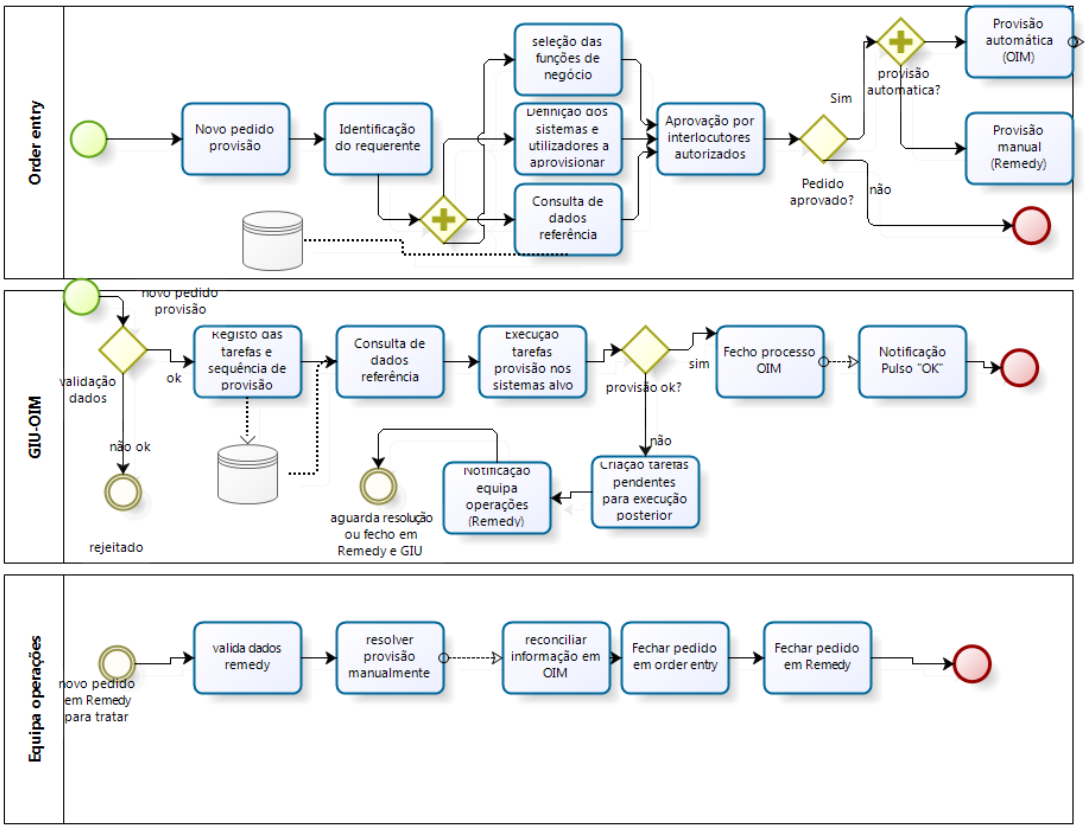
Susman, G. (1983). *Action Research: A Sociotechnical Systems Perspective*, ed. G. Morgan (London: Sage Publications) 102.

Toelen O. (2008). *Identity and Access Management*, Master Thesis in Information Security Technology, Technische Universiteit Eindhoven, Department of Mathematics and Computer Science.

Winter, Richard (1989). Learning From Experience: Principles and Practice in Action-Research. *Philadelphia: The Falmer Press*, 43-67.

Xie, Shuyan; Helfert, Marcus (2010). Assessing Information Quality deficiencies in emergency medical service performance. *Proceedings of the 15th International Conference on Information Quality (ICIQ2010)*, Little Rock, Arkansas, 12-14 Nov. 2010.

Anexo I - Processo de negócio - provisão



Anexo II – Requisitos de aplicações SOX

As exigências relativas às aplicações sujeitas à norma SOX estão resumidas na tabela que se segue. Há dezenas de aplicações abrangidas, que geralmente estão relacionadas com a consulta de dados que obrigam a elevado nível de confidencialidade. O requisito «R7» é particularmente difícil de implementar, pois a informação de horas de *login* tem lugar nos sistemas-alvo e a consolidação desta informação num único ponto obriga à consulta periódica a todos os sistemas-alvo.

Requisito	Descrição
«R1»	Eliminação de contas que nunca foram acedidas desde que foram criadas, ao fim de um dado número de dias.
«R2»	Expiração de palavra-chave – ao fim de um dado número de dias, o utilizador de uma conta tem que alterar a palavra-chave, exceto se houver uma exceção aprovada.
«R3»	Constituição da palavra-chave deve seguir a política de segurança.
«R4»	Bloqueio de contas por inatividade (falta de acesso) ao fim de um dado número de dias, exceto se houver uma exceção aprovada.
«R5»	Contas que tenham sido bloqueadas de acordo com «R4» e não tenha sido pedido o seu desbloqueio ao fim de um dado número de dias, deverão ser revogadas ou fisicamente eliminadas, desde que estejam asseguradas condições de rastreabilidade.
«R6»	Não devem existir utilizadores genéricos. As excepções devem estar de acordo com o disposto na Política de Segurança – excepção aprovada e identificação de um colaborador responsável.
«R7»	Deve ser produzido um relatório, com periodicidade mensal, no 1º dia de cada mês, contendo a seguinte informação: • **Username***– Login na aplicação; • **Name*** – Nome do utilizador (Nome Completo preferencial); • **N_Emp** – Se colaborador interno; • **Doc_Type** – Tipo de documento de identificação (BI, PA, AR, NC); • **Doc_Num** – Número de documento de identificação (preferencialmente validado e sem duplicados);

	• **Company_Orig** – Empresa de onde provém (se colaborador externo) ou onde tem contrato (se colaborador interno); • **Company_Dest** – Empresa onde trabalha; • **Dir_Dest** – Direção onde trabalha; • **Domain_AD** – Domínio na *Active Directory*; • **User_AD*** – Identificador de utilizador na *Active Directory*; • **Email** – Caixa de correio no servidor Exchange; • **Telef** – Telefone do local de trabalho; • **Mobile** – Telemóvel de serviço; • **Request_Id** – Nº de pedido no sistema de *ticketing*, no *Order Entry* ou no GEL; • **Create_Date*** – Data de criação do utilizador na aplicação; • **Last_Login*** – Data de último acesso à aplicação; • **Profile** – Perfil de acesso na aplicação; • **Status*** – Estado do utilizador na aplicação; • **Expiration_Date** – Data de expiração da palavra-chave na aplicação; Se a aplicação não conseguir devolver a informação solicitada, mesmo assim deverá incluir/respeitar todos os elementos, ainda que com valores em branco. Os campos identificados com um asterisco (*) são obrigatórios.

Anexo III – Gestão de funções de negócio

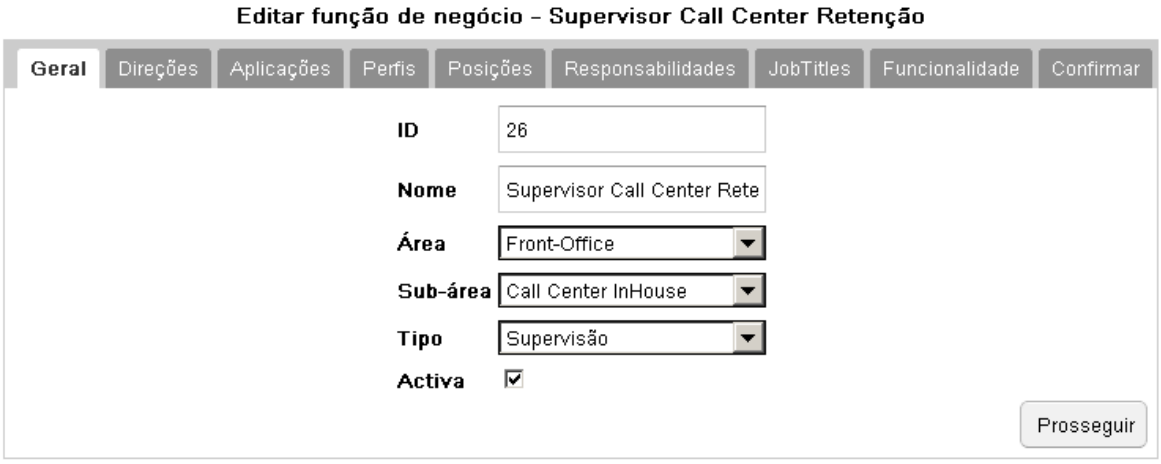


Figura 5 – Gestão de Funções de Negócio – Dados genéricos da função

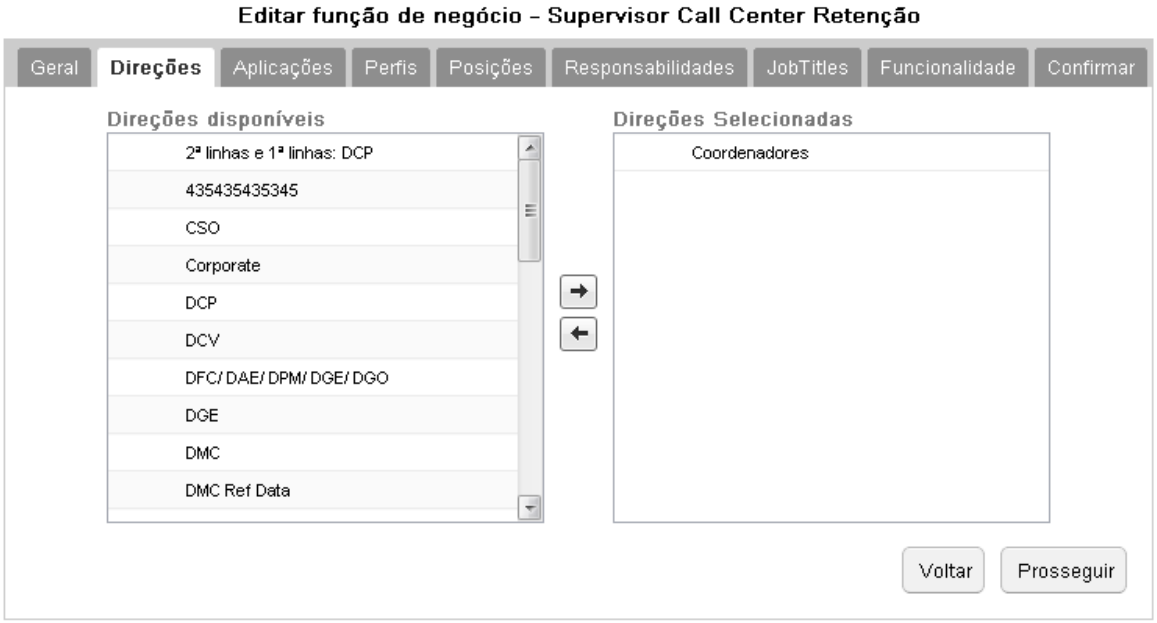


Figura 6 – Escolha da direção empresarial da função de negócio

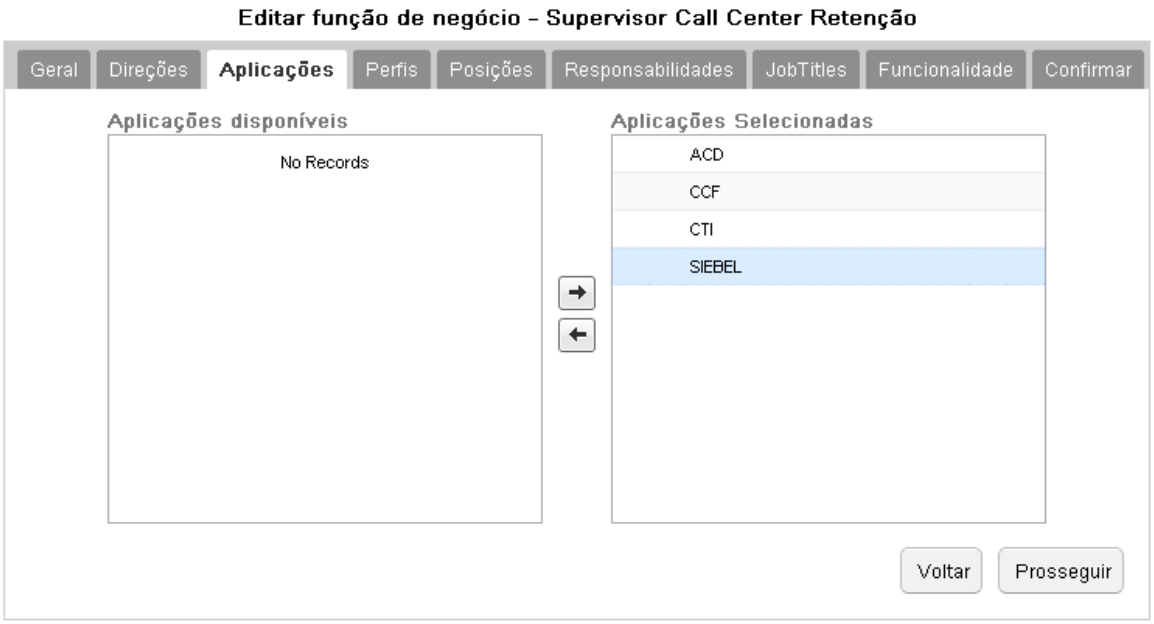


Figura 7 – Escolha das aplicações para a função de negócio

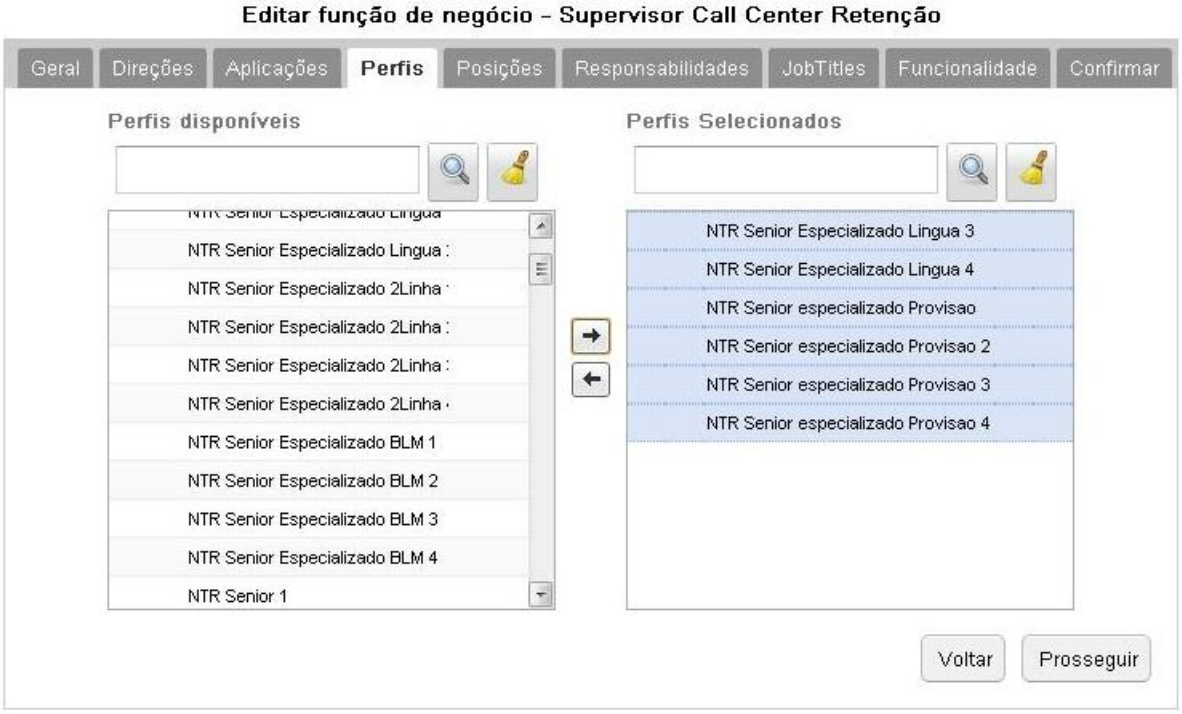


Figura 8 – Escolha de perfis para a aplicação CTI (determinam posições CRM pré-selecionadas)

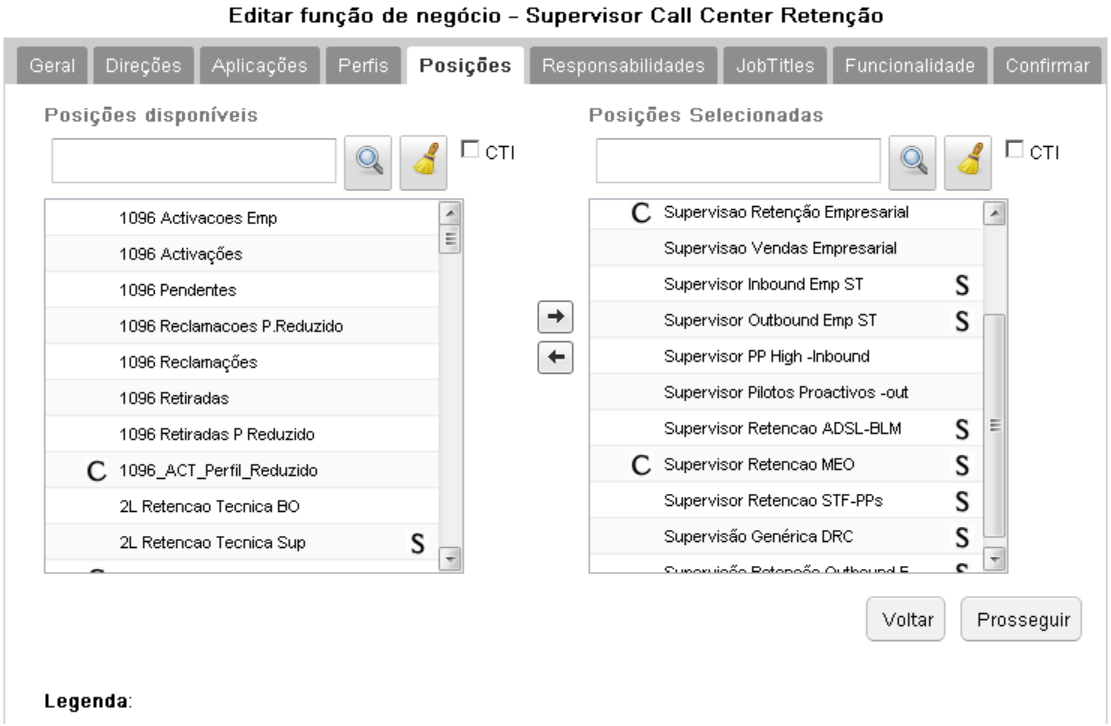


Figura 9 – Escolha de Posições Siebel (CRM) – algumas só para quem tiver acesso à aplicação CTI

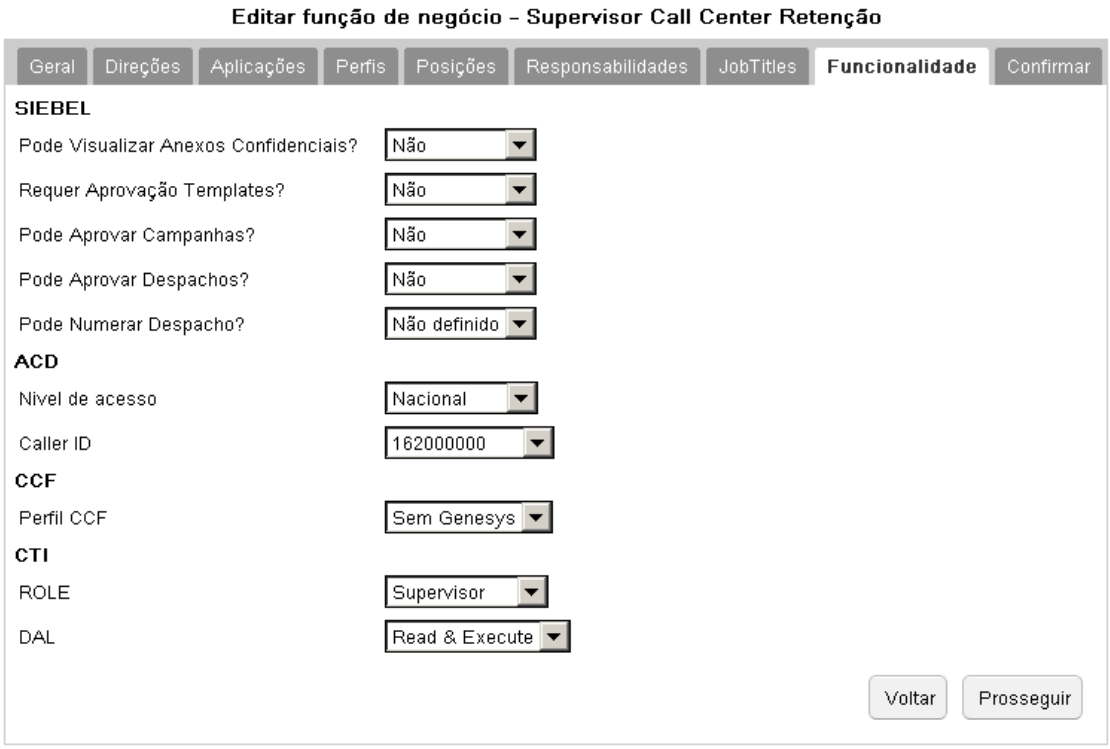


Figura 10 – Outras características da função de negócio por aplicação
(algumas podem ficar por definir)