INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Sistema de autenticação centralizada num grande retalhista

SANDRO MIGUEL GONÇALVES VARA
Outubro de 2017

POLITÉCNICO
DO PORTO

Instituto Superior de Engenharia do Porto

Sistema de autenticação centralizada num grande retalhista

Sandro Miguel Gonçalves Vara

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Sistemas Gráficos e Multimédia

Orientador: Doutor António Cardoso Costa

Porto, Outubro de 2017

Ao meu eterno Avô,

que sempre esteve presente.

"desistir nunca vai fazer parte de ti"

Resumo

Os grandes retalhistas estão constantemente focados no crescimento dos seus negócios e reconhecem a importância de inovar e definir a melhor solução tecnológica num mercado em constante evolução.

A ambição de implementar um sistema ideal tornou-se um desafio sem precedentes para os retalhistas, com o objetivo de melhorar os processos de negócio e compreender o comportamento dos consumidores. Neste sentido, o sistema de retalho (Oracle Retail) oferece vários domínios de produtos que proporcionam melhorias nos processos operacionais e permitem a tomada de decisão adequada, de acordo com as necessidades do mercado, ajudando a organização a obter uma infraestrutura operacional e analítica que a diferencia da concorrência.

Para além disso, durante a definição da solução de retalho torna-se necessário seguir boas práticas de segurança da informação para garantir a proteção aos ativos do retalhista, visto que a informação é considerada um recurso fundamental para o sucesso da organização, e essa importância e dependência tem as suas desvantagens, pelo que potenciais riscos de segurança representam ameaças significativas para o negócio.

Um elemento-chave do programa de segurança de informação é a implementação de processos de gestão de identidades e acessos, que permitem controlar e restringir o acesso dos utilizadores nos sistemas, assim como assegurar o ciclo de vida das identidades de forma automática sem a intervenção de terceiros.

Neste contexto, o objetivo desta tese de mestrado é descrever as atividades realizadas no âmbito do Projeto Autorização, que consiste na integração do sistema de retalho (Oracle Retail) com a plataforma de gestão de identidades e acessos (IBM Identity and Access Management) num grande retalhista internacional. A solução deverá ser capaz de cumprir os seguintes objetivos:

- Aprovisionamento automático de utilizadores de negócio;
- Gestão de acessos baseado em função de negócio;
- Autenticação unificada;
- Políticas de palavras-passe;
- Técnicas de criptografia.

Palavras-chave: Gestão de identidades e acessos, Aprovisionamento de utilizadores para soluções Oracle Retail, Autenticação, Autorização.

Abstract

Good Retailers are continually focused on growing their core businesses and awareness of the need to innovate and define the best technology solution in a constantly evolving market.

The ambition to implement an ideal system has become an unprecedented challenge for retail companies to improve business processes and understand customer's behavior. In this sense, the retail system (Oracle Retail) offers several products domains that provide operational processes improvements and appropriate decision-making according to the market needs, thereby helping the organization to obtain an operational and analytical infrastructure that sets it apart from the competition.

Furthermore, during the retail solution definition, it becomes necessary to follow information security best practices to ensure retailer's data assets protection. Since information is considered a valuable resource for the organization's success, this importance and dependency presents some disadvantages, potential security risks pose significant threats to the business.

A key element of the information security program is the Identity and Access Management implementation process, which allows users to control and restrict systems access and assure the identity life-cycle, including automatic provisioning without third-party intervention.

In this context, the aim of this master thesis is to describe the activities performed during Authorization Project in a large international retailer, which consists in the integration of the Identity and Access Management platform (IBM) for the Retail System (Oracle). The solution should be able to deliver the following objectives:

- Automated user-provisioning;
- Role-based access management;
- Single Sign-on authentication;
- Password policies;
- Encryption techniques.

Keywords: Identity and Access Management, Oracle Retail user provisioning, Authentication, Authorization.

Agradecimentos

Quero agradecer ao Instituto Superior de Engenharia do Porto, em especial ao Departamento de Engenharia Informática, a oportunidade concedida em apresentar um projeto que me orgulho imensamente de ter participado e de ter deixado grande parte de mim mesmo.

Ao meu orientador, Professor António Costa, pela sua dedicação ao caso apresentado, pela prontidão das suas respostas a qualquer questão, e pelo seu conhecimento universal e empírico no desenvolvimento deste estudo.

A minha gratidão pela competência, motivação e apoio da Professora Susana Nicola. Confesso que me fez pensar de forma diferente no problema.

Aos eternos colegas e amigos de projeto, fez um ano que por pouco perdíamos duas finais. A nossa perseverança foi premiada. E a minha equipa técnica, os que seguiram caminhos diferentes e os que estão presentes, sempre disponíveis a ajudar quem mais precisa.

Aos meus de sempre, família e afilhados, pela compreensão da minha ausência nestes últimos tempos, eu sei que não existe nenhuma magia para o tempo voltar atrás. Espero recompensar-vos por este esforço.

Por fim, quero deixar uma palavra de apreço pelo vosso tempo e amizade. Pela confiança que sempre depositaram em mim e no meu trabalho. Ao António S., Jacco, Martin, Quaresma, Oleksandr, Rui e Sérgio. Ao Marco e Pedro, que muito me ajudaram e motivaram nesta etapa final.

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos

Lista de Acrónimos

AD	*Active Directory*
CRP	*Conference Room Pilot*
CSAT	*Customer Satisfaction Score*
DNS	*Domain Name System*
IAM	*Identity and Access Management*
IBM	*International Business Machines*
IdM	*Identity Management*
IEC	*International Electrotechnical Commission*
ISF	*Information Security Forum*
ISO	*International Organization for Standardization*
J2EE	*Java Platform Enterprise Edition*
JDBC	*Java Database Connectivity*
LDAP	*Lightweight Directory Access Protocol*
OID	*Oracle Internet Directory*
OIM	*Oracle Identity Manager*
ORW	*Oracle Retail Workspace*
OSSO	*Oracle Single Sign-On*
RBAC	*Role Base Access Control*
ReIM	*Retail Invoice Matching*
RMS	*Retail Merchandising System*
RPM	*Retail Price Management*
RTM	*Requirement Traceability Matrix*
SAML	*Security Assertion Markup Language*
SOGP	*Standard of Good Practice for Information Security*
SSL	*Secure Socket Layer*
TI	Tecnologia da Informação
TIM	*Tivoli Identity Manager*
TLS	*Transport Layer Security*

1 Introdução

1.1 Contexto

O fenómeno da globalização dos mercados e os avanços tecnológicos com a utilização das tecnologias digitais por parte dos consumidores [Delloi15] forçaram mudanças significativas nas estruturas sociais, políticas e económicas das grandes organizações mundiais ligadas ao setor do retalho. Em consequência, de acordo com o posicionamento competitivo da organização, tornou-se preponderante conhecer a concorrência, assim como as necessidades e perceções dos consumidores com o objetivo de proporcionar uma evolução contínua do negócio.

Estes paradigmas impulsionaram os retalhistas a direcionar estratégias de negócio por diferentes áreas de atuação, procurando encontrar oportunidades em novas geografias, como meio de expandir as suas operações e atividades ao mercado global. Além disso, as iniciativas de investimento em novas soluções tecnológicas e sistemas de informação surgem como medidas imprescindíveis para compreender as expectativas dos consumidores e melhorar os processos de negócio de retalho.

Atualmente, as perspetivas de crescimento dos grandes retalhistas são tipicamente ambiciosas, e pela necessidade de manter os níveis de expansão e sustentabilidade, torna-se determinante implementar a solução e as aplicações de retalho adequadas a um mercado cada vez mais competitivo. Contudo, sendo a informação considerada um elemento vital para o sucesso do negócio, os sistemas implementados devem garantir que as normas de segurança e as suas políticas atendem aos requisitos fundamentais da segurança da informação, uma vez que potenciais riscos podem representar uma ameaça significativa para a organização.

A segurança da informação identifica-se como um requisito essencial de modo a garantir confidencialidade, integridade e disponibilidade da informação, definindo-se como um processo pelo qual a organização protege os sistemas, meios de comunicação e instalações que processam e mantêm informações fundamentais para suas operações [RWRF05].

A necessidade de assegurar os princípios da segurança da informação pode levar a alterações processuais, visto que deve ser aplicada um conjunto de regras e políticas a partir de normas padrão. A intenção é apoiar as organizações a integrar as melhores práticas de segurança nos seus processos e mitigar adequadamente os riscos. Existem várias normas aplicáveis, no entanto serão apenas referenciadas as seguintes normas corporativas: ISO/IEC 27001 e SOGP.

A norma ISO/IEC 27001 é uma referência universal estabelecida por onze domínios (e. g. controlo de acessos). Esta norma especifica requisitos, procedimentos e controlos a implementar num sistema de gestão de segurança de informação. Este modelo é sustentado numa perspetiva lógica de melhoramento contínuo e, em alguns casos, pode ser adaptado às necessidades da organização, enquanto a norma SOGP disponibiliza um conjunto de controlos por vinte áreas (e. g. gestão de acessos). Esta norma aborda a segurança da informação segundo uma estrutura conceptual orientada para o negócio, com a finalidade de manter os riscos associados aos sistemas de informação sob controlo.

Para atender aos princípios da segurança da informação em conformidade com as normas mencionadas, surge a necessidade de controlar o acesso dos utilizadores aos sistemas na organização. Isto é, garantir que apenas os utilizadores autorizados têm acesso a determinada informação e assegurar que os privilégios atribuídos sejam os suficientes para que possam desempenhar as suas funções.

Neste contexto, um programa de gestão de identidades e acessos (IAM - Identity and Access Management) é uma referência universal para a gestão do controlo de acessos em ambientes complexos e heterogéneos. Em linhas gerais, pode ser definido como um conjunto de processos que, através de mecanismos automáticos e centralizados, proporcionam o controlo de acessos sobre os sistemas de informação e a gestão do ciclo de vida das identidades em tempo real.

Em áreas de negócio dinâmicas como o retalho, no qual existem diversas aplicações e serviços, numerosos utilizadores internos e externos, a definição de uma estratégia de gestão de identidades e acessos é uma ação prioritária, sobretudo porque gerir a informação pode ser tão crucial como controlá-la.

Este documento descreve a existência de um problema num contexto real, presente num grande retalhista internacional.

1.2 Problema

O retalhista decidiu implementar uma solução de gestão de identidades e acessos (da empresa tecnológica IBM) com a intenção de fortalecer as políticas de segurança da informação, face às normas instituídas. A plataforma centralizada estende-se para todas as marcas do grupo pertencente a este retalhista, estando distribuída por dois continentes (Europa e América do Norte) e destina-se a fornecer mecanismos eficazes na administração e controlo de acessos dos utilizadores da organização.

No ímpeto de superar a concorrência e aumentar as oportunidades de negócio na área de retalho, o retalhista procurou diversificar a oferta de produtos e serviços, uma vez que considera que as novas tecnologias alteraram por completo os hábitos na sociedade, e consequentemente, o comportamento e tendências dos consumidores.

Perante este cenário, o retalhista definiu um plano estratégico para atender e competir com as exigências do mercado, sendo que a tomada de decisão em investimento tecnológico é uma realidade presente na organização, através da aquisição de aplicações digitais, sistemas de informação ou produtos desenvolvidos à medida. Assim, o grupo tomou a decisão de recomendar soluções *Oracle Retail* (da empresa tecnológica Oracle Corporation) para suportar de forma adequada a sua estratégia e melhorar os processos de negócio.

A implementação da solução preconizada foi considerada um sucesso. Apesar do resultado, reconhecido unanimemente dentro do grupo como um marco importante na reestruturação do sistema operacional, foram observados desvios nas políticas de segurança da informação do retalhista. Na Tabela 1 constam as vulnerabilidades identificadas pelo departamento de segurança e que são, em grande parte, relacionadas com o domínio do controlo de acesso.

Tabela 1 – Vulnerabilidades identificadas

Vulnerabilidade	**Descrição**
Gestão de privilégios e acessos do utilizador	Os acessos e privilégios do utilizador no sistema de retalho não são controlados automaticamente por um processo de reconciliação
Identificação do utilizador no sistema	O utilizador em algumas circunstâncias pode autenticar-se no sistema com um utilizador genérico, podendo este ser partilhado entre equipas operacionais
Gestão de palavras-passe	O utilizador não é forçado por nenhuma política de segurança a utilizar palavras-passe complexas ou alterá-las periodicamente
Tempo limite da sessão	O utilizador pode permanecer inativo por tempo indeterminado, pelo que o tempo limite da sessão não é aplicado

Vulnerabilidade	Descrição
Tentativas de autenticação no sistema	O utilizador pode errar vezes consecutivas a autenticação no sistema sem que a conta seja automaticamente bloqueada

A exploração das vulnerabilidades reportadas pode despoletar ameaças de acesso não autorizado ao sistema de retalho. Estas vulnerabilidades devem-se nomeadamente à impossibilidade de integrar a plataforma global de gestão de identidades e acessos (IAM) do retalhista com a nova solução implementada.

O departamento de segurança de informação, após analisar o problema, informou a direção a sobre a inexistência de meios que possibilitem mecanismos de controlo de acesso a recursos de informação. Estes aconselharam o projeto a colocar em prática uma solução temporária e assumir as consequências das decisões tomadas perante quaisquer riscos e responsabilidades até resolverem o problema em definitivo.

Neste seguimento, foi disponibilizado um serviço externo suportado por processos estruturados para acompanhar todos os pedidos relacionados com os acessos e privilégios dos utilizadores. Os processos estabelecidos tornaram-se ineficazes e suscetíveis a erros, em que a execução das atividades é completamente manual e depende de ações de múltiplas entidades, originando um elevado número de discrepâncias (foram contabilizadas 400 diferenças na última reconciliação) entre os privilégios dos utilizadores definidos no sistema de gestão de identidades e os que estão realmente atribuídos nas aplicações de retalho. Em alguns casos, o acesso dos utilizadores deveria ter sido eliminado ou suspenso, mas mantêm-se ativo no sistema.

A presente situação considera-se insustentável e está fora do controlo do retalhista, pois não consegue controlar quem está autenticado no sistema e que decisões está autorizado a realizar. Existe ainda outra preocupação que pode impactar o próximo objetivo: como avançar com uma nova solução integrada para centenas de lojas, no qual o índice de rotatividade dos colaboradores é elevado, sem o suporte apropriado de uma plataforma de gestão de identidades e acessos para controlar os acessos e privilégios dos utilizadores aos seus ativos.

Nesse sentido, foi proposta a realização de um projeto dedicado ao problema existente, composto por elementos de diferentes áreas de atuação. O projeto recorre a uma adaptação da metodologia de integração de soluções para alcançar a entrega da solução até ao ambiente produtivo. Esta metodologia é completamente estruturada e constituída por seis fases distintas (consultar Figura no Anexo I).

Na primeira fase (Definição da Solução) há obrigatoriamente o levantamento de requisitos com o intuito de obter todas as necessidades do retalhista. Esta interação é realizada entre sessões

com o negócio, arquitetos, fornecedores e parceiros, com o objetivo de produzir a *Requirement Traceability Matrix* (RTM).

Na Tabela 2 são descritos os requisitos identificados durante as sessões.

Tabela 2 – Listagem de requisitos

ID	Requisito	Descrição
1	Processo de identificação do utilizador	O utilizador tem de aceder a todas as aplicações com uma identidade única
2	Processo de reconciliação	Todas as identidades dos utilizadores presentes no sistema têm de ser reconciliadas
3	Processo de gestão de utilizadores	A gestão de identidades dos utilizadores tem de funcionar com processos automatizados
4	Política de palavras-passe	O utilizador tem de alterar a palavra-passe periodicamente
		As palavra-passes não devem ser armazenadas em texto simples
5	Sistema de autenticação unificado (SSO)	O utilizador deve aceder a todas as aplicações (registadas e protegidas) com autenticação única (SSO)
6	Segurança nas comunicações e criptografia	O utilizador deve autenticar-se em todas as aplicações através de protocolos seguros (e. g. HTTP com SSL/TLS)
7	Modelo de acessos baseado em funções de negócio (role-based access)	A gestão de utilizadores tem de seguir o modelo baseado em funções ou papéis de negócio
		Um utilizador tem apenas uma função ou um papel de negócio no sistema de retalho
8	Processo de auditoria	Todas as atividades entre o sistema e o utilizador deve ser monitorizada
9	Tempo limite da sessão (inatividade)	O utilizador pode permanecer inativo por um período de quinze minutos durante uma sessão

Os sistemas envolvidos estão ambos em produção, o que inevitavelmente aumenta a complexidade do problema.

1.3 Objetivos

O presente projeto é disruptivo ao nível do setor e visa o desenvolvimento de novo conhecimento tecnológico no domínio do controlo de acessos e na gestão do ciclo de vida dos utilizadores. A contribuição deste projeto destina-se igualmente a descrever as etapas necessárias em como converter o problema numa oportunidade de negócio para os atuais e futuros clientes.

Pretende-se com este estudo integrar a plataforma de gestão de identidades e acessos (IBM) com o sistema de retalho (Oracle Retail), seguindo as melhores práticas de segurança de acordo com as normas e políticas vigentes, para satisfazer as necessidades do retalhista conforme os requisitos identificados. A solução deve ser capaz de cumprir os seguintes objetivos:

- **Gestão do ciclo de vida dos utilizadores de negócio** – automatizar o processo de aprovisionamento de utilizadores para os produtos *Oracle Retail*, desde a reconciliação, criação, eliminação e suspensão dos mesmos, cumprindo a matriz de controlo de acessos com separação de responsabilidades;

- **Gestão de acessos baseado em funções** – restringir o acesso dos utilizadores aos objetos e funcionalidades dos aplicativos estabelecidos por papéis de negócio;

- **Sistema de autenticação unificado** – permitir a todos os utilizadores acederem a múltiplos aplicativos com as mesmas credenciais;

- **Política de palavras-passe** – forçar que todos os utilizadores utilizem a política de palavras-passe definida;

- **Técnicas de criptografia** – proteger os dados e comunicações com técnicas de criptografia.

Este estudo foi desenvolvido no âmbito do Projeto Autorização, rege-se pelos princípios da metodologia de integração de soluções e enquadra-se com os objetivos da unidade curricular (UC) na preparação da dissertação:

- **Interpretar o problema a resolver** – identificar os requisitos de negócio, requisitos funcionais e não funcionais que devem ser considerados na solução;

- **Sintetizar conhecimento existente relacionado com o problema** – estudar as abordagens para a resolução do problema mediante os requisitos previamente levantados e sistematizar as metodologias para desenvolvimento da solução;

- **Avaliar diferentes abordagens para a resolução do problema** – avaliar as melhores abordagens para resolução do problema, sem introduzir impactos para o negócio;

- **Desenhar uma solução para o problema** – desenhar uma solução de gestão de identidade e acessos conforme os requisitos analisados, seguindo a metodologia de integração de soluções;

- **Construir a solução para o problema aplicando** – desenvolver/implementar a solução desenhada de acordo com as especificações técnico-funcionais;

- **Avaliar a solução desenhada** – avaliar a solução recorrendo a uma estratégia de testes previamente definidos (e. g. testes unitários, aceitação, etc.).

1.4 Resultados esperados

O sistema de gestão de identidades deve ser capaz de assegurar o ciclo de vida dos utilizadores sem intervenção de terceiros. O processo deve ser gerido internamente por intermédio do departamento de recursos humanos que, através de um conjunto de regras objetivas para o negócio, consegue garantir e restringir o acesso aos ativos (e. g. sistemas, informação, etc.) do retalhista.

O sistema de gestão de acessos deve providenciar um mecanismo de autenticação, autorização e auditoria.

Através do processo de autenticação é esperado um único ponto de acesso, que permite a todos os utilizadores acederem a múltiplos aplicativos com as mesmas credenciais. O utilizador, depois de autenticado, deverá ser autorizado a consultar apenas a informação à qual tem acesso e todas as suas atividades podem ser registadas, sendo expectável ainda, resolver ou mitigar vulnerabilidades de comunicação entre sistemas.

Devido à complexidade do problema, visto que as mudanças atingem áreas sensíveis na organização, todas as operações em curso não devem afetar a continuidade do negócio ou originar impactos no sistema produtivo.

1.5 Abordagem preconizada

A abordagem preconizada consiste no estudo exaustivo dos produtos *Oracle Retail* sobre o processo de aprovisionamento de utilizadores e no domínio do controlo de acessos, sobretudo no módulo de autenticação, pois a integração entre as aplicações e a plataforma de gestão de acessos corporativa carece de conhecimento.

A recomendação, através da prova de conceito sobre o comportamento dos componentes de diferentes tecnologias, permite uma avaliação teórico-prática específica para cada produto.

2 Contexto e Estado da arte

2.1 Detalhes sobre contexto e problema

A evolução das tecnologias de informação e os fenómenos subjacentes são fatores preponderantes na influência do sucesso dos negócios atuais. Estes suplantaram os modelos de negócios tradicionais de retalho e influenciaram inequivocamente a dinâmica organizacional das grandes empresas retalhistas. Na atual conjuntura, associada ao ritmo acelerado de crescimento económico, os retalhistas procuram um sistema centralizado e especializado que proporcione uma infraestrutura integrada para permitir uma análise confiável dos dados e tomar decisões baseadas na informação recolhida. Neste contexto, enquadrado por um programa estratégico de reestruturação e atualização do sistema operacional de um grande retalhista internacional (presente em onze países), realizou-se a implementação de um sistema Oracle Retail, em função das suas necessidades específicas e críticas para o negócio.

A (Figura 1) representa uma adaptação da solução implementada. Os artefactos que descrevem a arquitetura e a decomposição do sistema em todos os seus componentes significativos pode ser visualizada no modelo *Retail Reference Architecture* [RRA11].

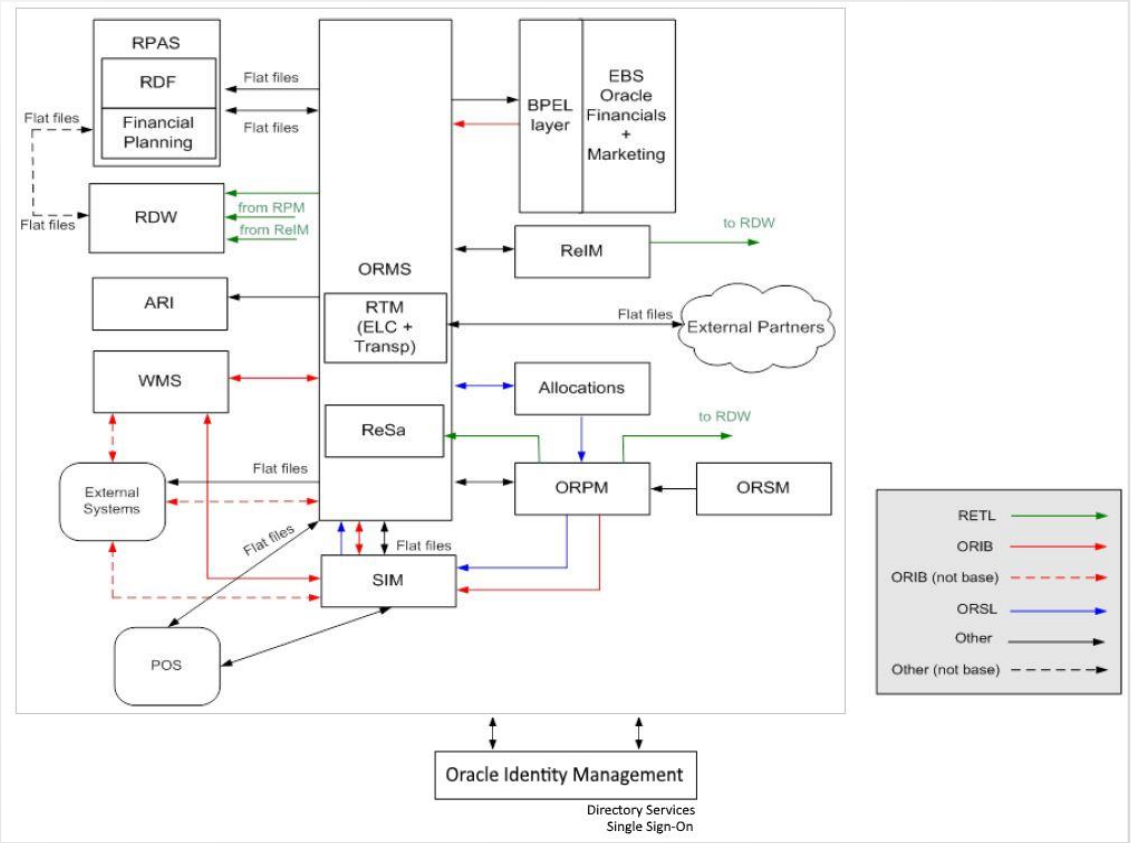


Figura 1 – Sistema Oracle Retail
(Imagem de: Wipro LTD. 2012. Oracle Retail Fundamentals, p. 8)

O sistema (Oracle Retail) implementado compreende vários domínios de produtos e estes são constituídos por vários módulos aplicacionais para suportar as operações globais da organização. Os módulos aplicacionais interagem e comunicam entre si como parte de uma arquitetura modular multicamada, fornecem informações precisas e desempenham funções distintas para cada processo de negócio num ambiente totalmente integrado.

Observa-se igualmente (Figura 1) uma plataforma de gestão de identidades (Oracle Identity Management) desenvolvida para aumentar o nível de segurança do sistema de retalho, sendo constituída por componentes que oferecem funcionalidades específicas para suportar o processo de controlo de acessos e a gestão de utilizadores. Os componentes podem ser instalados individualmente ou em blocos dependentes, consoante as necessidades identificadas no contexto do projeto ou mediante os requisitos das aplicações, uma vez que no processo de autenticação o serviço de diretórios torna-se praticamente obrigatório para grande parte dos módulos aplicacionais do sistema de retalho.

Existem aplicações, como no caso do (ORMS), que podem confirmar a identidade do utilizador na base de dados, mas como recomendação de boas práticas de segurança, a informação dos utilizadores deverá ser armazenada e centralizada num repositório único.

A plataforma de gestão de identidades abrange três áreas funcionais [IdM08]:

- **Serviço de diretórios** – o serviço de diretórios armazena os dados da identidade do utilizador e as respetivas credenciais de acesso. O principal componente da maioria das plataformas de gestão de identidades é o serviço de diretórios LDAP, este serviço é fundamental no processo de autenticação e autorização;

- **Gestão de identidades** – engloba um conjunto de atividades como a gestão de utilizadores, grupos e workflows de aprovação. Enquanto no serviço de diretório, contém os objetos e informações dos utilizadores, esta área de administração proporciona a gestão da identidade do utilizador através de recursos fornecidos por tecnologias de aprovisionamento;

- **Gestão de acessos** – representa um conjunto de políticas e regras formalizadas. A gestão de acessos reforça a segurança com mecanismos de autenticação, controla e audita o acesso dos utilizadores aos recursos da empresa e bloqueia atividades fraudulentas de forma pró-ativa.

As três áreas funcionais anteriormente descritas são apoiadas por componentes[1] dedicados e tecnologias no desenvolvimento destes processos. Na definição da solução, para servir diferentes propósitos e segundo as evidências recolhidas durante o estudo do problema, foram instalados e configurados apenas dois componentes da plataforma [IdM08]:

- **Oracle Internet Directory (OID)** – serviço de diretórios (Figura 2) baseado em padrões LDAP v3, caracteriza-se como um elemento fundamental no processo de autenticação nas aplicações *Oracle Retail*. Este funciona como um repositório central e contém informações sobre a identidade dos utilizadores, credencias de acesso, atributos, objetos e grupos essenciais no processo de autorização;

- **Oracle Single Sign-On (OSSO)** – componente de autenticação (Figura 3) para as aplicações *Oracle Retail* implementadas. Dependente do módulo que reside no Servidor *OracleAS Middle Tier* (mod_osso) e do serviço de diretórios (OID) para verificar a identidade e validar as credenciais do utilizador.

[1] Podem ser encontrados vários componentes para além dos mencionados, tais como: *Oracle Virtual Directory, Oracle Identity Manager, Oracle Access Manager, Oracle Role Manager, Oracle Identity Federation, Oracle Enterprise Single Sign-On*, etc.

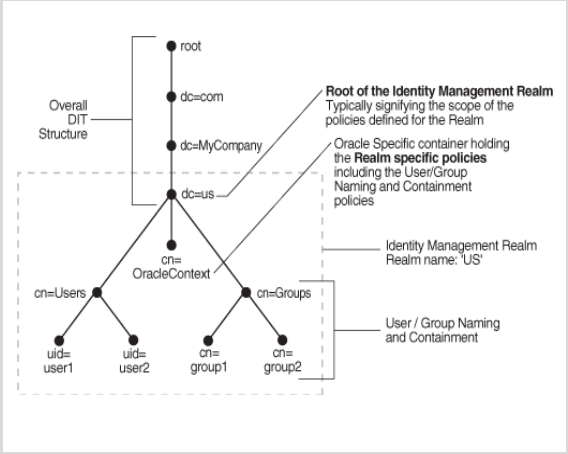


Figura 2 – Oracle Internet Directory
(Imagem de: Oracle. 2009.[AGOID], p. 32-3)

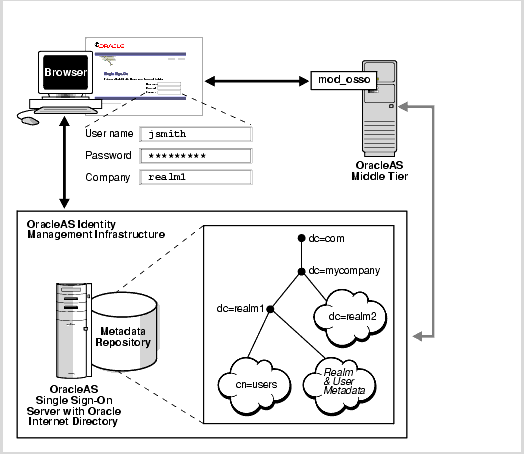


Figura 3 – Oracle Single Sign-On
(Imagem de: Oracle. 2005. [AGCS], p. 7-3)

Estes componentes devem ser incluídos no desenho da solução no sentido de satisfazer os requisitos das aplicações de retalho e garantir um bom funcionamento do sistema. Apesar do componente de autenticação (OSSO) ser classificado como facultativo, este apresenta-se como o único em conformidade com a matriz de certificação suportada pela Oracle para fornecer um serviço de autenticação unificada.

Para melhor compreender as abordagens identificadas e a decisão de instalar somente estes dois componentes durante a implementação do sistema Oracle Retail, procedeu-se a uma análise técnico-funcional das soluções propostas para o desenvolvimento de um modelo de gestão de identidades e acessos. Esta análise passa obviamente por uma consulta dos documentos elaborados pelo projeto sobre as três áreas funcionais anteriormente apresentadas.

Um outro objetivo desta análise é reunir toda a informação relevante aquando da tentativa de integração entre os sistemas e identificar a causa raiz do problema.

Solução OR-IdM-EU

A solução OR-IdM-EU consiste no desenvolvimento de uma API (Oracle Retail Provisioning) que fornece as funcionalidades de aprovisionamento para os utilizadores de negócio. Na (Figura 4) apresenta-se a interface de interação entre o sistema de gestão de identidades do retalhista (TIM) e o sistema de retalho (Oracle). No entanto, não existem evidências que sustentem a concepção de uma nova solução para atender todos os requisitos em detrimento do próprio sistema de gestão de identidades.

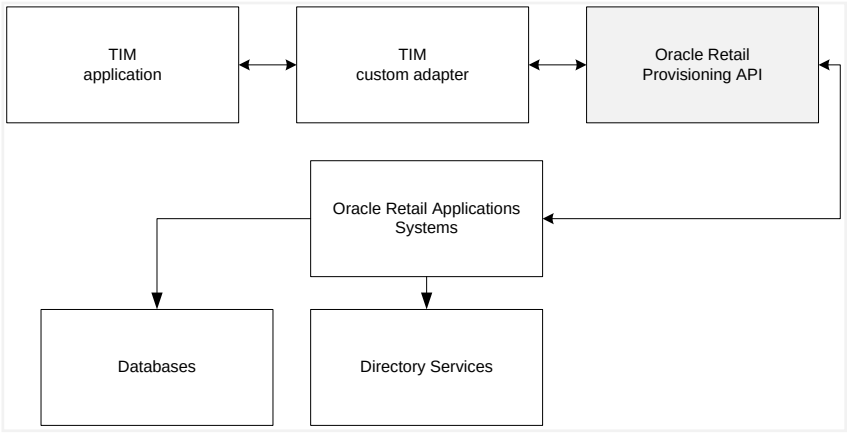


Figura 4 – API OR-IdM

Foram encontrados outros aspetos que merecem ser considerados na análise desta solução, também relacionados com processo de autenticação:

- Apresenta um estudo cuidado e rigoroso sobre o processo de aprovisionamento, mas contrapõe com alguns procedimentos inadequados sobre a lógica de aprovisionamento das aplicações de retalho, com especial enfâse no método de eliminação dos utilizadores;

- Apresenta referências genéricas sobre as responsabilidades de cada sistema e não fornece informação relevante das políticas de segurança a serem adotadas;

- Confirma o serviço de diretórios LDAP (Oracle) como repositório central de utilizadores e encontra-se de acordo com os requisitos das aplicações, mas apresenta uma referência abstrata e pouco objetiva ao serviço de diretórios existentes (i.e. IBM-LDAP, AD) e não esclarece uma possível abordagem de integração conforme os requisitos identificados;

- Confirma o *Oracle Single Sign-On* (OSSO) como serviço de autenticação e encontra-se de acordo com os requisitos das aplicações, mas apresenta uma arquitetura que não corresponde às funcionalidades pretendidas;

- Apresenta evidências sobre a possibilidade de utilizar outros componentes de autenticação com as aplicações de retalho. Uma decisão questionável, visto que no processo de autenticação, somente o *Oracle Single Sign-On* (OSSO) se encontra na lista de produtos certificados com as aplicações *Oracle Retail*.

Solução OR-IdM-US

A solução OR-IdM-US consiste no desenvolvimento de uma nova solução de gestão de identidades baseado em padrões de arquitetura J2EE, com vista a facilitar a construção de um modelo flexível que possibilite recursos eficazes de administração de utilizadores entre os vários sistemas.

Durante a análise identificaram-se os aspetos críticos na concepção da solução:

- Confirma o serviço de diretórios LDAP (Oracle) como repositório central de utilizadores e encontra-se de acordo com os requisitos das aplicações, mas não esclarece uma possível abordagem de integração com o serviço de diretório existente conforme os requisitos identificados;

- Apresenta um estudo vago e abstrato sobre o processo de gestão de identidades, proporcionando alterações significativas no modelo de dados dos aplicativos;

- Evidencia procedimentos incoerentes sobre a lógica de aprovisionamento e na relação entre componentes, possibilitando a ocorrência de inconsistência de dados;

- Carece de um modelo de acessos baseado em funções de negócio;

- Definida pela ausência de processos fundamentais na reconciliação e gestão das identidades;

- Desprovida de mecanismos seguros, políticas e normas de segurança;

- Apresenta um modelo de autenticação através do protocolo SAML, ao contrário de utilizar o componente certificado *Oracle Single Sign-On* (OSSO);

- Remetida a uma lista de atividades genéricas agrupadas por designações igualmente superficiais, sendo inconclusiva na informação apresentada.

As abordagens identificadas pelo projeto apresentam-se ambíguas e contraditórias, descontextualizadas da solução pretendida, visto que não atendem aos requisitos estabelecidos pelo retalhista. Verifica-se ainda que as abordagens não tiveram em consideração as restrições tecnológicas e dependências das aplicações instaladas.

Na definição do modelo de gestão de identidades decidiu-se pelo desenvolvimento de novas soluções e componentes totalmente customizados. Isto porque não existe uma solução no mercado que permita sem esforço automatizar o processo de aprovisionamento de utilizadores para os vários módulos aplicacionais.

No módulo de autenticação, ignoraram-se as dependências entre os componentes, inclusive encontradas na documentação oficial. Os produtos contêm os seus próprios requisitos para o funcionamento num ambiente SSO (Figura 5) e estão tecnologicamente dependentes entre si, com um componente de autenticação (OSSO) e um serviço de diretórios (OID).

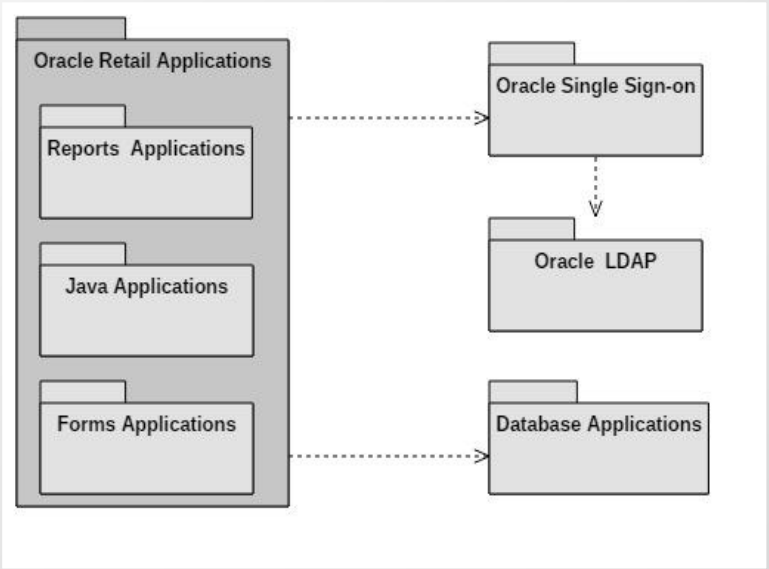


Figura 5 – Aplicações configuradas com SSO

A interoperabilidade entre sistemas parece ser uma das origens do problema, embora conceptualmente simples, os produtos apresentam múltiplas tecnologias (e.g. Java, Forms, Reports) e especificidades próprias de segurança para cada módulo. De acordo com a análise efetuada, foi observado a ausência de requisitos elementares, mesmo ao nível da limitação dos produtos que condicionaram substancialmente o estudo de abordagens capazes para integrar as soluções e, por conseguinte, um desenho adequado para o problema.

Pela documentação consultada do projeto sabe-se também que o sistema de gestão de identidades e acessos (Tivoli Identity and Access Management) do retalhista suporta um conjunto de requisitos que carecem de conhecimento técnico por parte das entidades envolvidas, apresentando riscos ao nível da capacidade de integração entre os vários componentes da solução de retalho.

O sistema apresentado na (Figura 6), doravante designado pelo acrónimo (TIM/TAM) representa a solução global de autenticação, autorização e aprovisionamento de utilizadores do grupo retalhista. É composto por dois módulos principais:

- **TIM (Tivoli Identity Manager)** – fornece uma solução de gestão de utilizadores segura, automática, baseada em políticas e normas. A solução permite a gestão do ciclo de vida das identidades na organização em ambientes heterogêneos e centraliza o acesso dos utilizadores a recursos distintos, usando políticas que simplificam as operações associadas ao acesso do utilizador [IBMPo]. Os adaptadores têm um papel importante na solução, fornecem uma interface entre um recurso e o servidor (IBM Tivoli Identity Manager) e funcionam como administradores virtuais na plataforma de destino para o aprovisionamento de contas. Desempenham tarefas que envolvem a criação, suspensão, modificação de contas e atributos [IBMIad].

- **TAM (Tivoli Access Manager) –** fornece uma solução completa para autenticação, autorização e gestão de políticas de segurança para proteção de recursos dentro e fora da rede. O componente *WebSEAL* surge para suportar o serviço de autenticação e integra-se o com o serviço de autorização (TAM). Este pode ser integrado com *Tivoli Access Manager* (TIM) de modo a fornecer uma solução global de controlo de acessos [IBMTam].

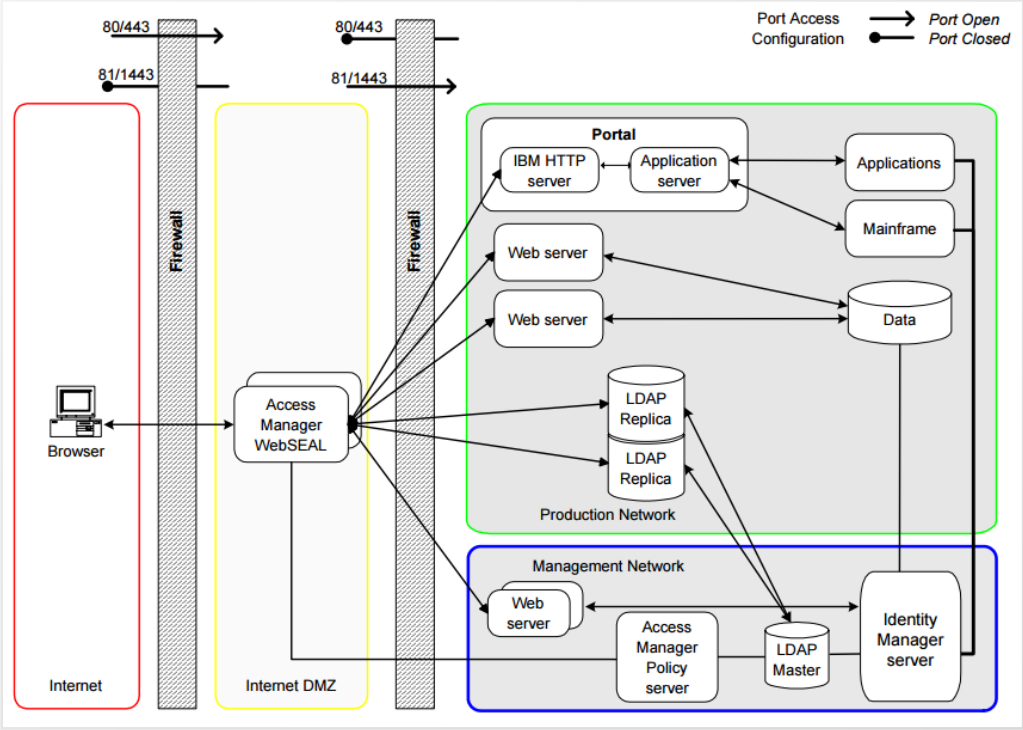


Figura 6 – Sistema TIM/TAM

(Imagem de: IBM. 2009. Identity Management Design Guide with IBM Tivoli Identity Manager, p. 99)

No entanto era necessário ao projeto promover uma das soluções descritas anteriormente para integrar os dois sistemas, apesar da incerteza técnica relativa ao desafio tecnológico, tentando-se alcançar este objetivo, mas sem sucesso.

A solução (**OR-IdM-EU**) revela evidências de uma tentativa fracassada ao integrar diretamente o componente de autenticação (TAM) com as aplicações de retalho e o projeto recomenda a realização de uma prova de conceito. Termina a fase de especificação da API (Oracle Retail Provisioning) mas não inicia a fase de construção. Enquanto a solução (**OR-IdM-US**) apresenta um modelo de autenticação federada utilizando o protocolo SAML, mas o componente (Oracle Identity Federation) não foi contemplado na solução, para além disso demonstra-se incompatível com as aplicações *Oracle Retail*. Durante a avaliação da solução de gestão de identidades falha os testes de aceitação, não satisfazendo os critérios de aceitação.

Em consequência, o valor de disponibilizar uma infraestrutura adequada pode estar em risco, pela incapacidade da gestão dos acessos dos utilizadores de forma garantir os elementos fundamentais da segurança da informação, mas igualmente ao nível do crescimento operacional da organização. Este resultado também pode ser relevante para o aparecimento de novas ameaças, que podem ser exploradas indevidamente sobre os sistemas críticos que suportam processos operacionais, financeiros ou confidenciais. Segundo os especialistas na área de segurança, estimam que 80% a 90% dos ataques aos sistemas de informação são praticados por pessoas internas [KDSJ10].

2.2 Estado da arte em abordagens existentes

O sistema Oracle Retail é um sistema de gestão de retalho construído pela Oracle essencialmente à base de aquisições externas. Tudo se iniciou em 2005 com a aquisição da ER Retek, seguida de várias aquisições posteriores, às quais ainda se somam alguns desenvolvimentos próprios. Este modelo de crescimento garante uma plataforma de soluções especializada na área de negócio de retalho, reconhecida a nível mundial com vários domínios de produtos (e.g. Stores, Merchandising, Planning and Optimization, Infrastructure), alguns dos quais exclusivos (ver Anexo II).

Contudo, pode gerar um conjunto de dificuldades quando é pretendido implementar soluções que se relacionam com a integração de plataformas de gestão de identidades e acessos, uma vez que o sistema não é construído com o foco na integração destes processos e este comportamento reflete-se obviamente nos produtos de retalho. Numa primeira fase serão descritos os principais conceitos relativos ao domínio do controlo de acessos e outras referências como o processo de aprovisionamento que são de maior importância para o caso:

- **Controlo de acessos** – processo de restringir o acesso de uma determinada entidade (e.g. sistemas, aplicações, redes) a um utilizador, com base em políticas e critérios aos quais devem ser atribuídos os privilégios suficientes para desempenharem as suas tarefas. O controlo de acesso é um conceito abrangente e a sua implementação assume geralmente um modelo de acessos baseado em funções de negócio, garantindo que somente os utilizadores autorizados possam ter acesso ao sistema e a determinada informação.

- **Autenticação** – processo de confirmar a identidade do utilizador que procura o acesso. O processo de autenticação requer normalmente que o utilizador forneça um nome e credenciais de acesso para se identificar e se autenticar no sistema, permitindo o início de uma possível sessão. Este processo pode ser estendido para incluir certificados digitais, mecanismos biométricos ou autenticação multi-factor.

- **Autorização** – processo que determina quais as ações que um utilizador autenticado pode realizar ou executar no sistema.

- **Autorização de dados** – processo que determinar os direitos e privilégios de um utilizador autenticado sobre um conjunto particular de dados e objetos de negócio. Este processo verifica igualmente se o utilizador autenticado está associado a algum nível na hierarquia organizacional e mercadológica.

- **Auditoria** – processo que documenta as atividades dos utilizadores no sistema, nomeadamente quem acede, que ação tomou, quando e onde. Esses registos são importantes na reconstrução de eventos e posteriormente na identificação de incidentes de segurança.

- **Aprovisionamento** – processo que permite a gestão do ciclo de vida das identidades no sistema, desde a criação, modificação, suspensão ou eliminação dos utilizadores.

- **Atributos do utilizador** – dados associados a um utilizador de negócio. Não têm impacto no processo de autenticação ou autorização. Exemplos típicos de atributos são: nome do utilizador, preferência de idioma e endereço de correio eletrónico.

- **Repositório do utilizador** – repositório que contém os dados (i.e. user store: identidade digital, senha) do utilizador, necessários para os processos de autenticação e autorização.

As aplicações integrantes do sistema Oracle Retail contêm vários modelos de segurança que podem variar consoante os métodos de controlo aplicados e objetivos em termos de funcionalidades da solução. Os modelos também definem características importantes de segurança para diferentes tecnologias presentes no sistema, em particular atenção para o aprovisionamento de utilizadores de negócio, mais especificamente as tabelas de segurança afetadas, que influenciam o acesso e as operações que podem efetuar nas aplicações.

Os procedimentos operacionais a utilizar na gestão de utilizadores são aspetos essenciais a ter em consideração, dado que cada aplicação *Oracle Retail* apresenta as suas próprias necessidades de aprovisionamento, que podem incluir múltiplas operações no serviço de diretórios, originar a criação de utilizadores de base de dados e registos adicionais em tabelas pertencentes a um esquema. O motivo principal está relacionado com as tecnologias de desenvolvimento do produto e especificidades que constituem a lógica aplicacional [ORSP14].

As figuras seguintes pretendem exemplificar diferentes modelos de segurança e as necessidades intrínsecas de várias aplicações *Oracle Retail* referentes ao processo de aprovisionamento.

Modelo de segurança – RMS, ReSA, RTM

As aplicações *Oracle Retail Merchandising System* (RMS), *Sales Audit* (ReSA) e *Trade Management* (RTM) são soluções desenvolvidas em tecnologia *Oracle Forms*[2], partilham as mesmas tabelas no esquema relacional da base de dados (RMS) e utilizam os mesmos mecanismos de autenticação e autorização (Figura 7).

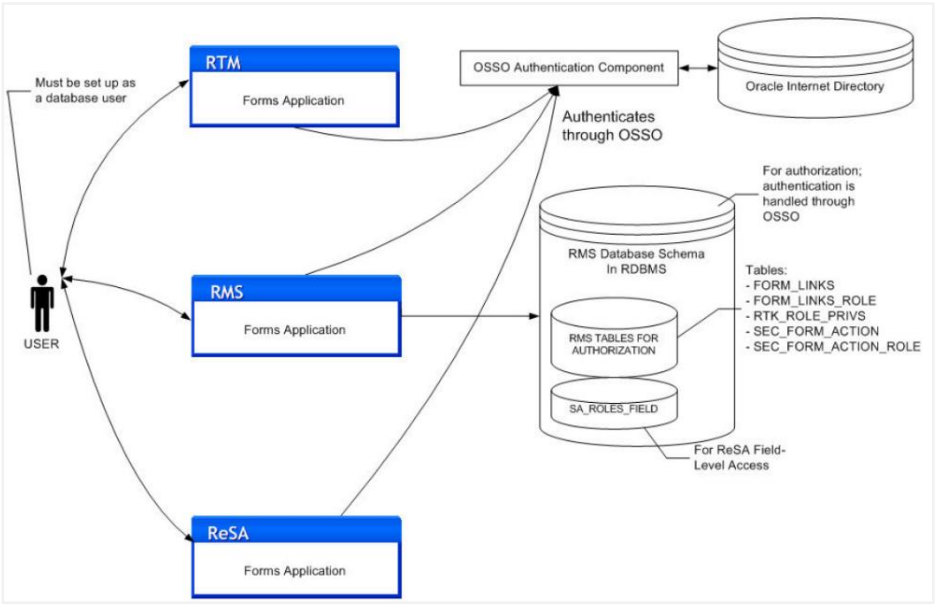


Figura 7 – Modelo de segurança (RMS, ReSA, RTM)
(Imagem de: Oracle. 2009. [ORSP13], p. 10)

[2] Oracle decidiu-se por uma nova estratégia no desenvolvimento tecnológico dos novos produtos e este comportamento reflete-se nas versões mais recentes (v16), que são desenvolvidas em ADF (Application Development Framework), exceto o produto RPM.

O processo de aprovisionamento das aplicações (RMS, ReSA, RTM) para novos utilizadores de negócio, deve-se refletir na seguinte abordagem:

1. Criar um utilizador de base de dados
   1.1. Conceder privilégios de sistema (e.g. session)
   1.2. Atribuir funções de negócio (e.g. Buyer)
   1.3. Criar sinónimos (objetos que são propriedade de outro utilizador no esquema relacional)
2. Inserir registos nas tabelas (e.g. USER_ATTRIB) para garantir a autorização a menus, pastas ou links
3. Inserir registos nas tabelas (e.g. SEC_USER_GROUP) para garantir a autorização de dados
4. Inserir registos nas tabelas (e.g. SA_EMPLOYEE) para garantir acesso ao módulo de auditoria de vendas (ReSA)

Os passos realizados para a criação do utilizador podem ser incrementados no caso de as aplicações participarem no processo de autenticação única (Figura 8):

5. Criar um utilizador no serviço de diretórios LDAP (OID)
   5.1. Associar o RAD[3] ao utilizador LDAP
      5.1.1. Determinar ORCLGUID (identificador único do utilizador)
      5.1.2. Criar o ORCLOWNERGUID (no contexto Oracle)
      5.1.3. Criar o RAD com os detalhes de ligação da base de dados (RMS) e as credenciais de acesso do utilizador criado (Ponto 1)
6. Associar privilégios no serviço de diretórios de acesso ao Portal (ORW), caso exista.

[3] *Resource Access Descriptors* (RAD) são um requisito para a autenticação (SSO) das aplicações *Oracle Forms*. Ao contrário do que acontece com as aplicações desenvolvidas com a tecnologia *Oracle ADF* (Application Development Framework).

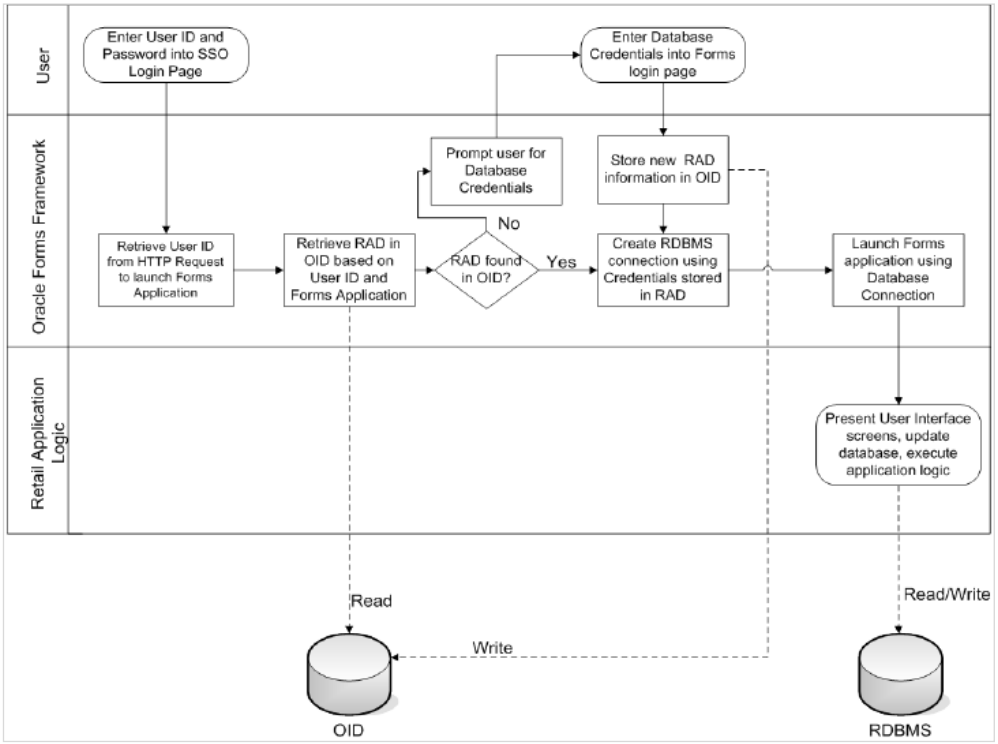


Figura 8 – Autenticação SSO - Oracle Forms
(Imagem de: Oracle. 2009. [ORSP13], p. 6)

As aplicações (RMS, ReSA, RTM) que utilizam a tecnologia *Oracle Forms* apresentam particularidades singulares, dependendo de um conjunto de operações que devem ser respeitadas durante o processo da criação de um utilizador. As operações podem ser divididas e organizadas por três áreas de atividades: Criar o utilizador na estrutura de base de dados com os privilégios, funções de negócio e sinónimos; Acrescentar atributos e privilégios do utilizador nas tabelas de segurança no esquema da base de dados; Adicionar o utilizador ao repositório central LDAP, assim como providenciar acesso ao Portal e associar o RAD.

Na eventualidade de qualquer falha ou omissão entre as diferentes operações a serem executadas, tal implica a revisão e análise de todas as etapas, tornando-se num processo complexo, por vezes penoso e suscetível a múltiplas ações que exigem intervenções manuais na correção dos erros encontrados.

A criação do RAD (Resource Access Descriptor) é o tipo de erro mais comum durante a criação do utilizador, sendo obrigatório no processo de autenticação (SSO) das aplicações *Oracle Forms* mencionadas. O RAD representa tecnicamente uma entrada adicional no serviço de diretórios LDAP (OID) com os detalhes de identificação do utilizador de base de dados e funcionalmente corresponde a uma camada adicional de segurança no processo de autenticação, comportando-se de forma completamente transparente para o utilizador.

O RAD pode ser definido essencialmente de duas formas: podem ser criadas as entradas no serviço de diretórios pelo administrador do sistema, através do carregamento de ficheiros em

formato LDIF (LDAP Data Interchange Format), ou podem ser criadas dinamicamente pelo utilizador através de um formulário, após a primeira autenticação com sucesso (Figura 10). No entanto, de modo a ser possível concluir a operação, deve ser partilhado com o utilizador a informação considerada confidencial, como detalhes que especificam ligações da base de dados e as credenciais de acesso, contrariando dessa forma as boas práticas de segurança.

A informação apresentada refere-se unicamente ao processo de criação do utilizador no sistema seguindo os procedimentos oficiais da Oracle, mas o ciclo de vida de um utilizador compreende outros processos inerentes a um sistema de gestão de identidades. Quando o pedido for para eliminar ou modificar privilégios do utilizador, não existem documentos oficiais a facultar essa informação.

Modelo de segurança – WMS

A aplicação *Oracle Retail Warehouse Management System* (WMS) é uma solução desenvolvida em tecnologia *Oracle Forms*, utiliza as tabelas (DMS_USER) e (DMS_MENU) para garantir a autenticação e autorização (Figura 9) no esquema relacional da base de dados (WMS). A aplicação denota limitações ao nível da autenticação, dado que não suporta (SSO) e, por esse motivo, não tem como requisito um serviço de diretórios LDAP.

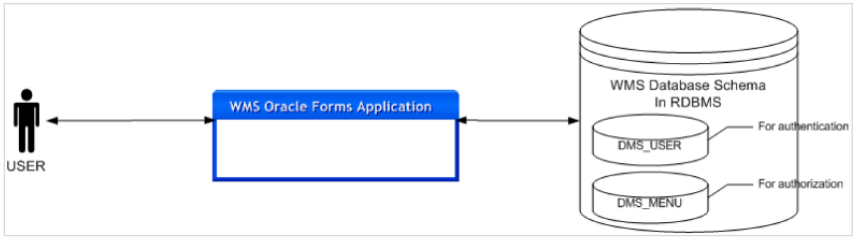


Figura 9 – Modelo de segurança (WMS)
(Imagem de: Oracle. 2009. [ORSP13], p. 32)

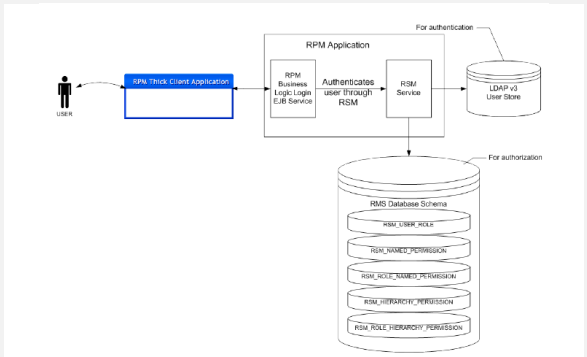
Modelo de segurança – RPM, SIM, ReIM, ALLOC

A aplicação *Oracle Retail Price Management* (RPM) funciona com base na tecnologia *WebStart/Fat Client*, assim como o *Oracle Retail Store Inventory Management* (SIM), enquanto que as aplicações *Oracle Retail Invoice Matching* (ReIM) e *Oracle Retail Allocation* (ALLOC) funcionam baseadas na tecnologia *Web Java*.

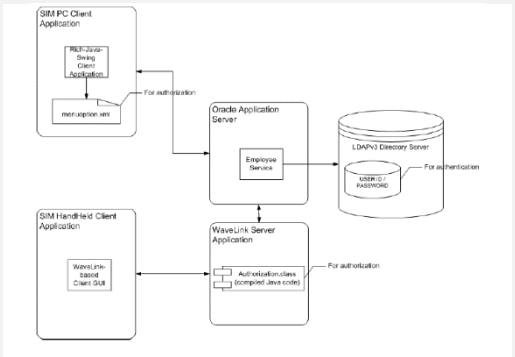
O componente de autenticação (OSSO) pode ser parte integrante das aplicações, caso seja desejada uma autenticação unificada. Neste cenário, o serviço de diretórios LDAP v3 (e.g. OID) torna-se requisito e armazena informações referentes ao utilizador para assegurar a autenticação.

O módulo de segurança *Oracle Retail Security Manager* (RSM) fornece mecanismos para autenticação e autorização exclusivos para o RPM. As aplicações descritas partilham o mesmo esquema da base de dados, com a exceção da aplicação de loja (SIM), conforme os modelos de segurança apresentados (Figura 10).

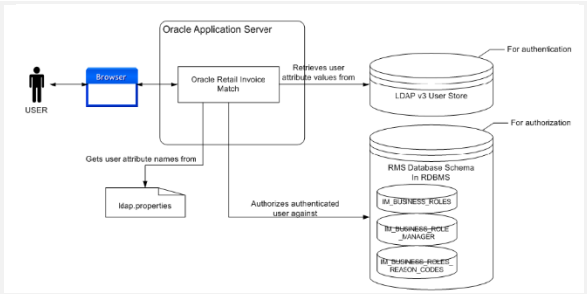
RPM



SIM



ReIM



ALLOC

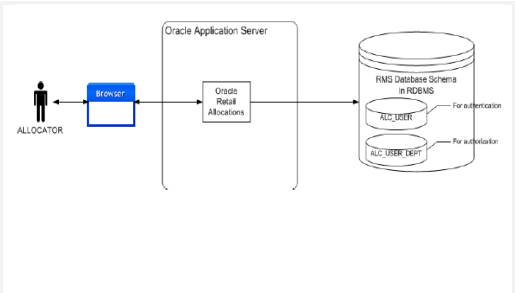


Figura 10 – Modelo de segurança (RPM, SIM, ReIM, ALLOC)
(Imagem adaptada de: Oracle. 2009. [ORSP13], p. 5-22)

No processo de aprovisionamento as diferenças são mais acentuadas. Na tabela seguinte, podem ser identificadas as particularidades e necessidades das aplicações no contexto da autenticação e autorização (Tabela 3).

Tabela 3 – Necessidades no processo de autenticação e autorização

Aplicação	**Autenticação** (com Single Sign-on)	**Autorização**
RPM	• Criar utilizador no LDAP (depende do objectClass: retailUser)	• Inserir utilizador e associar função de negócio na tabela RSM_USER_ROLE (depende da tabela RSM_ROLE)
SIM	• Criar utilizador no LDAP (depende do objectClass: simUser)	• Associar função de negócio e loja(s) ao utilizador no LDAP v3 (depende do objectClass: simUserRole e dos atributos: userstores, userrole e userrolestores)
ReIM	• Criar utilizador no LDAP	• Inserir utilizador na tabela IM_USER_AUTHORIZATION • Associar função de negócio ao utilizador na IM_BUSINESS_ROLE_MEMBER (depende da IM_BUSINESS_ROLES)
ALLOC	• Criar utilizador no LDAP • Inserir utilizador na tabela ALC_USERS	• Associar departamentos ao utilizador na tabela ALC_USER_DEPTS

No processo de aprovisionamento percebe-se que cada aplicação tem o seu próprio módulo de gestão de identidades. O método diverge entre os produtos, apresentando algumas variantes consoante as funções e acessos.

2.3 Incertezas que o estudo procurou resolver

O projeto apresenta um elevado nível de complexidade e desafios técnicos associados ao objetivo de integrar os sistemas atualmente em produção, podendo provocar grandes impactos nas estruturas do retalhista. Este estudo pretende descrever e resolver qualquer incerteza científica ou tecnológica existente no projeto.

2.3.1 Arquitetura da solução

Diferentes pontos de vista merecem atenção neste contexto, isto porque uma reestruturação completa dos processos existentes e da arquitetura aumenta exponencialmente a complexidade do problema. Considera-se então, sempre que for exequível, definir a solução com a arquitetura existente, reutilizar componentes e proceder com configurações não intrusivas para o sistema como abordagens primárias. Qualquer problema identificado que seja resolvido com alterações profundas (e.g. a nível da infraestrutura, mudança de tecnologia) ou uma abordagem supostamente intrusiva é prontamente avaliado pelo programa.

2.3.2 Sistema Ideal

O estudo realizado sem explorar detalhadamente os requisitos dos produtos originou o insucesso da integração, que se tornou numa desilusão transversal a toda a organização. Consequentemente e segundo as normas e boas práticas de segurança em vigor, coloca em causa os objetivos delineados pelo grupo:

- Manter as operações de negócio contínuas, confiáveis, eficazes e competitivas;
- Garantir a confidencialidade de informações críticas;
- Proteger dados de clientes e funcionários;
- Cumprir os requisitos legislativos;
- Prevenir danos financeiros;
- Evitar danos à reputação.

Para além dos sacrifícios durante a implementação e do resultado que compromete a operacionalidade de áreas de negócio, o retalhista considera-se exposto a riscos de diferentes naturezas, devido à impossibilidade de controlar os acessos das identidades no sistema.

O diagrama (Figura 11) descreve o comportamento dos vários elementos e atores do sistema atual, este é governado com ausência de processos no domínio do controlo de acessos e na gestão dos utilizadores, totalmente descentralizado e gerido de forma independente por entidades externas.

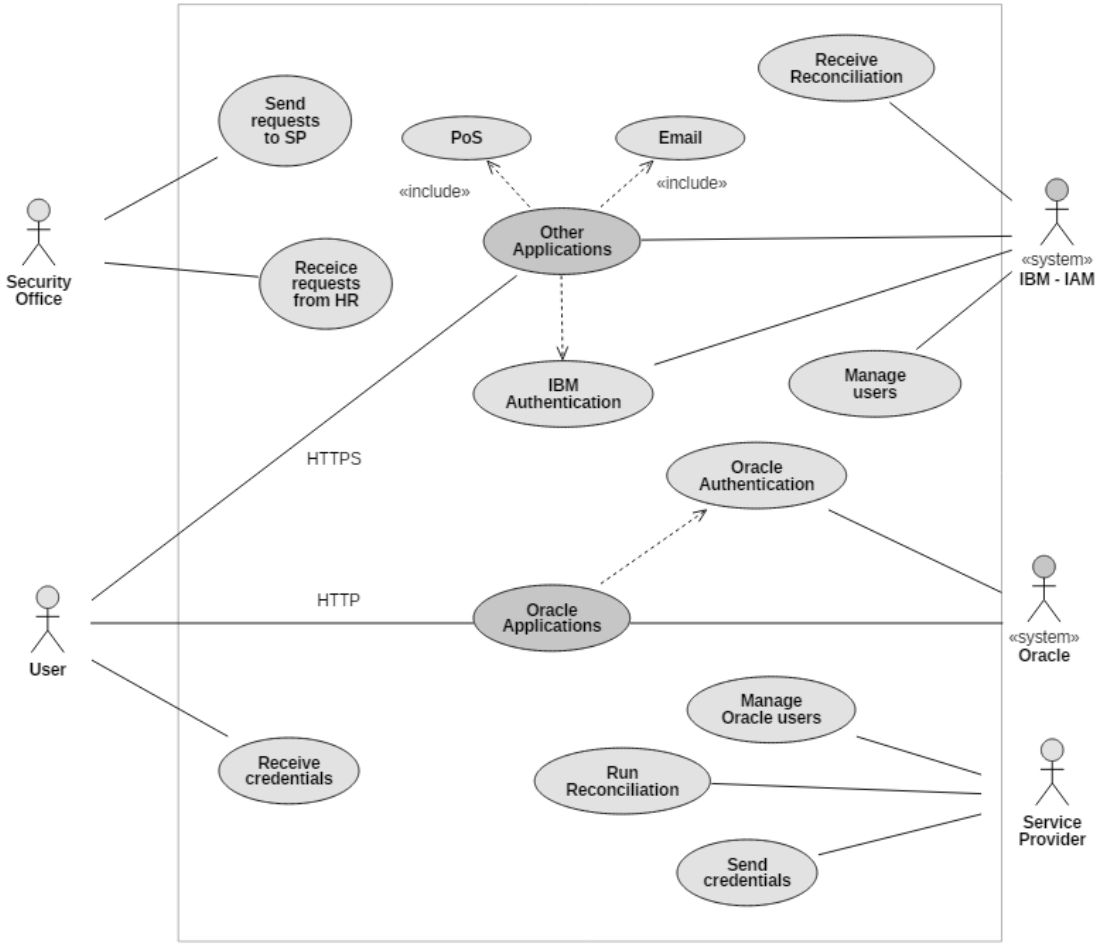


Figura 11 – Sistema atual do retalhista

- Comprova-se que o sistema apresenta uma plataforma de autenticação sustentada por múltiplos pontos de acesso, seguros e não seguros, inviabilizando o processo de verificação do utilizador no sistema de retalho;
- Confirma-se a ausência de mecanismos eficazes para controlar o acesso do utilizador sobre determinada funcionalidade no sistema e o respetivo acesso à informação;
- Manifesta-se incapaz na gestão do ciclo de vida dos utilizadores, o processo de aprovisionamento de utilizadores denota fragilidades e encontra-se inteiramente dependente de terceiros;
- Verifica-se de que todo o processo de reconciliação revela inconsistências, permite uma tomada de decisão errada de ações de aprovisionamento;
- Evidencia-se inapto para a autorização e privilégios dos utilizadores no sistema, não garantindo correções em caso de diferenças;

- Constata-se que os utilizadores podem ter diferentes credenciais e demonstra a ausência de mecanismos para a recuperação de palavras-passe no acesso ao sistema de retalho, colocando em causa uma possível continuidade do negócio;

- Denota-se que a relação entre os diversos atores envolvidos aumenta a entropia do sistema.

O sistema ideal relaciona-se com o propósito desta solução, que consiste na integração do sistema de gestão de identidades e acessos (IBM) e o sistema de retalho (Oracle) numa adaptação da atual infraestrutura. Pretende-se que seja autónoma e centralizada, provida de mecanismos seguros com a capacidade de garantir um sistema único de identidades. O sistema que melhor satisfaz os requisitos do retalhista está representado na Figura 12.

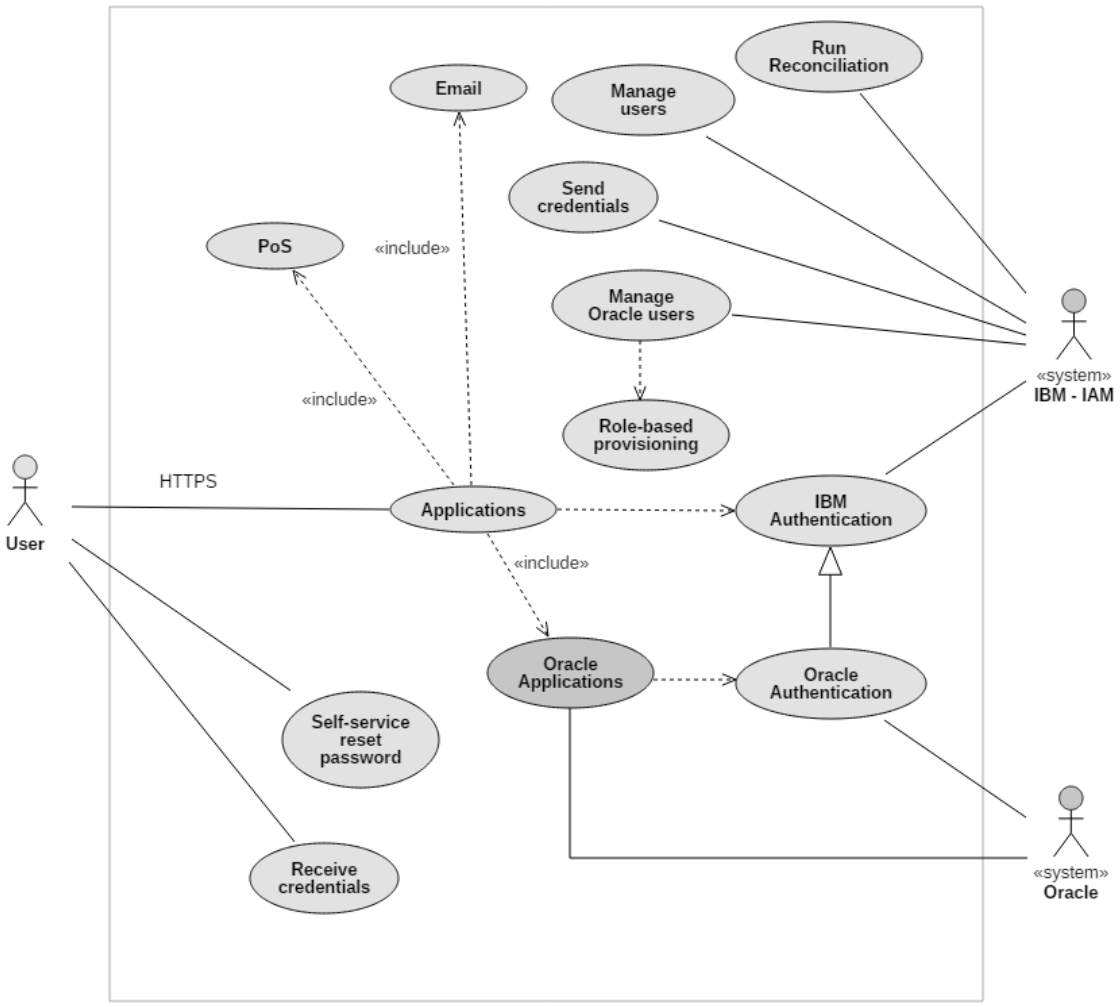


Figura 12 – Sistema ideal

Em termos gerais é percetível que o sistema ideal:

- Reutiliza componentes da arquitetura existente;
- Apresenta uma plataforma de autenticação unificada, com o uso de protocolos seguros de acesso às aplicações;
- Descreve um sistema completamente autónomo no processo de aprovisionamento de utilizadores, com a faculdade de reconciliar e corrigir as diferenças caso sejam encontradas discrepâncias;
- Define o controlo de acessos baseado em funções de negócio e os utilizadores têm unicamente uma identidade digital e uma palavra-passe, com a particularidade de oferecer um mecanismo para a recuperação da mesma, sem intervenção de terceiros.

2.3.3 Plataforma de gestão de identidades

Existe um produto Oracle que é dedicado exclusivamente para a gestão de identidades (Oracle Identity Manager). Este distingue-se no mercado por oferecer um sistema altamente flexível e escalável que controla de forma centralizada o ciclo de vida das identidades e os privilégios de acesso nas organizações [IdM08].

Apesar de apresentar os mecanismos basilares no domínio de competências fundamentais das plataformas IdM, evidencia as mesmas dificuldades de integração e carece de um modelo lógico ou um facilitador que permita, com pouco esforço, providenciar a automatização do processo de gestão de identidades para os produtos *Oracle Retail*. A razão deste facto deve-se às diferentes necessidades das aplicações de retalho e ainda não existir, por parte da Oracle, uma plataforma central para o aprovisionamento de utilizadores [ORSP14].

A oferta em soluções de segurança para a computação na nuvem são uma resposta estratégica da Oracle para superar as limitações existentes e reduzir os custos de implementação de uma solução IdM. O *Oracle Identity Cloud Service* (IDCS) representa a nova plataforma de IDaaS (Identity as a Service) fundamentada em padrões abertos, com a finalidade de ultrapassar os desafios referidos, oferecendo um serviço inovador para suportar as necessidades de negócio e totalmente integrado com os processos de gestão de identidades. O (IDCS) baseia-se na arquitetura microservice[4] seguindo os princípios da computação na nuvem tais como: facilidade de instalação de funcionalidades, escalabilidade, flexibilidade e resiliência [GOA16]. No momento atual, esta abordagem torna-se inexequível uma vez que as versões *Oracle Retail*, mesmo as mais recentes (v16), não são certificadas com este serviço.

[4] Desenvolvimento de um aplicativo único como um conjunto de pequenos serviços. Esta arquitetura apresenta-se como o oposto do padrão arquitetural monolítico.

As soluções IBM também devem ser consideradas nesta área, mesmo com as limitações sobre os produtos (Oracle) é a solução atual do retalhista que garante o cumprimento das políticas de segurança e das normas da organização. Para além disso, a plataforma está integrada com os restantes sistemas e serviços para controlar e gerir acessos de forma centralizada e destaca-se pela funcionalidade (True RBAC) que suporta o aprovisionamento automático dos utilizadores, após a entrada no Sistema de Gestão de Recursos Humanos, sem a intervenção do administrador de sistemas [IBMAP]. Por estes motivos e por reutilizar componentes da arquitetura existente, representa a melhor abordagem ao problema.

Existem, no entanto, outros modelos de crescimento no mercado, como por exemplo nas aplicações da empresa Microsoft. Esta empresa tecnológica tem como política o desenvolvimento interno das suas aplicações tendo como preocupação fulcral a completa integração das mesmas, nomeadamente ao nível de gestão das identidades e acessos.

2.3.4 Restrições tecnológicas

A solução (Figura 13) representa o cenário típico de autenticação unificada para as aplicações *Oracle Retail* implementadas. O utilizador é autenticado pelo servidor de autenticação (OracleAS SSO) após receber um pedido do módulo (mod_osso), no qual valida as credenciais de acesso no serviço de diretórios LDAP (OID), permitindo dessa forma o utilizador aceder aos vários aplicativos corporativos com a mesma identidade digital e palavra-passe. De mencionar que as aplicações são apenas certificadas pelo componente proprietário (OSSO) e tal constatação pode limitar a utilização de protocolos de federação tais como o SAML.

No entanto, o objetivo do presente estudo passa por explorar a integração entre o servidor de autenticação (OracleAS SSO) e o servidor *Tivoli Access Manager* (TAM), que faz parte da solução de controlo de acessos da organização. O retalhista reconhece as dificuldades em cumprir este requisito. Trata-se de um problema complexo *"makes it very difficult, perhaps impossible, to integrate TIM/TAM"* pois ambas as empresas de tecnologia não oferecem informação detalhada sobre os procedimentos a seguir para integrar a solução, representando uma adversidade que causa preocupação no projeto.

Uma nova abordagem ao problema foi estudada. Pela interpretação ilustrada (Figura 14) pode ser possível estabelecer uma relação de confiança entre sistemas e delegar a autenticação a terceiros. Segundo o diagrama (Figura 14), com a instalação de um agente (Third-Party Agent) no servidor de autenticação (OracleAS SSO) e a sincronização entre os repositórios, o processo de autenticação torna-se transparente para os utilizadores e as aplicações continuam a funcionar no domínio Oracle.

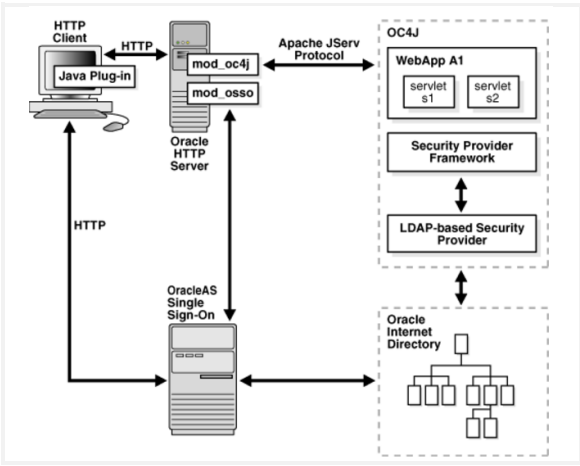


Figura 13 – Cenário típico
(Imagem de: Oracle. 2009. [OCSG], p. 32-3)

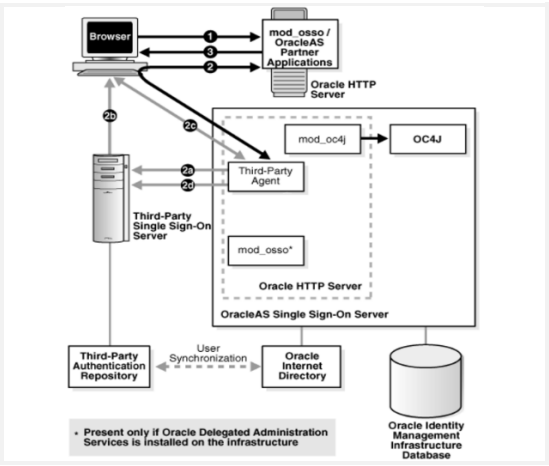


Figura 14 – Cenário possível
(Imagem de: Oracle. 2005.[OASSSO], p. 14-2)

2.3.5 Gestão de utilizadores no sistema Oracle Retail

Como anteriormente explicado, o sistema Oracle Retail não é construído com o foco na integração de processos relacionados com a gestão de utilizadores. A constatação deste facto é evidenciada pela própria Oracle, por não fornecer uma plataforma global para tratar o problema devido às diferentes necessidades das aplicações dos vários domínios [ORSP14].

As aplicações do sistema de retalho apresentam modelos de segurança que divergem entre si quanto ao nível da autenticação ou autorização. Cada aplicação tem especificações próprias de segurança e requisitos de aprovisionamento que podem compreender diferentes sintaxes e variadas tecnologias, dificultando a gestão de utilizadores em qualquer ambiente.

Todo o processo de gestão e aprovisionamento é classificado como complexo. No processo de criação de utilizadores os procedimentos são explícitos, mas implicam várias interações, quer no serviço de diretórios ou nas diferentes bases de dados, o que se traduz num processo demorado e suscetível a falhas. Quando se pretende eliminar uma identidade não existe informação de como proceder, havendo casos em que os procedimentos partilhados são incompletos e inconsistentes.

Um outro pormenor a ter em consideração pelo grau de complexidade são os passos de criação do RAD (Resource Access Descriptor) para as aplicações (Oracle Forms) que participam no processo de autenticação única. Para cada utilizador criado deve ser associado um registo no serviço de diretórios com a informação (Oracle System ID, Database User Name, Password), a fim de estabelecer uma ligação com a base dados (RMS) e autenticar-se na aplicação. Segundo a documentação, são necessárias três interações [ORS11g] completamente manuais.

O projeto de investigação e desenvolvimento [ORUP15] procurou resolver este problema. Os modelos de dados relacionais (consultar Anexo III) e especificidades das aplicações *Oracle Retail* foram estudadas minuciosamente, de forma a ser possível a aplicação de novos conceitos satisfazendo elementos chave para o negócio, sem causar problemas de integridade para o sistema. O projeto consistiu no desenvolvimento de um algoritmo "inteligente" que visa responder às necessidades levantadas no domínio da gestão de identidades, por forma a criar, reconciliar, atualizar e eliminar um ou mais utilizadores para cada aplicação de forma automática.

Na (Tabela 4) apresenta-se um breve resumo da investigação realizada.

Tabela 4 – Oracle Retail User Provisioning

Domínio	**Produto**	**Tecnologia**	**SSO**	**Aprovisionamento**
Merchandising	Oracle Retail Merchandising System	Oracle Forms	Suporta a tecnologia (OSSO)	Suporta as operações CRUD [5], exceto eliminar registos do utilizador das tabelas de autorização no caso de existirem transações associadas ao mesmo
	Oracle Retail Price Management	WebStart Fat Client	Suporta a tecnologia (OSSO)	Suporta as operações CRUD, exceto eliminar o registo do utilizador da tabela de autorização. A opção é atualizar o registo na tabela com uma data de fim
	Oracle Retail Invoice Matching	Java Web Application	Suporta a tecnologia (OSSO)	Suporta as operações CRUD, exceto eliminar os registos do utilizador das tabelas de autorização. A opção é eliminar o registo que faz a associação entre o utilizador e a função de negócio
	Oracle Retail Sales Audit	Oracle Forms	Suporta a tecnologia (OSSO)	Suporta as operações CRUD, exceto eliminar registos do utilizador das tabelas de autorização no caso de existirem transações associadas ao mesmo
Planning	Oracle Retail Allocation	Java Web Application	Suporta a tecnologia (OSSO)	Suporta as operações CRUD, exceto eliminar o registo do utilizador da tabela de autenticação mas podem ser eliminados os departamentos da tabela de autorização

[5] CRUD (acrónimo de create, read, update e delete)

Domínio	Produto	Tecnologia	SSO	Aprovisionamento
Business Intelligence	Oracle Retail Analytics	Oracle BIEE	Suporta a tecnologia (OSSO)	Suporta as operações CRUD
Supply Chain Planning & Execution	Oracle Retail Warehouse Management System	Oracle Forms	Não suporta SSO	Suporta as operações CRUD
Infrastructure	Oracle Retail Workspace	Java Web Application	Suporta a tecnologia (OSSO)	Suporta as operações CRUD
Store	Oracle Retail Store Inventory Management	WebStart Fat Client	Suporta a tecnologia (OSSO)	Suporta as operações CRUD

2.4 Análise de valor

Seguindo as diretrizes estratégicas do retalhista, a informação é classificada como um ativo valioso, um recurso tão importante quanto as pessoas e o capital. Esta importância permite identificar novas oportunidades de mercado, potenciar vantagens competitivas através de processos de tomada de decisão e, inclusive, eliminar hipotéticas ameaças dos concorrentes.

O valor da informação considera-se imprescindível para o sucesso dos negócios e esta dependência tem as suas desvantagens, tornando a organização potencialmente vulnerável aos riscos de segurança da informação. Nesse sentido, proteger os ativos da informação contra acessos não autorizados por intermédio de soluções de gestão de identidades e acessos (IAM) é uma condição indispensável.

Esta proposta de valor pretende oferecer um modelo integrado de processos, no domínio do controlo de acessos e gestão de utilizadores, em conformidade com as políticas de segurança da informação do retalhista. Contempla um conjunto significativo de benefícios intangíveis para a organização, tais como: automatizar o aprovisionamento de utilizadores, reduzir custos, simplificar atividades administrativas, minimizar desafios operacionais e aumentar a flexibilidade nos negócios.

A presente proposta pode ser ampliada a novos valores, como seja o aumento da produtividade resultante de uma melhor experiência do utilizador no sistema, pelo facto de usarem as mesmas credenciais de acesso e inequivocamente, podendo contribuir como novo conhecimento tecnológico para futuras implementações em retalhistas.

2.4.1 Modelo NCD *(new concept development model)*

O desenvolvimento de produtos com características inovadoras podem promover o sucesso das empresas. Um fator decisivo para a concepção de novos produtos fundamenta-se na escolha de modelos que oferecem uma visão estruturada de atividades, e neste contexto destaca-se o de modelo de Koen (NCD). Na fase inicial do processo de inovação (Fuzzy front end) sustentado no modelo de Peter Koen são identificadas cinco etapas distintas no desenvolvimento do produto:

Identificação da oportunidade

A oportunidade foi identificada devido a uma necessidade de um cliente na área de negócio de retalho. Numa fase posterior, na oferta de novos serviços e na participação de projetos, novos recursos em conjunto com os centros de competência identificaram a oportunidade de explorar o domínio de gestão de utilizadores, com o intuito de reduzir consideravelmente o esforço no aprovisionamento. A análise de tendências de comportamento dos clientes e uma pesquisa de soluções no mercado, que permita resolver o problema do provisionamento de utilizadores, são métodos refletidos no estudo.

Análise da oportunidade

Requer uma avaliação para determinar a viabilidade da oportunidade. Na presença de informações adicionais por parte do departamento de pré-vendas, confirma-se a realização de um investimento por parte do cliente para satisfazer a sua própria necessidade. Por consequência, reduz incertezas e transforma esta oportunidade em negócio. Internamente permite novo conhecimento tecnológico e a extensão do portfólio de produtos ou serviços com valor acrescentado.

Geração da ideia e enriquecimento

As diferentes opiniões neste processo descrevem o quanto as ideias são evolutivas e em constante reformulação. Inicialmente, promoveu-se discussões internas de caracter criativo, com a partilha de conhecimento e experiências entre vários elementos técnicos e funcionais da organização, no âmbito de racionalizar estratégias objetivas e explorar o conceito. Entre o cliente e parceiros, a metodologia *Conference Room Pilot* (CRP) possibilita uma série de sessões organizadas com as pessoas mais relevantes de diferentes áreas de negócio para alinharem ideias, proporcionado um exercício orientado ao domínio do problema.

No decorrer de várias reuniões, o conflito de interesses entre arquitetos de solução e de segurança dificultou o sucesso de ideias concretas. Persistia o objetivo da reutilização dos adaptadores desenvolvidos no âmbito da solução OR-IdM-US, anteriormente descrita, e a utilização de procedimentos não certificados com o sistema de retalho.

Seleção de ideias

Num consenso geral, mesmo com contradições e momentos flutuantes as ideias selecionadas decidiram o sucesso do produto. Alguns exemplos citados:

- Reconciliação – o processo interpreta as informações sobre a autorização dos utilizadores no destino, corrigindo automaticamente em caso de diferenças;
- Gestão de utilizadores – o aprovisionamento de utilizadores deve gerido sem intervenção de terceiros;
- Eliminação de utilizadores – a identidade do utilizador deve ser removida sem criar impactos no sistema e garantir o rastreio de toda a informação produzida pelo mesmo;
- Autorização ao Portal – os utilizadores devem ter permissões de acesso a um portal único (ORW) de forma a acederem aos aplicativos autorizados;
- Exclusão da reutilização de adaptadores – a lógica de aprovisionamento evidencia procedimentos incoerentes e os adaptadores são dominados por múltiplas tecnologias, não facilitando a gestão do produto. Considera-se como limitada.

A seleção e formalização das ideias teve como critérios: princípios de segurança, limitações tecnológicas e retorno de valor para o negócio.

Conceito

A etapa de desenvolvimento do novo produto depende do sucesso e aprovação do conceito. O consentimento é generalizado, a elaboração de um plano de negócios por parte do cliente estima potencial interno, torna-o dependente desta necessidade fundamental. Apesar disso, há alguma apreensão relativamente ao fato de terem existido experiências menos conseguidas no passado.

Numa demonstração de iniciativa e pro-atividade interna, procedeu-se a uma investigação e concepção teórica do ciclo de vida do utilizador no sistema de retalho, baseado no estudo dos seguintes tópicos:

- Modelo de dados de cada módulo;
- Procedimentos certificados pela entidade Oracle;
- Eliminação de utilizadores de negócio e identificação de impactos;
- Criação de utilizadores sem auxílio de interfaces disponíveis em cada aplicação de retalho.

Depois da análise procedeu-se à avaliação das tecnologias envolvidas, sendo finalizado com o desenvolvimento de um produto [ORUP15] no domínio de gestão de utilizadores, totalmente adaptado à realidade das necessidades de negócio do retalhista, transmitindo assim mais confiança sobre a integração da solução neste domínio.

2.4.2 Conceito de valor, valor percebido, valor para o cliente, benefícios e sacrifícios

O conceito de valor pode representar um grau de subjetividade e complexidade de acordo com o contexto e ambiente. De uma forma percetível, o valor é estabelecido com a satisfação de necessidades, através da aquisição de um produto ou serviço, que convergem com atributos tangíveis e intangíveis, proporcionando experiências aos consumidores e vantagens competitivas às empresas nas suas atividades e operações.

Na definição do valor percebido, os conceitos tendem a divergir, tanto pode refletir sobre a avaliação de um produto sobre a sua utilidade, ou o valor concebido pelo mercado referente a um serviço, na relação entre benefícios e sacrifícios.

O conceito de valor para o cliente descreve como as empresas oferecem valor acrescentado sob a perspetiva de aumento de benefícios e redução de sacrifícios. Compete às empresas encontrar formas de estabelecer as suas diferenças, a partir do valor que agregam à oferta dos seus produtos ou serviços, não só conquistar clientes, mas principalmente conseguir a sua lealdade ao longo do tempo.

De acordo com o problema identificado, o valor percebido pode ser visualizado na (Tabela 5), em que os sacrifícios para o cliente, estão associados ao custo, tempo e energia. Os benefícios estão relacionados com questões do foro operacional, estratégico e de segurança:

- Operacional – reduzir o esforço e tempo despendido na gestão e criação de utilizadores para o negócio;
- Estratégico – investir em novas geografias e expandir as suas operações utilizando instâncias da mesma plataforma;
- Segurança – garantir os princípios da segurança da informação em conformidade com as normas e políticas instituídas.

Tabela 5 – Valor percebido

	Produto	Serviço	Relação com o cliente
Benefícios	• Gestão do ciclo de vida dos utilizadores • Redução de riscos • Ponto de acesso único de autenticação • Garantia do acordo de nível de serviço	• Satisfação • Produtividade • Segurança • Conformidade	• Confiança • Fidelização • Credibilidade
Sacrifícios	• Custo • Tempo • Inovador	• Custo • Tempo	• Tempo • Esforço • Energia

2.4.3 Proposta de valor

Esta proposta de valor pretende oferecer um modelo integrado de processos, no domínio do controlo de acessos e gestão de utilizadores sobre o sistema Oracle Retail, conforme as políticas de segurança da informação do retalhista.

2.4.4 Modelo de negócio de Canvas

A (Figura 15) ilustra o Modelo de negócio de Canvas na forma como geramos valor para o cliente através da entrega de um produto e serviço. Este modelo está divido em quatro áreas e deve responder a quatro perguntas fundamentais:

- Quem é o cliente? – Destina-se a retalhistas. Serve todos os colaboradores que interagem com o sistema de retalho e que acedem à informação crítica de negócio. Pode ser expandido para outras áreas de negócio (p. ex. instituições financeiras bancárias).

- Qual é o problema? – Reside em garantir um sistema de autenticação unificado, que permita fornecer mecanismos que identifiquem automaticamente os direitos das identidades no sistema de retalho.

- Como se resolve? – Através da identificação de atividades-chave que suportem o modelo de negócio, por intermédio da cooperação entre parceiros e recursos na área da segurança e do retalho.

- Como se ganha dinheiro? – Pela redução de atores nas atividades de suporte e pela automatização do aprovisionamento dos utilizadores de negócio, sem estar dependente de outras entidades. Além destes benefícios, protegem os ativos da informação.

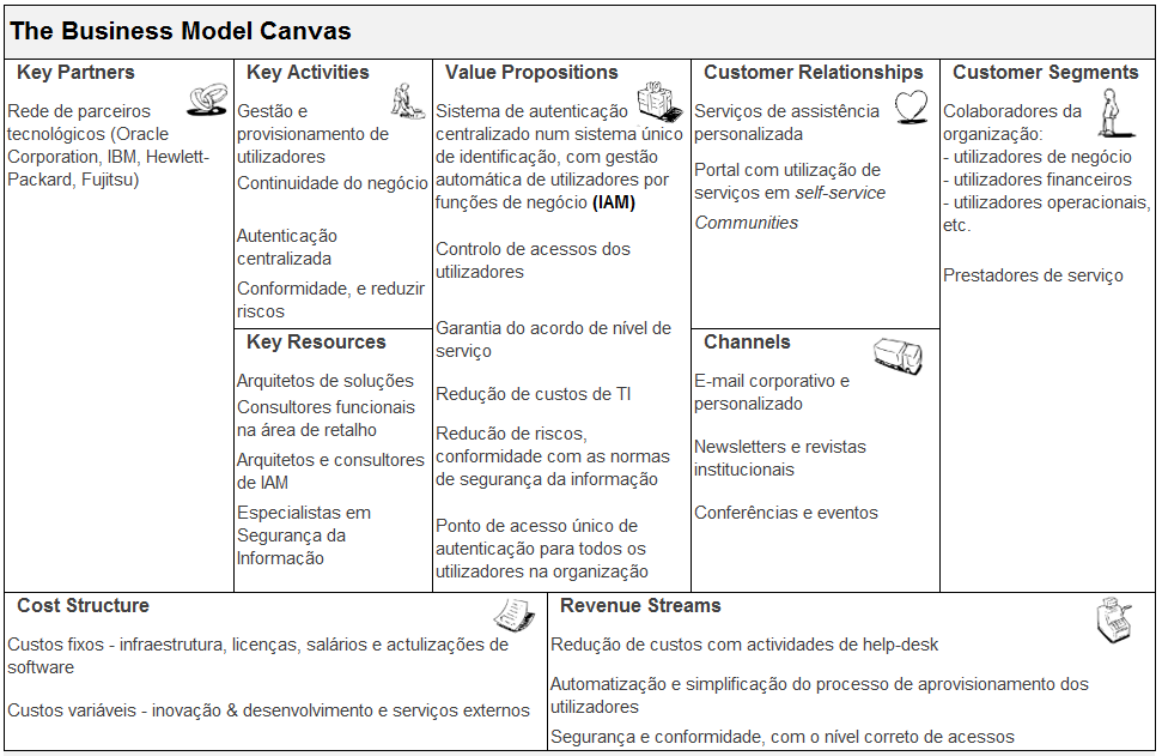


Figura 15 – Modelo de negócio de Canvas

2.4.5 Cadeia de valor IAM

Neste contexto podemos visualizar a cadeia de valor IAM (Figura 16). Este modelo foi desenvolvido a partir da cadeia de valor de Porter, surge com uma adaptação das atividades primárias e secundárias tradicionalmente apresentadas. As atividades primárias relacionam-se com os processos de um sistema de gestão de identidades e acessos, essenciais para a continuidade do negócio e segurança numa organização:

- Gestão de utilizadores – processo de gestão do ciclo de vida de uma identidade no sistema (criar, mudar, suspender, reativar, eliminar e reconciliar).
- Autenticação – processo de verificar a identidade de um utilizador no sistema.
- Autorização – processo que determina os acessos de um utilizador autenticado, e quais os direitos ou permissões que pode exercer no sistema.
- Auditoria – processo que documenta todas as atividades de um utilizador no sistema.

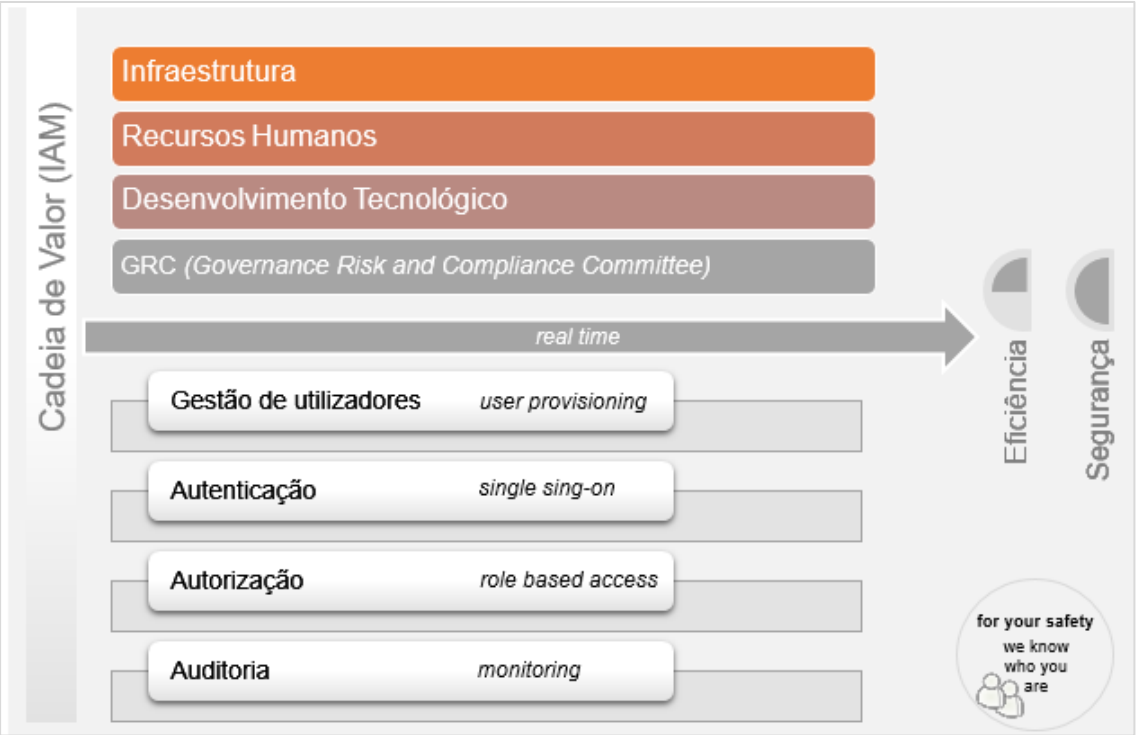


Figura 16 – Cadeia de valor IAM

As atividades de apoio suportam a tomada de decisão e execução das atividades primárias, com a finalidade de garantir eficiência e segurança em tempo real:

- Infraestrutura – gestão, planeamento e controlo dos sistemas de informação.
- Recursos Humanos – gestão de entrada e saídas de colaboradores sem intervenção de terceiros.
- Desenvolvimento Tecnológico – concepção de novos produtos e implementação de programas complexos.
- GRC – revisão contínua de normas e políticas de segurança corporativas, gestão de riscos da segurança da informação, proteção e classificação de dados.

3 Avaliação da Solução e Abordagens

3.1 Introdução

A escolha de abordagens depende em grande parte da incerteza tecnológica considerada no problema. Todas as abordagens que apresentam maior risco e que podem condicionar a funcionalidade ou operacionalidade dos produtos devem ser remetidas para um segundo plano. A reutilização de componentes da arquitetura existente e configurações não intrusivas para o sistema são definidas como abordagens primárias.

Em caso específicos, sobretudo pela falta de detalhes na documentação e das incertezas que subsistem no domínio do problema, após a identificação das abordagens, foi necessário proceder à realização de provas de conceito (PoC) sobre o sistema de autenticação e qual o seu comportamento quando funciona sobre o protocolo seguro (SSL/TLS) entre as aplicações de retalho, com o intuito de identificar potenciais riscos técnicos entre os vários componentes da solução.

Após formalização da prova de conceito, é necessário elaborar um plano de atividades que descreva as entidades envolvidas, recursos e as operações a realizar no ambiente de desenvolvimento. No final, deve ser produzido um documento com os resultados obtidos, evidências e limitações existentes. No caso de aprovação, pode ser considerado para um possível desenho da solução.

Para os restantes casos, o método encontrado para comparar os conceitos e avaliar as melhores abordagens foi a *Pugh Matrix*.

3.2 Descrição da prova de conceito

A prova de conceito foi realizada no âmbito do Projeto Autorização de forma a aplicar um agente no servidor (OracleAS SSO), delegando o processo de autenticação a terceiros, com o objetivo de providenciar a funcionalidade *Single Sign-on* (SSO) sobre o protocolo seguro (SSL/TLS) para os utilizadores de negócio do retalhista.

Esta prova de conceito pode representar a base para a concepção final da solução de autenticação.

A metodologia utilizada para a execução da prova de conceito é uma adaptação da metodologia de integração de soluções que consiste em cinco fases:

- Definir a equipa e responsabilidades;
- Identificar requisitos;
- Desenhar solução;
- Construir;
- Avaliar através de testes funcionais.

3.2.1 Problema

O retalhista implementou uma solução *Oracle Retail* constituída por múltiplos módulos e funcionalidades específicas para cada área de negócio e durante o processo de implementação verificou-se a impossibilidade de integrar a nova solução de retalho com o sistema de gestão de identidades e acessos do retalhista.

A solução atualmente em produção apresenta um sistema de autenticação sustentado por múltiplos pontos de acesso que utiliza protocolos não seguros (e.g. HTTP) para a comunicação entre as aplicações. Para além de não garantir um sistema de autenticação centralizado, em que os utilizadores podem ter diferentes credenciais, compromete as políticas de segurança do domínio que asseguram a integridade do acesso ao sistema.

3.2.2 Objetivos

O objetivo consiste em providenciar as melhores práticas de segurança com um mecanismo de autenticação centralizado, garantindo dessa forma um sistema de acesso único de identidades.

A solução deve ser capaz de cumprir os seguintes objetivos:

- Providenciar uma administração de políticas de segurança centralizada;
- Conceber uma plataforma de gestão de identidades e acessos global;
- Resolver as vulnerabilidades de comunicação entre sistemas;

- Garantir um sistema de autenticação unificado, permitindo a todos os utilizadores acederem a múltiplos aplicativos com as mesmas credenciais.

3.2.3 Identificação de requisitos

Esta fase refere-se ao levantamento de requisitos (Tabela 6) que a solução deve satisfazer, estes consideram-se fundamentais para garantir a segurança no domínio do controlo de acessos e a operacionalização dos processos pretendidos.

Tabela 6 – Listagem de requisitos (PoC)

Requisito	**Descrição**
Aplicações de retalho c/SSO	Solução de autenticação unificada para as seguintes aplicações: • Oracle Retail Merchandising System • Oracle Retail Sales Audit • Oracle Retail Invoice Matching • Oracle Retail Allocation • Oracle Retail Price Management • Oracle Retail Workspace • Oracle BI Publisher
SSL Offloading no balanceador de carga	As comunicações efetuadas no sistema de retalho utilizam o protocolo HTTPS com a aplicação do conceito de SSL Offloading
Delegação da autenticação	O Oracle Single Sign-On (OSSO) delega autenticação a terceiros (TAM)
Sincronização de utilizadores de negócio	Os utilizadores de negócio têm de ser sincronizados entre o serviço de diretórios LDAP da Oracle e serviço de diretórios LDAP da IBM
Cabeçalho para autenticação $^{iv\_user}$	O agente (Third-Party Agent) tem de ser implementado no servidor (OSSO). Este consiste em passar os campos específicos do cabeçalho para autenticação $^{IV\_USER}$ que contém a identidade do utilizador

Quando à sua representação e organização, podem ser visualizados no diagrama de caso de utilização (Figura 17), o qual fornece uma visão geral das aplicações envolvidas, sendo ainda possível verificar o fluxo das ações dos intervenientes e a interação entre eles.

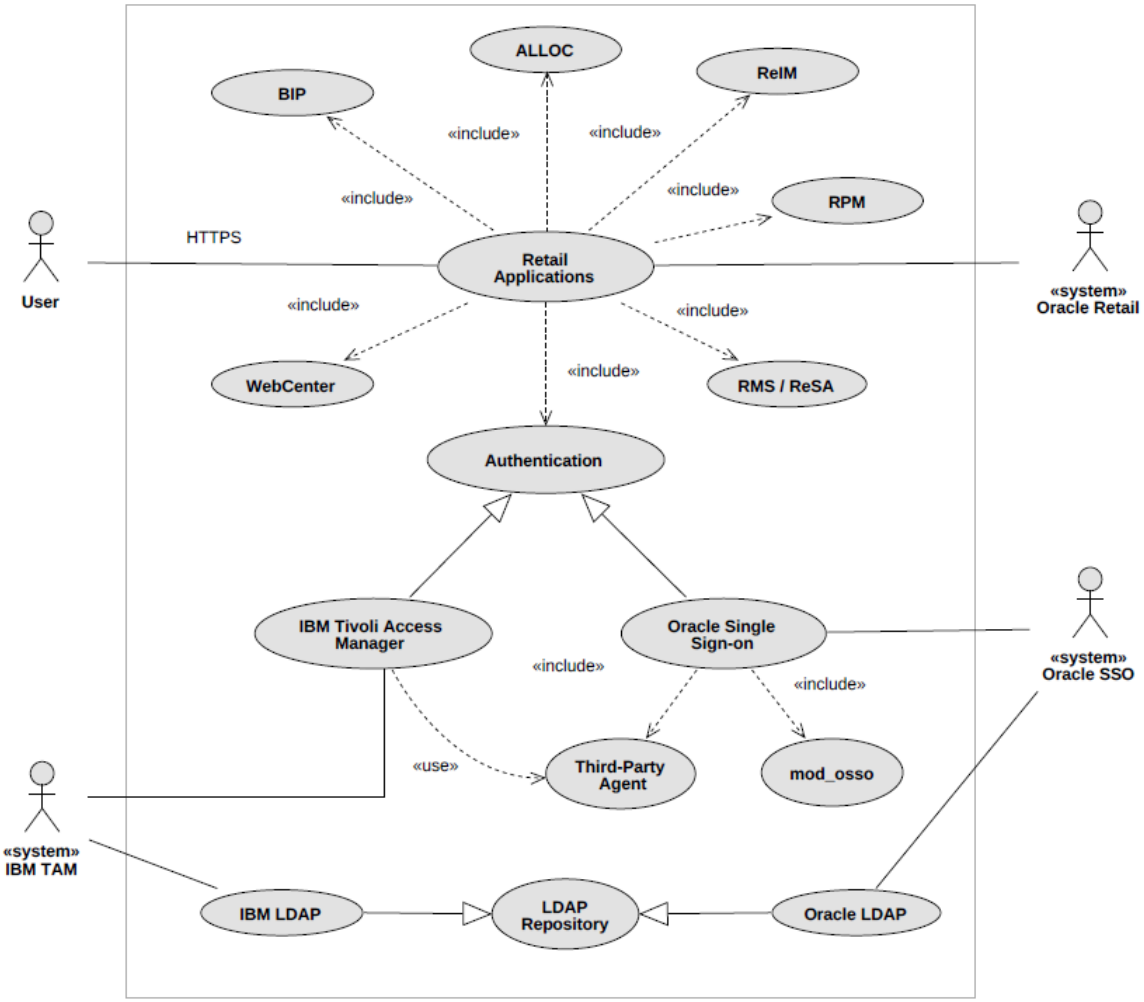


Figura 17 – Requisitos identificados

- As aplicações do sistema de retalho (RMS/ReSA, RPM, ReIM, ALLOC, BIP, WebCenter) deverão ser integradas com o sistema de autenticação centralizada;
- No acesso ao sistema de retalho deverá ser implementado o protocolo HTTPS;
- O sistema (Oracle SSO) deverá fornecer um agente (Third-Party Agent) e delegar a autenticação ao sistema (IBM TAM);
- O serviço de diretórios deverá ser único durante o processo de autenticação.

3.2.4 Visão da solução

A arquitetura da prova de conceito foi definida de acordo com os requisitos identificados, apresentando a solução proposta para o problema, baseada na utilização de componentes existentes e numa adaptação contínua, consoante as necessidades.

A figura seguinte (Figura 18) descreve um diagrama de componentes que exemplifica o processo de integração entre os sistemas de autenticação.

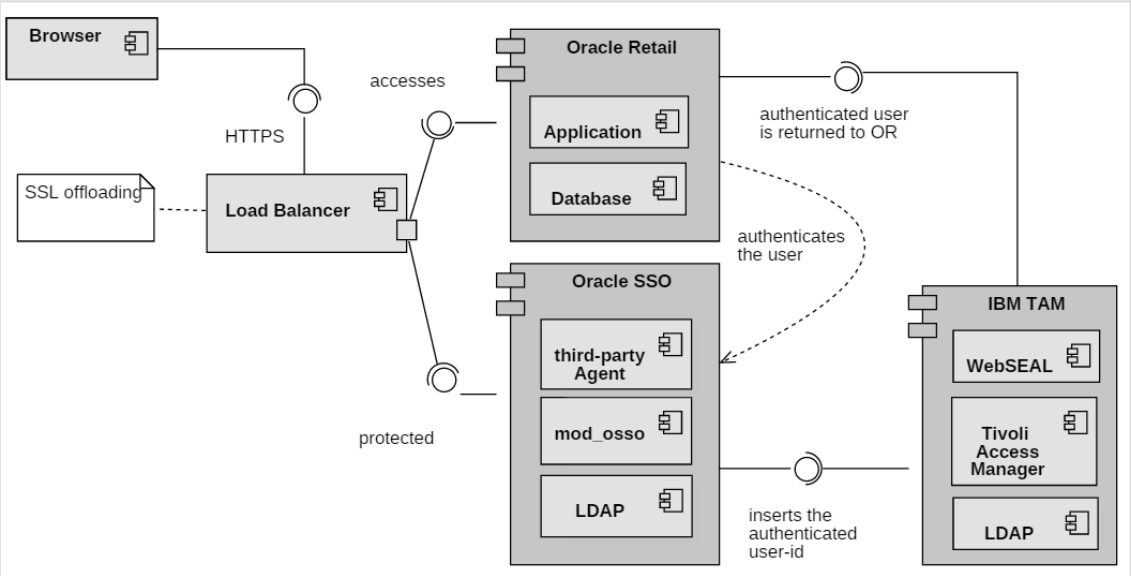


Figura 18 – Diagrama de componentes (PoC)

As comunicações realizadas no sistema utilizam o protocolo HTTPS, assegurando que a transmissão de toda a informação é protegida por recursos criptográficos, para garantir a integridade e confidencialidade dos dados. O balanceador de carga oferece um mecanismo (Offloading) que trata estes pedidos e constitui-se responsável pelo processo de encriptação SSL/TLS e pela gestão dos certificados digitais. Assim sendo, retira dos servidores aplicacionais todo este processamento de comunicação encriptada, melhorando o desempenho durante o processo de autenticação.

As aplicações de retalho são apenas certificadas para funcionar com o componente *Oracle SSO* e essa configuração deve ser assegurada e testada individualmente em cada aplicação. Estes requisitos técnicos são fundamentais para garantir o sucesso da próxima etapa, no âmbito de estabelecer uma relação de confiança entre os sistemas e delegar a autenticação para o *Tivoli Access Manager* (TAM).

O agente (Third-Party Agent) torna-se o componente responsável por interpretar o cabeçalho HTTP de autenticação com variável (iv-user) e extrair somente a identidade do utilizador do através do servidor *proxy WebSEAL*.

A sincronização dos utilizadores entre os repositórios LDAP surge como ação obrigatória, o mapeamento deve ter em consideração a identidade do utilizador, constituindo um sistema único de identificação, em que o processo de autenticação se torna transparente para os utilizadores de negócio e as aplicações de retalho continuam a funcionar no domínio Oracle.

3.2.5 Conclusões

A prova de conceito avaliou a integração da solução de autenticação do sistema de retalho com aplicação do conceito de *SSL Offloading*.

Durante os testes unitários foram encontradas algumas adversidades ao longo da construção da solução, mas prontamente resolvidas pelas equipas responsáveis. Provavelmente um dos erros que merece maior atenção relaciona-se com o comportamento do navegador Web (Internet Explorer), que depois da integração com *Tivoli Access Manager* (TAM), obriga o utilizador a facultar as credenciais de acesso, por duas vezes, durante o processo de autenticação. Para contornar este problema, a abordagem foi utilizar um nome de domínio com mais de duas letras[6] e registar novamente as aplicações com o novo endereço.

Depois da conclusão dos testes unitários surgem os testes de integração.

A equipa de testes, em conjunto com alguns elementos do negócio, avaliou a solução e encontrou erros que devem ser corrigidos, mas sem impacto para o retalhista. Estes erros são em grande parte relacionados com o acesso aos menus de ajuda das aplicações, após a implementação do protocolo HTTPS. No entanto estas pequenas alterações podem ser intrusivas e, por esse motivo, deve ser estudado o melhor método a aplicar sem reinstalar as aplicações e disponibilizar os menus de ajuda, caso se necessitem.

Os resultados obtidos da prova de conceito revelam-se positivos, pois cumprem todos os requisitos previamente identificados e, de acordo com os critérios de avaliação, não foram encontrados erros críticos nem graves que impactassem o funcionamento do sistema.

Para além disso, foram reportados problemas de desempenho quando tentavam aceder ao Portal, contudo as evidências partilhadas eram aleatórias e poucos utilizadores conseguiam reproduzir esse mesmo comportamento. Para o efeito deste estudo e desta tese, procedeu-se à recolha de amostras (Tabela 7) para testar uma hipótese, com o objetivo de compreender através de factos se existem diferenças ao nível de desempenho durante o processo de autenticação no Portal.

Tabela 7 – Amostras (resultados da experiência são expressos em segundos)

Ambiente PoC (SSO IBM c/HTTPS)	**Ambiente UAT** (SSO Oracle c/HTTP)	**Ambiente PRD** (SSO Oracle c/HTTP)
1.37	1.31	1.24
1.28	1.64	1.17
1.81	1.28	1.37
1.32	1.52	1.39
1.57	1.29	1.41
1.31	1.43	1.17
1.75	1.67	1.2

[6] Https://support.microsoft.com/en-ie/help/310676/internet-explorer-does-not-set-a-cookie-for-two-letter-domains

I. Hipótese a ser testada

Tempo de resposta de acesso ao Portal (ORW) durante o processo de autenticação em três ambientes distintos: PoC, UAT e PRD.

II. Definição das hipóteses

H_0 – as médias são iguais
H_1 – pelo menos uma das médias é diferente

III. Especificação do nível de significância

Nível de significância – 5%
Nível de confiança – 95%

IV. Método estatístico

Método ANOVA (one-way) devido à presença de amostras com distribuições normais de igual variância e independentes.

V. Tipo de erros

Tipo 1 – Aceitar a hipótese quando ($p > 0,05$)
Tipo 2 – Rejeitar a hipótese quando ($p < 0,05$)

VI. Resultado

Como a significância do resultado obtido (0,0791) é maior que o nível de significância do teste (0,05), não é possível rejeitar a hipótese nula (Figura 19). O tempo médio de resposta não é significativamente diferente entre os ambientes no acesso ao Portal (ORW), mesmo com a implementação do protocolo HTTPS no ambiente (PoC). No entanto, se o resultado for significativo com ($p <0,05$), poderá ser possível recorrer a um teste post-hoc (tukey).

Summary

Groups	n	df	df	Sum	Mean	Variance	SSW
Ambiente PoC	7	6	18	10,41	1,49	0,05	0,53
Ambiente UAT	7	6		10,14	1,45	0,03	
Ambiente PRD	7	6		8,95	1,28	0,01	

Variance Analysis

Source	SS	% SS	df	VAR	F	P Value	F Critical
Between Groups (SSB)	0,1724	24,57%	2	0,0862	2,9315	0,0791	3,5546
Within Groups (SSW)	0,5293	75,43%	18	0,0294			
Total (SST)	0,7017		20				

Hypothesis Testing

Null Hypothesis	p-value		Error
H0: sW - sB = 0	0,1581	Failed to Reject	0,0500
H0: sW - sB >= 0	0,9209	Failed to Reject	
H0: sW - sB <= 0	0,0791	Failed to Reject	

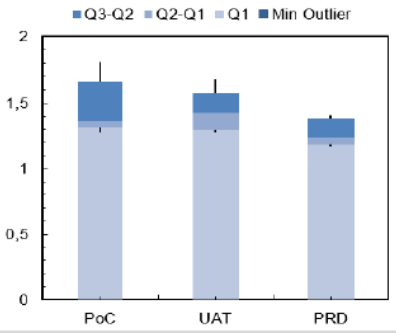


Figura 19 – Resultado com o Método Anova

A contribuição desta experiência evidencia, perante os resultados atingidos, a inexistência de qualquer problema de desempenho no ambiente onde ocorreu a prova de conceito. Apesar de esta hipótese ser testada em ambientes com diferentes características, o incidente reportado por alguns utilizadores relaciona-se com fatores externos ao caso.

3.3 Avaliação de abordagens existentes

A metodologia utilizada de modo a comparar e avaliar as abordagens identificadas é a *Pugh Matrix* [LSRHM09], também conhecida por matriz de análise ou matriz de decisão, desenvolvida por Stuart Pugh.

A *Pugh Matrix* procura identificar o conceito que melhor satisfaz os requisitos do cliente, através de uma análise de pontos fortes e fracos sobre as abordagens para o problema [LSRHM09].

O primeiro passo consiste em identificar um conjunto de critérios (Tabela 8) e quantificar cada um deles. Os critérios estão associados a um conjunto de medidas de avaliação, denominadas de grandezas (Tabela 8), de forma a reforçar a análise. A importância da sua identificação foi fundamental para avaliar a incerteza das diversas abordagens que foram usadas e discutidas durante o projeto. O critério risco e as restrições tenológicas apresentam maior peso, no primeiro caso pode-se afirmar que as grandezas são diretamente proporcionais, quanto mais tempo demorar a implementação, maior será o custo para o negócio.

Tabela 8 – Grandezas

Critérios	**Peso**	**Grandezas**
Risco	5	Tempo/custo
Restrições tecnológicas	5	Custo
Limitação dos produtos	4	Energia/esforço
Informação disponível	2	Quantidade
Produtividade	3	Tempo

Descrição com maior detalhe das grandezas a utilizar associadas aos critérios:

- Critério risco – tempo e custo de implementação para o negócio.
- Critério restrições tecnológicas – custo financeiro de mudança de tecnologia.
- Critério limitação dos produtos – energia e o esforço inerentes à customização dos produtos.
- Critério informação disponível – quantidade de informação detalhada no suporte ao problema.
- Critério produtividade – tempo despendido para executar uma ação/tarefa.

No segundo passo, com o suporte de um exemplo concreto (Tabela 8) será definida uma referência (**datum**) e procede-se à comparação entre as duas abordagens de criptografia de dados.

São apenas utilizados os sinais: mais (+), menos (-) ou igual (=).

Tabela 9 – Pugh Matrix (criptografia de dados)

		Abordagens	
Critérios	**Peso**	DBMS_CRYPTO (out-of-the-box)	HASH_FUNCTION (customized)
Risco	5	**D A T U M**	W
Restrições tecnológicas	5		W
Limitação dos produtos	4		W
Informação disponível	2		S
Produtividade	3		-
Resultado		0	**- 14**

Legend: B - Better, W - Worser, S - Same

O resultado (-14) advém do somatório dos três pontos negativos (w):

- Risco - 5
- Restrições tecnológicas - 5
- Limitação dos produtos - 4

Verifica-se então, que a primeira opção (DBMS_CRYPTO) pode ser considerada a abordagem mais adequada, apresentado menos risco para a solução. Este componente encontra-se por omissão presente nas bases de dados, contudo desativado. Ao contrário do que acontece com a opção alternativa (HASH_FUNCTION), que precisa de ser desenvolvida de raiz para responder às necessidades presentes.

Todas as abordagens identificadas devem ser avaliadas segundo os critérios previamente definidos, de modo a apoiar na tomada de decisão adequada ao problema. Como se está perante um sistema complexo e em produção, o objetivo deste exercício também serve para avaliar os impactos para o negócio.

4 Design da Solução

4.1 Introdução

Na fase de desenho pretende-se descrever os componentes lógicos da solução e o sistema proposto, de acordo com a identificação de requisitos e o estudo das abordagens para o problema, seguindo a metodologia de integração de soluções.

A nível conceptual, procura-se identificar a especificação de relações entre o sistema de retalho e os componentes do sistema de gestão de identidades e acessos, que são consideradas as entidades mais relevantes para o problema (Figura 20).

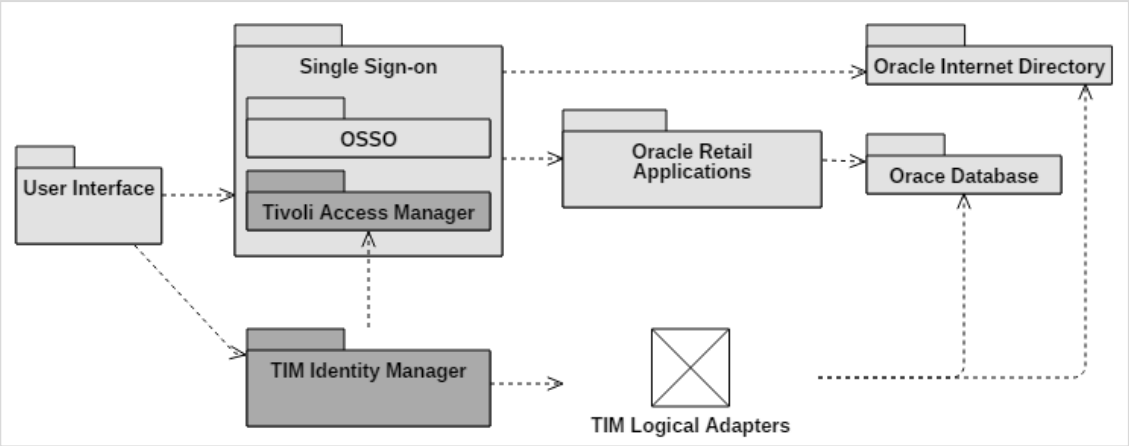


Figura 20 – Entidades do sistema

O sistema de retalho mantém a mesma infraestrutura tecnológica e características estruturais que asseguram a gestão operacional, minimizando potenciais riscos que possam afetar a continuidade do negócio e precavendo-se de avaliar novamente a solução por intermédio de testes de regressão.

O *Oracle Single Sign-On* (OSSO) reflete-se no único componente incluído no desenho, sujeito a uma modificação que influência o comportamento do sistema. A alteração consiste em estabelecer uma relação de confiança entre dois componentes (i.e. OSSO, TAM) de forma a conseguir delegar a autenticação para o *Tivoli Access Manager* (TAM). Este comportamento permite a introdução do novo processo de autenticação, sendo completamente transparente para os utilizadores finais, que poderão utilizar as mesmas credenciais de identificação no acesso às aplicações de retalho ou um outro serviço disponível no domínio.

A necessidade de uma infraestrutura adequada para suportar o acesso dos utilizadores usando políticas de aprovisionamento usa o componente TIM (Tivoli Identity Manager). Uma particularidade que o distingue é a utilização de uma metodologia modular e as características correspondentes a toda uma camada lógica de negócio. Os adaptadores são responsáveis por conter a lógica de integração, incluem o acesso a dados com módulos destinados à comunicação com cada tipo de base de dados, permitindo a gestão do ciclo de vida dos utilizadores nos ambientes de retalho.

4.2 Design arquitetural do sistema de gestão de identidades

O diagrama seguinte (Figura 21), baseado na utilização de componentes existentes, ilustra a arquitetura definida para o sistema de gestão de identidades, a qual permite uma interpretação abstrata. Representa apenas as características principais para possibilitar a distinção dos vários elementos por parte dos utilizadores, o que faz diminuir os níveis de complexidade e facilitar a compreensão do sistema a implementar [GERMO12]. A respeito da separação de conceitos (SoC), o sistema encontra-se organizado por módulos independentes, em que cada componente apresenta comportamentos singulares e um conjunto de responsabilidades não relacionadas.

Do ponto de vista do uso de padrões arquiteturais, apresenta-se como uma arquitetura típica multicamada (N-Tier), tratando-se de uma variante da arquitetura cliente/servidor, na qual o sistema é distribuído em camadas lógicas com funcionalidades específicas, visando responder às necessidades operacionais de cada unidade de negócio.

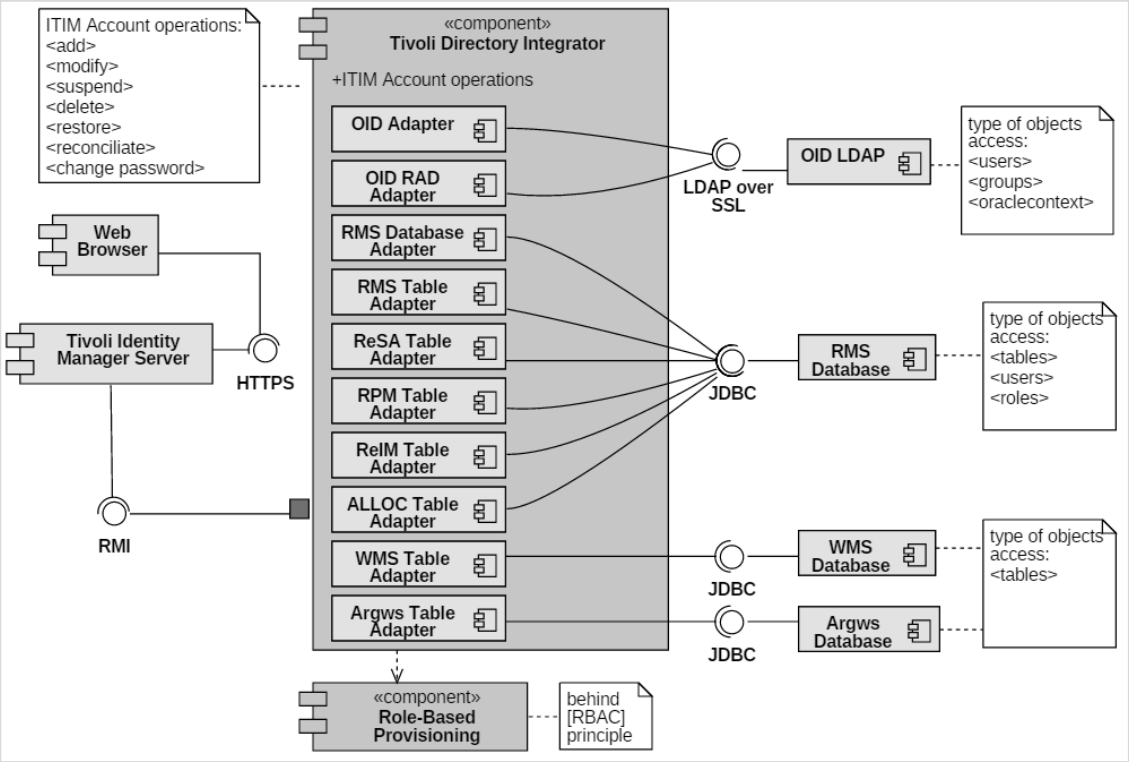


Figura 21 – Diagrama de componentes IdM

O sistema de gestão de identidades inclui as seguintes camadas:

- **Camada Cliente / Apresentação** – consiste na camada de interface com o administrador do sistema que, através do componente navegador Web, interage com o servidor aplicacional (TIM). O protocolo (HTTPS) assegura a comunicação segura entre os componentes. Por sua vez o TIM providência acesso a todas as funcionalidades disponibilizadas e proporciona a interação com o componente aprovisionamento de utilizadores.

- **Camada de Lógica de Negócio** – representa a camada lógica e desempenha uma função vital no processo de gestão do ciclo de vida das identidades nos ambientes de retalho. Nesta camada estão disponíveis os adaptadores funcionais, dez no total, com a lógica de integração que representam as funcionalidades mais importantes do sistema. Os adaptadores têm especificações próprias para cada aplicativo e quais as operações que podem efetuar. Essas regras [7] devem ser obedecidas de modo garantir o aprovisionamento dos utilizadores por funções de negócio.

- **Camada de Dados** – descreve os componentes físicos constituintes do sistema. Esta camada compreende um serviço de diretórios e três bases de dados relacionais. O acesso aos dados é realizado por meio de ligações JDBC e LDAPS e encontra-se protegida pela segunda camada, não sendo possível qualquer acesso direto.

4.3 Design detalhado do sistema de gestão de identidades

As atividades relacionadas com a fase de *design* detalhado iniciam-se depois da aprovação do *design* arquitetural por parte do cliente e de outras entidades envolvidas no projeto. Durante esta fase, para além da descrição dos detalhes necessários à implementação do sistema perante a arquitetura definida, serão especificados, no documento de *design*, os comportamentos dos componentes presentes na camada de lógica de negócio, de acordo com as funções atribuídas.

Embora as atividades associadas ao *design* detalhado apresentem várias técnicas, quase todas as metodologias têm em comum princípios subjacentes [SDKS14]. De seguida serão identificados três princípios que podem ser aplicados durante esta fase:

1. **Modularização** – esta técnica consiste em decompor um problema em partes percetíveis, de modo a simplificar a gestão de tarefas de todas as atividades. Esse mesmo princípio tem como vantagem a compreensão das estruturas lógicas, uma vez que cada componente pode ser estudado e analisado de forma singular, beneficiando da construção da solução, pois os componentes podem ser desenvolvidos e testados em paralelo. Na figura seguinte (Figura 22) ilustra-se um exemplo de decomposição das atividades, aquando da criação de uma nova conta para a aplicação de retalho (RPM).

[7] No Anexo IV (Tabela 11) apresenta em detalhe as especificidades dos adaptadores a serem desenvolvidos.

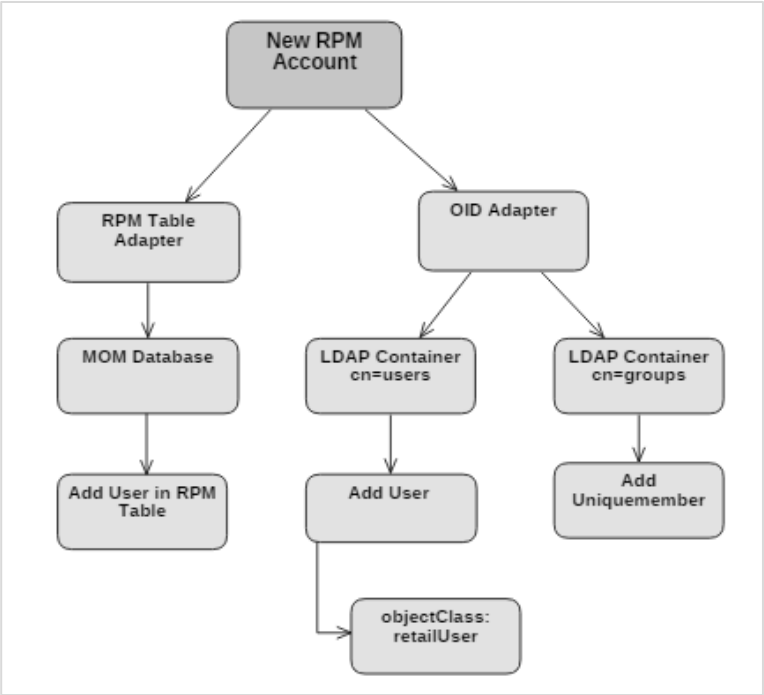


Figura 22 – Modularização

2. **Divisão e conquista** – esta técnica consiste em dividir um problema em subproblemas menores [GERMO12], com o intuito de resolver cada subproblema de forma independente, tornando a solução mais simples. O diagrama seguinte (Figura 23) apresenta a divisão do algoritmo de gestão de identidades em partes menores, procurando encontrar a solução através de raciocínio lógico para a criação de um utilizador no módulo (RPM), constatando-se que a combinação dessas partes define a solução pretendida.

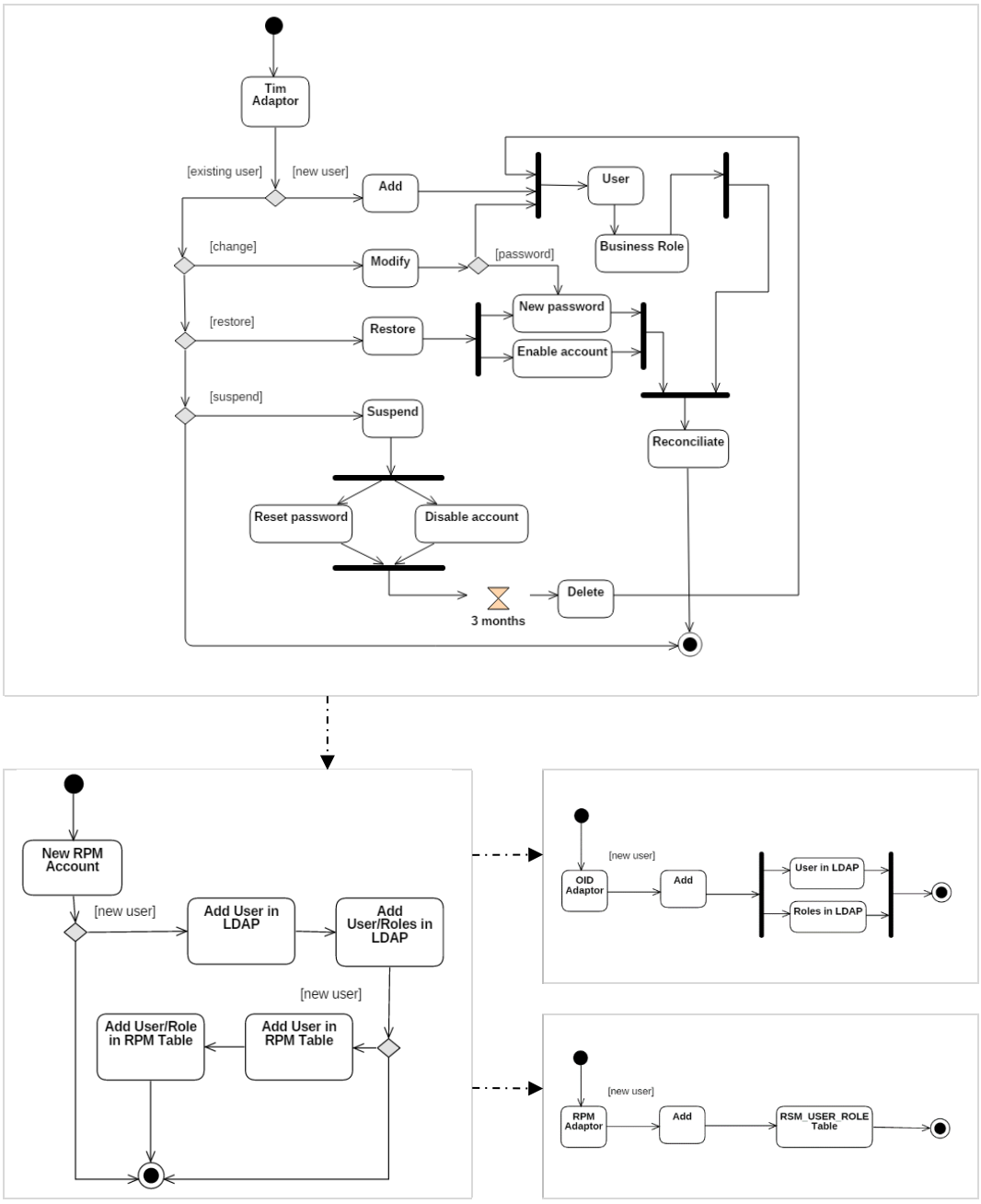


Figura 23 – Divisão e conquista

3. **Acoplamento** – este princípio mede a dependência entre os componentes definidos da solução. Ou seja, quanto mais dependente o componente (e.g. RPM Table Adapter) é da implementação do componente (e.g. ReIM Table Adapter), maior será o acoplamento entre os componentes mencionados. Uma situação de alto acoplamento entre os componentes envolvidos reflete-se numa maior dificuldade de interpretação, dado que precisam de ser compreendidos em conjunto. Outros aspetos a salientar relacionam-se com a complexidade de modificar, manter e suportar os componentes quando estão altamente acoplados [GERMO12]. A solução apresenta a vantagem de um baixo acoplamento, pois cada componente contém comportamentos e

responsabilidades próprias, não existindo dependências entre os adaptadores, do ponto de vista de implementação, podendo executar as devidas tarefas autonomamente sem dependerem de terceiros.

4.4 Sistema de gestão de identidades (alternativa)

Uma arquitetura deve apresentar estruturas bem definidas para permitir o sucesso dos objetivos do sistema, em que a definição dessas mesmas estruturas se fundamenta nas alternativas de *design* existentes. A decisão deve ser tomada entre as alternativas que propõem alcançar um ou mais atributos de qualidade do sistema, tais como: desempenho, escalabilidade, tolerância a faltas, compreensibilidade, usabilidade ou modificabilidade [GERMO12].

No entanto, os atributos de qualidade não devem estar completamente dependentes da fase de desenho, também deverão ser considerados durante a fase de construção/implementação da solução [BASS12].

No decurso do projeto foram identificadas alternativas de *design* da solução para o problema em questão. Os diagramas seguintes (Figura 24) e (Figura 25) apresentam um conjunto de componentes, com algumas variantes, que definem as particularidades e características do sistema IdM.

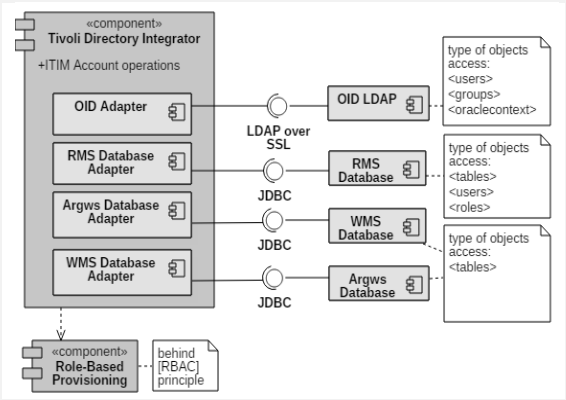


Figura 24 – idM alternativa de design I

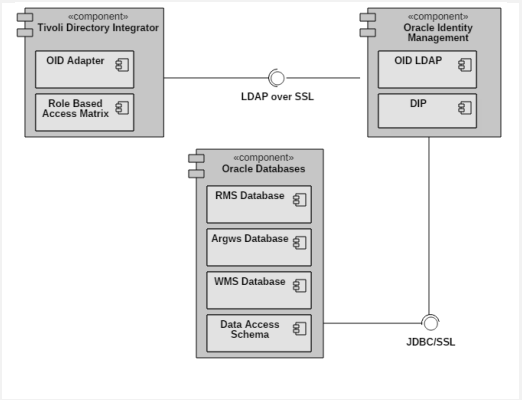


Figura 25 – idM alternativa de design II

A alternativa de *design* ilustrada na (Figura 24) apresenta igualmente uma arquitetura multicamada (N-Tier). A principal diferença reside no número de adaptadores de aprovisionamento implementados na camada lógica de negócio, em que os componentes apresentam o mesmo comportamento funcional, mas com uma elevada dependência entre as diversas operações a realizar. Para além do alto acoplamento existente, o sistema torna-se menos compreensível e dificulta a interação com os utilizadores responsáveis por suportar a plataforma ou quando necessitam de executar alguma funcionalidade no sistema.

A outra alternativa conhecida (Figura 25) apresenta uma solução de maior complexidade, requerendo a integração de novos componentes inexistentes na infraestrutura e alterações profundas no sistema de retalho. A correspondente camada lógica de aprovisionamento fica a cargo do componente (DIP)[8], contudo este módulo tem como propósito apenas sincronizar contas entre diferentes serviços de diretórios, tornando-se incapaz de cumprir os requisitos definidos para a gestão de identidades. A solução indicia uma solução incoerente e inadequada, que compromete atributos de qualidade como escalabilidade ou operabilidade, não sendo orientada para a usabilidade nem correspondendo a qualquer estilo ou padrão arquitetural.

4.5 Integração com o sistema de autenticação (TAM)

A prova de conceito realizada no âmbito deste projeto e as experiências decorridas durante a avaliação da solução contribuíram para concepção da solução de autenticação. Esta integração fornece uma solução de autenticação unificada entre a solução de autenticação do retalhista e as aplicações do sistema de retalho.

Pretende-se, com o seguinte diagrama, esquematizado na (Figura 26), descrever a arquitetura do sistema de autenticação e apresentar as funcionalidades introduzidas no sistema com a integração entre os componentes de autenticação.

O sistema oferece alta disponibilidade para todos os aplicativos, onde coexistem dois balanceadores de carga para distribuir os pedidos dos utilizadores entre os servidores onde estão alojadas as aplicações e os servidores que fornecem o serviço de autenticação.

Um dos balanceadores de carga torna-se responsável pela aplicação do conceito de *SSL Offloading*, retirando o processamento de encriptação dos servidores aplicacionais. Esta técnica permite também ter em consideração um baixo número de configurações, a serem realizadas nos servidores, para aceitarem apenas pedidos seguros.

Como referido anteriormente, os produtos de retalho instalados são certificados para funcionar com o componente (Oracle SSO), não sendo possível integrar diretamente com outros sistemas de autenticação. Neste caso, existe a necessidade de introduzir um agente na solução (Third-Party Agent) para estabelecer uma relação de confiança entre os sistemas e delegar a autenticação para o componente (IBM TAM), oferecendo a funcionalidade Single Sign-on (SSO) para as aplicações no domínio.

[8] Https://docs.oracle.com/cd/E28280_01/oid.1111/e10036/basics_09_dip.htm

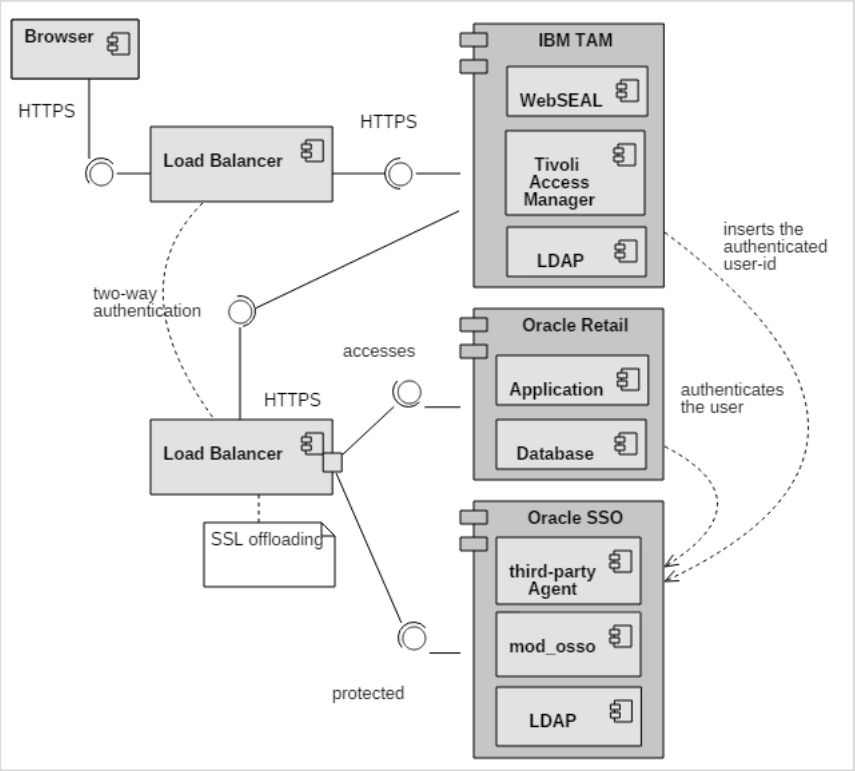


Figura 26 – Integração com o sistema de autenticação (TAM)

Durante a prova de conceito existiu uma tarefa obrigatória que consistia na sincronização dos utilizadores de negócio entre os repositórios LDAP, mas com a inclusão do sistema de gestão de identidades (TIM), esse mapeamento é efetuado automaticamente.

5 Construção da Solução

As tarefas de desenvolvimento da solução deverão ser iniciadas após a aprovação do documento de *design* arquitetural e detalhado.

A fase de construção corresponde ao desenvolvimento de código, configurações técnicas e testes unitários. O código e todas as alterações são registadas no sistema de controlo de versões, assim como os documentos com os passos detalhados sobre o procedimento de instalação/desinstalação das modificações, elementos que são parte integrante do processo estabelecido para esta etapa.

A construção da solução divide-se entre três fases distintas (Figura 27) mas sequenciais durante a implementação:

1. Implementar o conceito de *SSL Offloading* e reconfigurar as aplicações de retalho para utilizarem o protocolo HTTPS.

2. Integrar a solução de autenticação (TAM) com as aplicações de retalho.

3. Desenvolver e implementar os adaptadores lógicos para o aprovisionamento dos utilizadores de negócio.

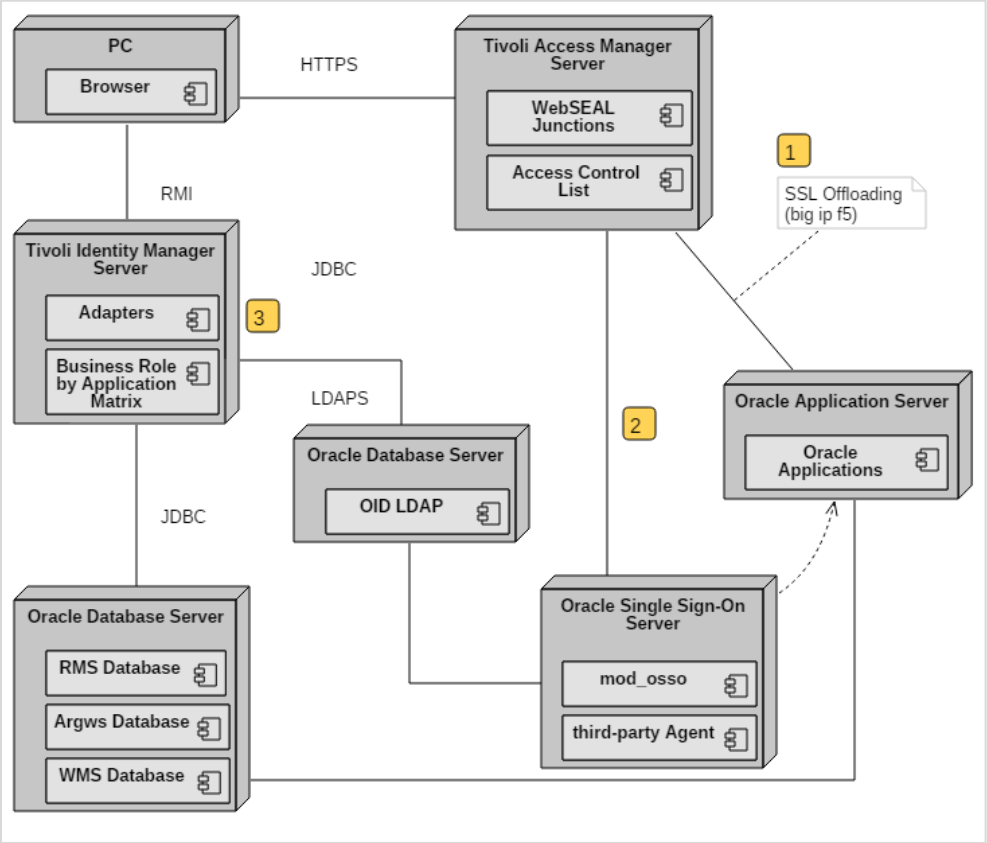


Figura 27 – Diagrama de instalação do sistema

5.1 Configuração *SSL Offloading*

A configuração representada (Figura 28) surge como pré-requisito para integrar a solução de retalho com o sistema de autenticação. Como descrito anteriormente na fase de desenho, o balanceador de carga torna-se responsável por duas funções: distribuir o tráfego de forma uniforme entre os servidores e garantir a utilização de protocolos seguros no acesso às aplicações, com a implementação da funcionalidade de *SSL Offload*. Este conceito retira as operações criptográficas por parte dos servidores.

Numa primeira fase pretende-se adicionar nomes canónicos (CNAME) ao servidor de DNS para mapear um nome de domínio com mais de duas letras e em seguida procede-se com a emissão dos certificados, assinados por uma autoridade de certificação de confiança. Depois da validação, deve-se importar o certificado digital com o novo domínio e concluir a configuração no balanceador de carga com as novas regras de criptografia. Estes detalhes encontram-se na documentação oficial [BIGIP].

As restantes configurações são realizadas nos servidores *Oracle*. A mudança dos nomes canónicos e a implementação do protocolo HTTPS provocaram um conjunto de alterações que deverão ser corrigidas nos servidores e aplicações:

- O repositório de metadata (DCM) do servidor (Oracle SSO) deve ser atualizado com as novas definições (nome, porta, protocolo de comunicação).
- Os produtos de retalho, incluindo o endereço do servidor (Oracle SSO) devem ser registados com o novo domínio[9] para funcionarem corretamente. Acrescem ainda alterações ao nível do servidor Apache, com a adição de novos elementos (certheaders module, SimulateHttps) para aceitarem pedidos seguros e terminarem no próprio servidor aplicacional.
- Os menus de ajuda deverão também ser alterados com os novos endereços.

[9] ssoreg.sh -oracle_home_path OraHome -site_name wls_server -config_mod_osso TRUE -mod_osso_url https://oracle_http_host.domain -config_file osso.conf

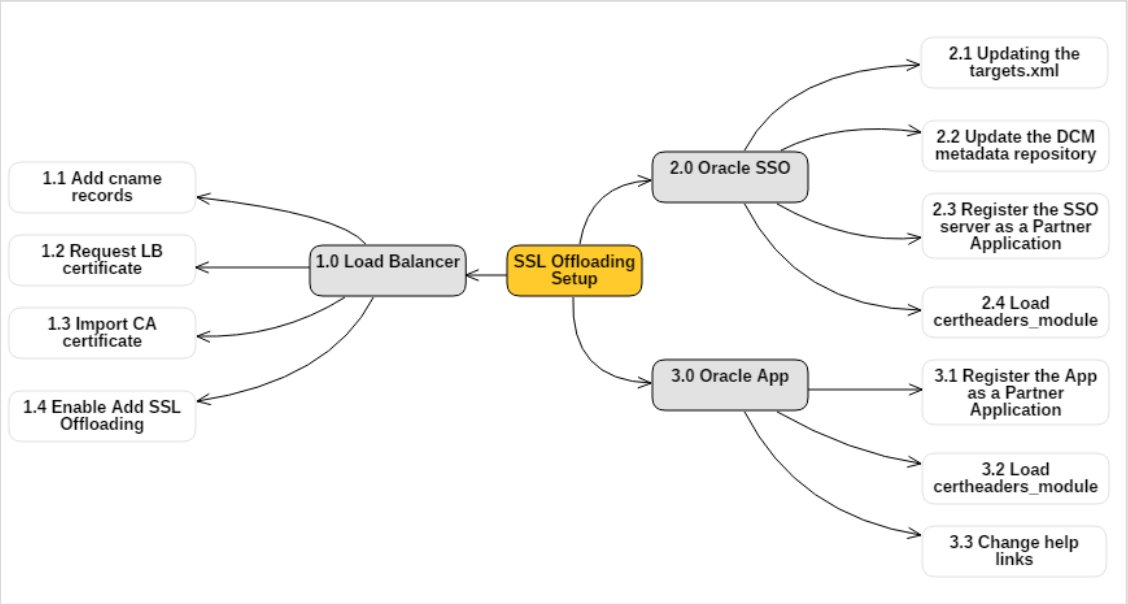


Figura 28 – Configuração do SSL Offloading

As configurações serão somente refletidas depois de reiniciar os serviços aplicacionais, o sistema operativo não será afetado depois das alterações realizadas.

5.2 Integrar a solução de autenticação

As aplicações encontram-se configuradas e registadas com o protocolo HTTPS. Após a execução deste passo obrigatório, estão reunidas as condições para iniciar as próximas atividades para integrar o sistema de retalho com o sistema de autenticação central.

A primeira atividade (Figura 29) começa com o processo de autenticação bidirecional entre o balanceador de carga e o *proxy* (WebSEAL), que envolve a troca de certificados digitais assinados pela mesma autoridade de certificação, cujo objetivo é garantir a troca segura de informação através da autenticação mútua entre as entidades.

Uma junção virtual estabelece uma ligação segura e permite que o componente (WebSEAL/TAM) ofereça o serviço de autenticação e de autorização. As junções virtuais correspondem individualmente a cada endereço definido para as aplicações que fazem parte da solução unificada. Uma das junções[10] requer um atributo que a distingue das restantes, em que deve ser especificado o parâmetro (iv_user) para permitir que o servidor de autenticação consiga passar a identidade do utilizador para o servidor (Oracle SSO). A composição das outras junções segue o procedimento padrão, sem o cabeçalho para autenticação.

[10] server task instance_name-webseald-host-name create -t ssl -h oracle_http_sso_host -f –v oracle_sso -c **iv_user** oracle_http_host.domain -ssl

Durante esta atividade deverão ser definidas as junções virtuais para os seguintes aplicativos da solução:

- *Oracle Single Sign-on* (iv_user)
- *Oracle Retail Merchandising System / Oracle Retail Sales Audit*
- *Oracle Retail Invoice Matching*
- *Oracle Retail Allocation*
- *Oracle Retail Price Management*
- *Oracle Retail Workspace*
- *Oracle BI Publisher*

Para além desta configuração e de forma a garantir outro nível de segurança, deve ser associado a cada objeto (junção virtual) uma lista de controlo de acesso (ACL) para determinar quais as operações o utilizador pode executar. Cada lista deverá ser constituída por regras e cada regra é identificada por um grupo.

O próximo passo a ser tomado nesta implementação relaciona-se com a instalação do agente (Third-Party Agent) no servidor Oracle SSO, que requer a customização da interface (IPASAuthInterface)[11]. Esta interface permite intercetar todos os pedidos com a variável (iv_user) durante o processo de autenticação e inclui um bloco de tratamento de exceções. A relação de confiança entre os sistemas e a delegação para o servidor (TAM) ficará dependente da alteração de um ficheiro de propriedades que contém as políticas e configurações do servidor (Oracle SSO), no qual deverão ser efetuadas as seguintes modificações:

- *MediumSecurity_AuthPlugin = com.ibm.tivoli.integration.SSOTAMAuth*
- *LogoutPageUrl = /sso/pages/webseal_logout.jsp*

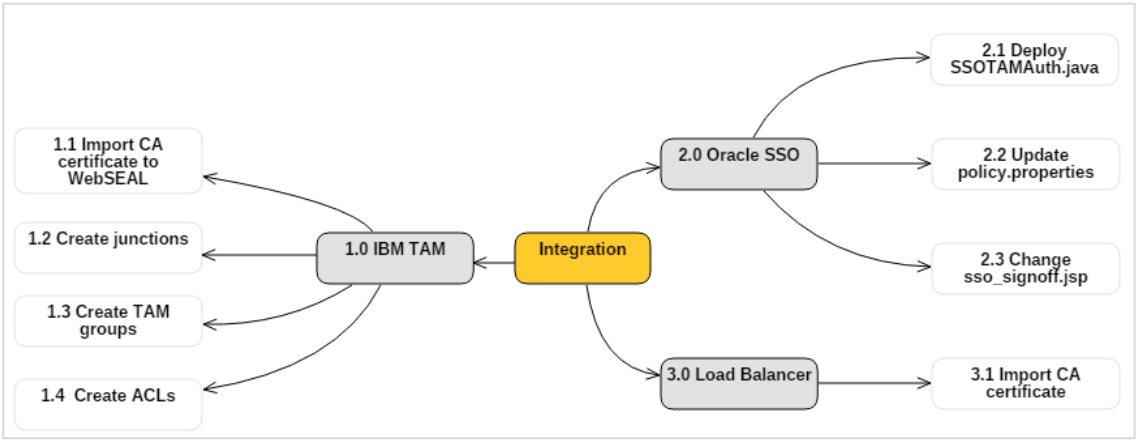


Figura 29 – Configuração da solução de autenticação

[11] Https://docs.oracle.com/cd/B28196_01/idmanage.1014/b15988/tpsso.htm#i1009109

Após as configurações descritas, o sistema de retalho deverá ficar integrado com o sistema de autenticação do retalhista, oferecendo a funcionalidade *Single Sign-on* (SSO) para as aplicações no domínio.

5.3 Desenvolver e implementar os adaptadores lógicos

A implementação dos adaptadores lógicos e a integração com a plataforma de gestão de identidades é a última tarefa a ser executada. O sistema tem os seus próprios requisitos e regras explícitas de funcionamento e, no seguimento destas dependências, foram identificadas as seguintes modificações, a serem realizadas nas bases de dados do sistema de retalho (Figura 30) antes de uma possível integração:

- Criação de contas de base de dados com o princípio do privilégio mínimo.
- Criação de um utilizador no serviço de diretórios com o princípio do privilégio mínimo.
- Desativação das políticas de palavras-passe.
- Funções criptográficas para cifrar as palavras-passe em duas bases de dados.

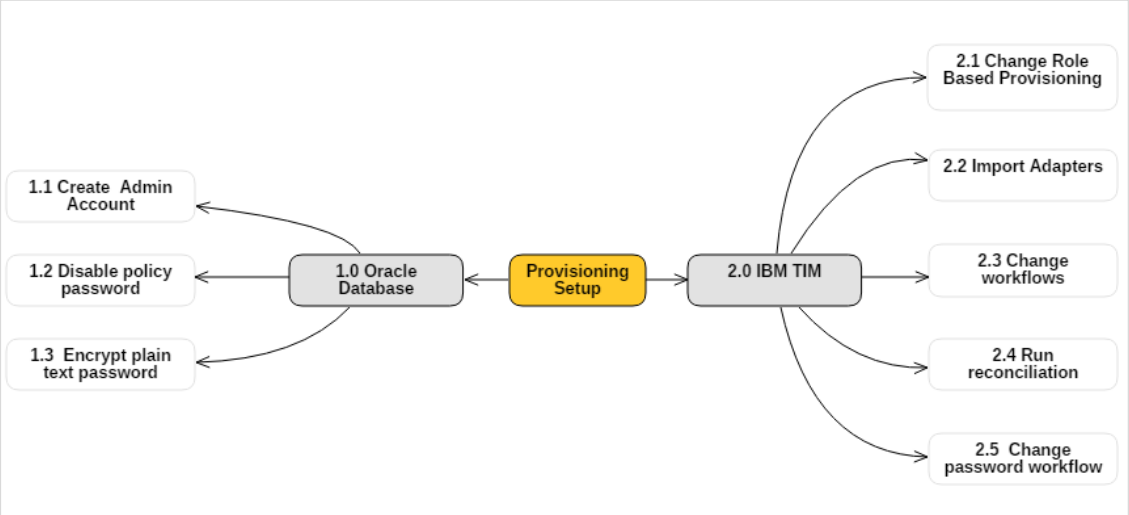


Figura 30 – Integração com o sistema de gestão de identidades

Depois da validação dos dados e das configurações efetuadas, procede-se à implementação da matriz de acessos baseada em funções de negócio, para gerir as permissões dos utilizadores no sistema, em que esta modificação garante de imediato o perfil do utilizador de negócio.

Adicionalmente, cada utilizador deve ter acesso apenas a uma função de negócio dentro da organização. Esta medida global, depois de aplicada, constitui-se redutora, pois os acessos dos utilizadores não são controlados por qualquer mecanismo para negar ou restringir o acesso ao sistema de retalho.

Os adaptadores são importados para o sistema de gestão de identidades e a partir desse momento torna-se possível automatizar o processo de aprovisionamento. A primeira operação a ser realizada durante a implementação é a execução do processo de reconciliação, sendo responsável por interpretar a informação sobre a autorização e privilégios atribuídos aos utilizadores nas aplicações de retalho. No caso de se identificarem diferenças entre a matriz de acessos estabelecida e o perfil do utilizador de negócio, o processo deve automaticamente retificar esses desvios.

Os adaptadores lógicos foram desenvolvidos de acordo com o estudo efetuado [ORUP15] sobre os vários modelos de segurança, requisitos de negócio e as diferentes especificações que caracterizam as aplicações. Na figura (Figura 31) encontra-se apresentado um exemplo relacionado com a gestão de um utilizador de negócio para a aplicação (ReIM). Neste contexto é necessário invocar dois adaptadores distintos, um para o serviço de diretórios, que é comum a todas as aplicações, e outro referente às tabelas de autorização da aplicação (ReIM).

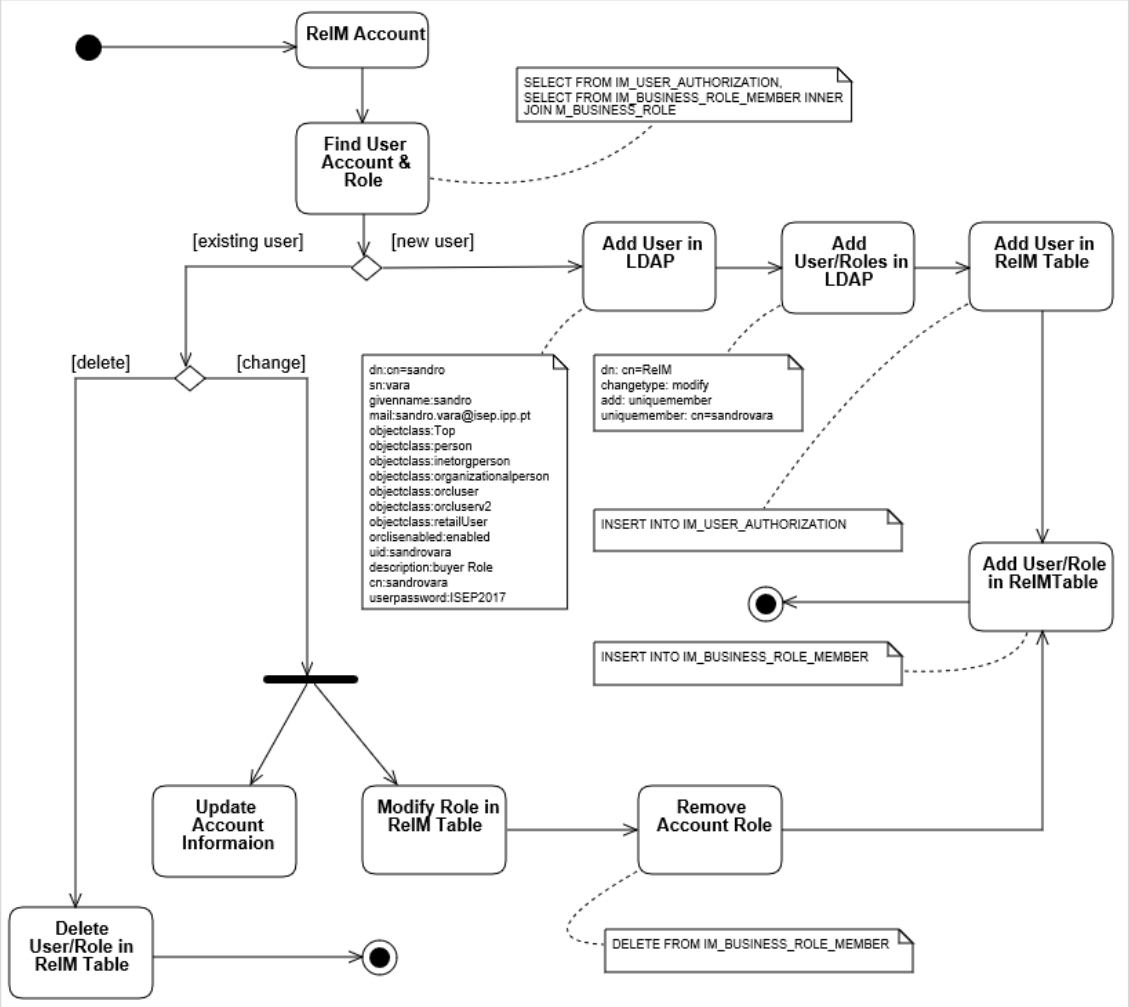


Figura 31 – Adaptador para a aplicação (ReIM)

6 Avaliação da Solução

6.1 Descrição da avaliação da solução preconizada

Este capítulo descreve o processo de avaliação da solução preconizada, com o objetivo de avaliar o funcionamento de todos os componentes, garantindo a qualidade da solução.

A estratégia de testes foi escolhida durante a fase de definição da solução, após o levantamento de requisitos e em acordo com a metodologia do projeto. A definição do ciclo de vida dos testes, tipo e nível é considerada na especificação da estratégia, em concordância com os objetivos do retalhista, seguindo as boas práticas recomendadas pelo *International Software Testing Qualifications Board*.

O diagrama de atividades representado na (Figura 32) descreve o comportamento do ciclo de vida dos testes, através de um conjunto de atividades interligadas, que se inicia com o estudo dos requisitos e termina com evidências conclusivas, que se refletem no estado atual de cada cenário de testes executado.

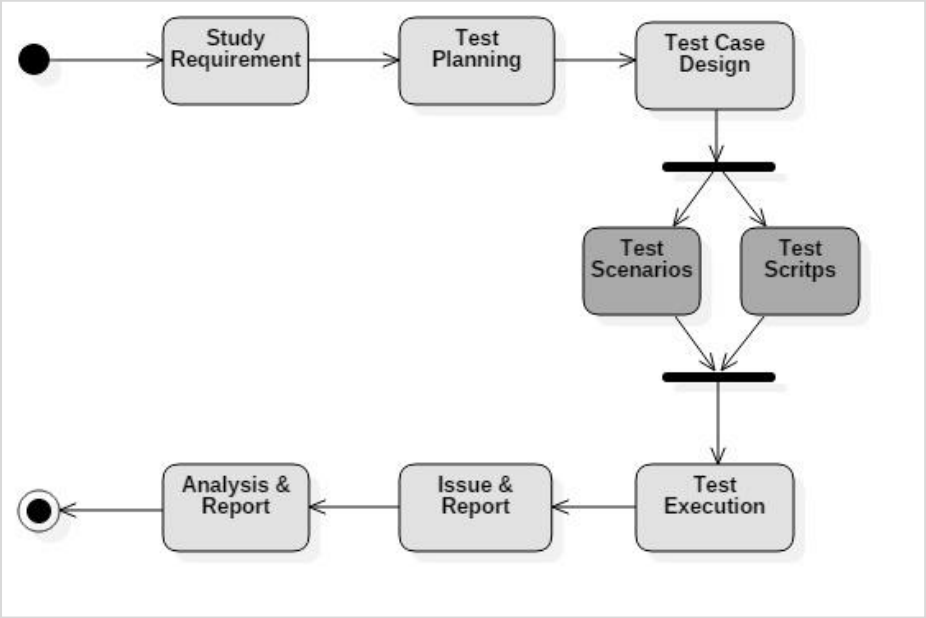


Figura 32 – Ciclo de vida dos testes

Em relação ao tipo de testes, destacam-se os testes funcionais e não funcionais, com o objetivo de avaliar se a solução funciona de acordo com a especificação dos requisitos previamente identificados. Em relação aos testes funcionais, identificaram-se os testes unitários, de integração e de aceitação.

Os testes unitários são o ponto de partida para a fase de execução de testes, verificam o funcionamento de um módulo ou componente desenvolvido. Os testes de integração verificam a comunicação entre os diferentes módulos ou componentes de um processo. Os testes de aceitação verificam se a solução cumpre os requisitos identificados para a solução preconizada e se satisfaz ou não os critérios de aceitação.

Relativamente aos testes não funcionais, identificaram-se os testes de desempenho e os testes de penetração, que verificam falhas de segurança na solução, sendo executados para encontrar anomalias e vulnerabilidades no sistema.

Para cada fase de testes são definidos critérios, os quais obedecem a um conjunto de regras que devem ser cumpridas. Para passar à fase seguinte de testes, todos os erros críticos devem ser obrigatoriamente solucionados, no entanto existem exceções que estão relacionadas com o nível de severidade, pois podem não impactar o negócio. Os detalhes sobre a classificação de erros podem ser consultados na seguinte figura (Figura 33).

Severity Level		Criteria	Impact on Project
1	Critical	Doesn't work; Avoid normal use; Originate critical errors.	Product cannot be released / promoted to Production (Take-off).
2	Severe	Doesn't perform as required; Doesn't avoid use, but has impacts on processes.	Project cannot be closed, but product can be released.
3	Annoyance	Doesn't affect normal use, but has to be solved.	Doesn't have any impact on Project Take-off.
4	Improvement	New request. Interface improvement.	Option: Evolutive maintenance, next release.

Figura 33 – Classificação dos erros
(Imagem de: Wipro Limited. 2015. Solution Integration Methodology, p. 8)

Existe uma etapa determinante na validação do processo de implementação. O retalhista recorre à metodologia de Cutover para certificar que existe uma única e comprovada abordagem para promover a solução para produção. Esta é constituída por um complexo número de ações e atividades necessárias para alcançar com sucesso a implementação da solução e mitigar riscos desconhecidos, que podem comprometer o negócio. Este exercício é denominado de ensaio, pois simula a implementação da solução em produção num ambiente de testes com as mesmas caraterísticas e com todas as entidades participantes. No final é apresentado um relatório com o resultado da simulação, onde estão incluídas as estimativas de tempo de execução de cada tarefa. No caso de um ensaio bem-sucedido, a solução poderá ser promovida para o ambiente produtivo.

Por fim, recomenda-se uma apreciação do serviço prestado por parte do cliente com base em inquéritos de avaliação. Deste modo e como prática corrente do implementador, deverá ser avaliado o índice de satisfação através de inquéritos CSAT (consultar Anexo V). Com esta medida é possível identificar melhorias contínuas a serem implementadas e reforçar a relação com o cliente.

6.2 Testes de aceitação

Os testes de aceitação representam a última fase no processo de testes. Os potenciais utilizadores do sistema devem estar envolvidos no seu planeamento e são geralmente os responsáveis pela execução dos testes de aceitação. Estes vão avaliar a solução desenvolvida com base no levantamento de requisitos (Tabela 2) efetuado durante a identificação do problema.

Na tabela seguinte (Tabela 10) são apresentados os casos de teste mais relevantes executados durante esta fase decisiva do projeto.

Tabela 10 – Testes de aceitação

Caso de Teste	Resultado Esperado	Resultado Final	Req ID
Criar um utilizador genérico no sistema de retalho	O utilizador genérico tem de ser prontamente eliminado do sistema de retalho	O sistema IdM elimina automaticamente os utilizadores quando são criados sem uma identidade única	**1**
Criar um utilizador para cada função de negócio no sistema de retalho	O utilizador tem de ser criado de forma automática seguindo o modelo baseado em funções de negócio	O sistema IdM garante uma plataforma central e automática para o aprovisionamento de utilizadores, em que cada utilizador tem o seu papel na organização	**3,7**
Atribuir uma nova função de negócio ao utilizador no sistema de retalho	O utilizador tem de ser modificado de acordo com o novo papel de negócio	O sistema IdM modifica o utilizador de acordo com a nova função de negócio	**3,7**
Suspender/eliminar um utilizador de negócio no sistema de retalho	O utilizador tem de ser suspendo e eliminado do sistema de retalho	O sistema IdM suspende e elimina o utilizador de negócio de acordo com as especificações e regras estabelecidas	**3,7**
Alterar indevidamente os privilégios e função de negócio do utilizador no sistema de retalho	O processo reconciliação deve detetar os desvios concedidos e corrigir automaticamente os privilégios do utilizador	O sistema IdM interpreta os privilégios e autorização dos utilizadores no sistema de retalho e automaticamente corrige as diferenças	**2,7,8**
Verificar o novo processo de autenticação no sistema de retalho	O utilizador deve autenticar-se através de protocolos seguros O Oracle Single Sign-On delega autenticação ao novo sistema TAM	O utilizador de negócio acede a todas as aplicações autorizadas e protegias pelo novo sistema TAM, através de protocolos seguros com uma autenticação única	**5,6**
Manter um utilizador autenticado inativo no sistema de retalho por um período superior a 15 minutos	O utilizador perde a sessão por inatividade	O utilizador ao permanecer mais de quinze minutos sem atividade no sistema de retalho, a sessão termina automaticamente	**9**
Alterar a palavra-passe do utilizador de negócio	O utilizador recebe uma palavra-passe gerada aleatoriamente, sendo forçado a alterá-la	O utilizador autentica-se no sistema de retalho com a nova palavra-passe modificada por si mesmo	**4,5**
Alterar a palavra-passe do RAD	A modificação da palavra-passe do RAD tem de ser totalmente transparente para o utilizador final	O utilizador autentica-se com sucesso na aplicação RMS/ReSA	**4,5**

Durante os testes de aceitação foram encontrados erros graves relacionados com a alteração da palavra-passe do RAD e erros menores na eliminação dos utilizadores de negócio em diversas aplicações de retalho. Os adaptadores lógicos foram revistos e alterados de modo a satisfazer as necessidades da solução, a qual deve cumprir os requisitos estabelecidos.

O cliente, após aceitar e aprovar a solução para o sistema produtivo, deverá fazer com que a solução passe pelo processo de Cutover, a fim de garantir a validação do processo de implementação.

7 Conclusões

Pretende-se com este estudo, num contexto real, abordar as diferentes atividades e métodos desenvolvidos de acordo com as especificações dos sistemas apresentados e a consequente resolução de qualquer incerteza existente num ambiente substancialmente complexo. As incertezas tecnológicas e científicas presentes no domínio do problema, em conjunto com as demais adversidades que surgiram ao longo do projeto, são aspetos característicos deste desafio tecnológico com particularidades inovadoras, cujo objetivo reside em explorar um modelo de gestão de identidades e acessos num sistema de retalho composto por vários módulos aplicacionais e componentes funcionalmente integrados. O desenvolvimento de competências necessárias pelos elementos intervenientes e as metodologias empregues no âmbito deste projeto constituíram-se como um fator decisivo, quer sob o ponto de vista da investigação de novos processos, quer no domínio do controlo de acessos e gestão de utilizadores no sistema de retalho (Oracle Retail), quer na concepção da solução denominada de ideal, utilizando componentes existentes na mesma infraestrutura tecnológica, conforme os princípios estabelecidos.

As decisões sobre o modelo desenvolvido descrevem boas práticas de engenharia e orientações metodológicas que permitiram, nomeadamente, utilizar abordagens estruturadas no desenvolvimento dos controlos de segurança no sistema e, por conseguinte, mitigar riscos para a organização durante a implementação. Permitiram ainda desenhar uma solução adequada para suportar as políticas de aprovisionamento e um mecanismo de autenticação centralizada sobre protocolos seguros, sem introduzir qualquer impacto para as diferentes funcionalidades aplicacionais de cada unidade de negócio. Verifica-se ainda que a solução permite alcançar diversos atributos de qualidade no sistema (e.g. escalabilidade, disponibilidade e manutenibilidade) e que satisfaz por completo todos os requisitos identificados durante a definição da solução.

Um outro aspeto de grande importância incidiu sobre a análise detalhada acerca das restrições tecnológicas que compõem o sistema, pois as aplicações de retalho têm as suas próprias especificações de segurança, as quais podem condicionar o seu funcionamento, em especial

quando integradas com sistemas de autenticação externos. Estes elementos, que são considerados essenciais na construção da solução pretendida, para além de objeto de estudo durante o projeto, foram sujeitos a uma avaliação sistemática, após a realização de provas de conceito (PoC) sobre os componentes de autenticação.

A solução desenvolvida foi promovida para o ambiente produtivo com distinção, sem apresentar qualquer erro ou defeito, cumprindo todos os critérios de aceitação. Assim, após várias tentativas frustradas, que decorreram durante cinco anos incessantes, a integração entre o sistema de retalho e o sistema de gestão de identidade e acessos TIM/TAM é uma realidade incontornável e por todos aceite como um resultado de grande sucesso para os objetivos estratégicos do grupo retalhista. Este acontecimento desencadeia uma mudança imediata nos processos fundamentais de gestão das identidades, estando também integrado com o sistema de recursos humanos. O ciclo de vida dos utilizadores é neste momento gerido de forma autónoma, controlado por funções de negócio, sem intervenção de terceiras entidades. A plataforma de autenticação unificada suporta múltiplos domínios, com um único ponto de acesso, pelo que permite aos utilizadores autenticaram-se nas aplicações de retalho com as mesmas credenciais.

Os processos implementados permitem ao grupo retalhista expandir as suas operações de negócio num ambiente plenamente controlado, segundo as normas e políticas de segurança da organização.

Numa perspetiva complementar, este estudo torna-se relevante e inovador. O conhecimento tecnológico adquirido durante o projeto permitiu ao implementador a especialização numa área que carece de regras objetivas sobre os processos referidos. Este fator diferenciador pode ser extremamente vantajoso para futuras implementações ou na conquista de novos clientes com as mesmas necessidades. Atualmente, o modelo desenvolvido, para além de fazer parte do portfólio de serviços, pode ser adaptado a qualquer empresa retalhista ou expandido para outras áreas de negócio.

Como trabalho futuro, poderia considerar-se um sistema de retalho composto por todos os domínios possíveis de autenticação. Independentemente da complexidade, a implementação do protocolo de autenticação Kerberos, integrado com o serviço de diretórios corporativo, acrescentaria uma camada de segurança ao sistema operativo (e.g. Linux, HP-UX). Desta forma, obter-se-ia um maior nível de controlo sobre as operações realizadas pelos utilizadores técnicos, que são responsáveis por suportar e manter os ambientes.

Como consideração final realça-se o sucesso da implementação e os objetivos alcançados.

Referências

[AGOID] Oracle Corporation, 2009. Administrator's Guide for Oracle Internet Directory 11g, p. 32-3;

[AGCS] Oracle Corporation, 2005. Administrator's Guide for Oracle Collaboration Suite, p. 7-3;

[BASS12] Bass L., Clements P., Kazman R. 2012. Software Architecture in Practice. Addison-Wesley Professional, 3rd edition, New Jersey, USA;

[BIGIP] Deploying the BIG-IP LTM System with Oracle Beehive Collaboration Suite P. 18-24;

[Delloi15] Deloitte Touch Tohmatsu Limited, 2015. Global Powers of Retailing 2016 - Navigating the new digital divide, p. 4-45;

[KDSJ10] Keesling D., Spiller J., 2010. Oracle Database 11g Security, California, USA, p. 1-8;

[IdM08] Oracle Corporation 2008. An Introduction to Oracle Identity Management, Oracle White Paper, p. 3-9;

[GERMO12] Germoglio G. 2012. Arquitetura de Software, Rice University, Houston, Texas, p. 33-88;

[GOA16] Atul Goyal, 2016. Oracle Identity Cloud Service - A Business White Paper, p. 3;

[IBMAP] IBM Corporation, 2008. Integrated Identity and Access Management Architectural Patterns, p. 20;

[IBMIad] IBM Corporation, Installing - Adapter and profile installation, p. 2-3;

[IBMPo] IBM Corporation, Product overview - Access management with IBM Tivoli Identity Manager and other products, p. 2-3;

[IBMTam] IBM Corporation, 2003. IBM Tivoli Access Manager for WebLogic Server, p. 1;

[LSRHM09] Lunau, S., Staudter, C., Roenpage O., Hugo C., Meran, R., Hamalides, A., Roenpage, O., Mollenhauer, J.P. 2009. Design for Six Sigma Lean Toolset: Implementing Innovations Successfully,

Frankfurt, Germany, Springer-Verlag Berlin Heidelberg, p. 156-159;

[OASSSO] Oracle Corporation, 2006. Application Server Single Sign-On, p. 14-2;

[OCSG] Oracle Corporation, 2009. Oracle Containers for J2EE- Security Guide, p. 8-4;

[ORS11g] Oracle Corporation, 2011. Publishing Reports to the Web with Oracle Reports Services 11g Release - Configuring and Administering OracleAS Single Sign-On, p. 17-9;

[ORSP13] Oracle Corporation, 2008. Security Architecture, p. 2-40;

[ORSP14] Oracle Corporation, 2014. Oracle Retail - Release 14.0 Security and Provisioning Overview, p. 2-35;

[ORUP15] Antunes, P., Vara, S., 2015, SIFID I&D - Oracle Retail User Provisioning;

[RRA11] Oracle Corporation, 2011. Oracle Retail Reference Architecture Overview Release 13.2.x, p. 3;

[RWRF05] Rittinghouse, J.W., Ransome, J. F. 2005. Business Continuity and Disaster Recovery for InfoSec Managers, Oxford, Elsevier Digital Press, p. 193;

[SDKS14] Shoemaker, D., Kenneth, S. 2014. Cybersecurity: Engineering a Secure Information Technology Organization, Stamford, USA, p. 127.

Anexos

Anexo I – Metodologia de Integração de Soluções

A adaptação da metodologia de integração de soluções (Figura 34) foi estabelecida no âmbito do Projeto Autorização para acompanhar as distintas fases da solução:

- Identificação da Solução;
- Análise;
- Design;
- Código e Testes Unitários;
- Testes de Aceitação e Cutover;
- Implementação e Estabilização.

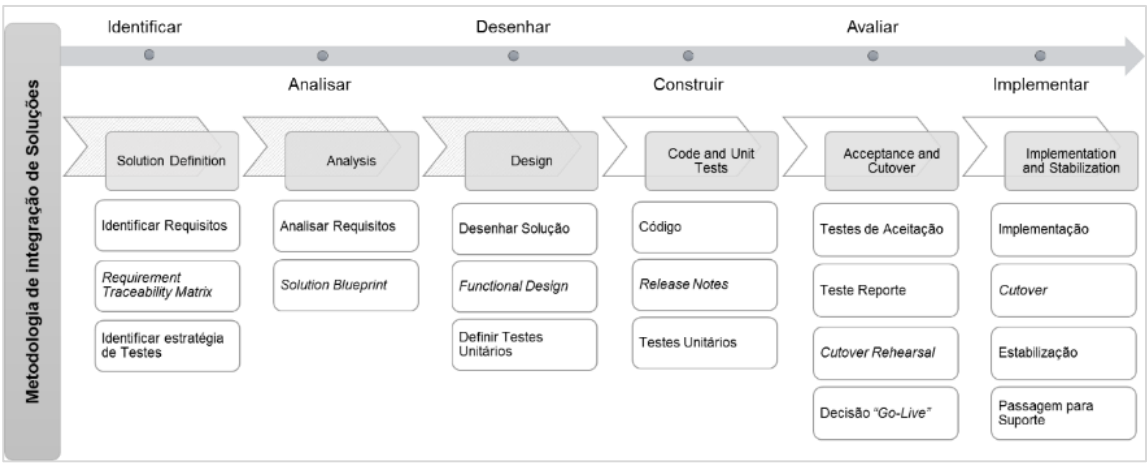


Figura 34 – Metodologia de integração de soluções adaptada ao problema
(Imagem adaptada de: Wipro Limited. 2015. Solution Integration Methodology, p. 1)

Anexo II – Domínios dos produtos Oracle Retail

Os domínios dos produtos *Oracle Retail* estão distribuídos por diferentes áreas de negócio, processos e competências para suportar as operações globais da organização (Figura 35). Cada domínio de produto tem o seu próprio modelo arquitetural e especificações de segurança para cada módulo aplicacional.

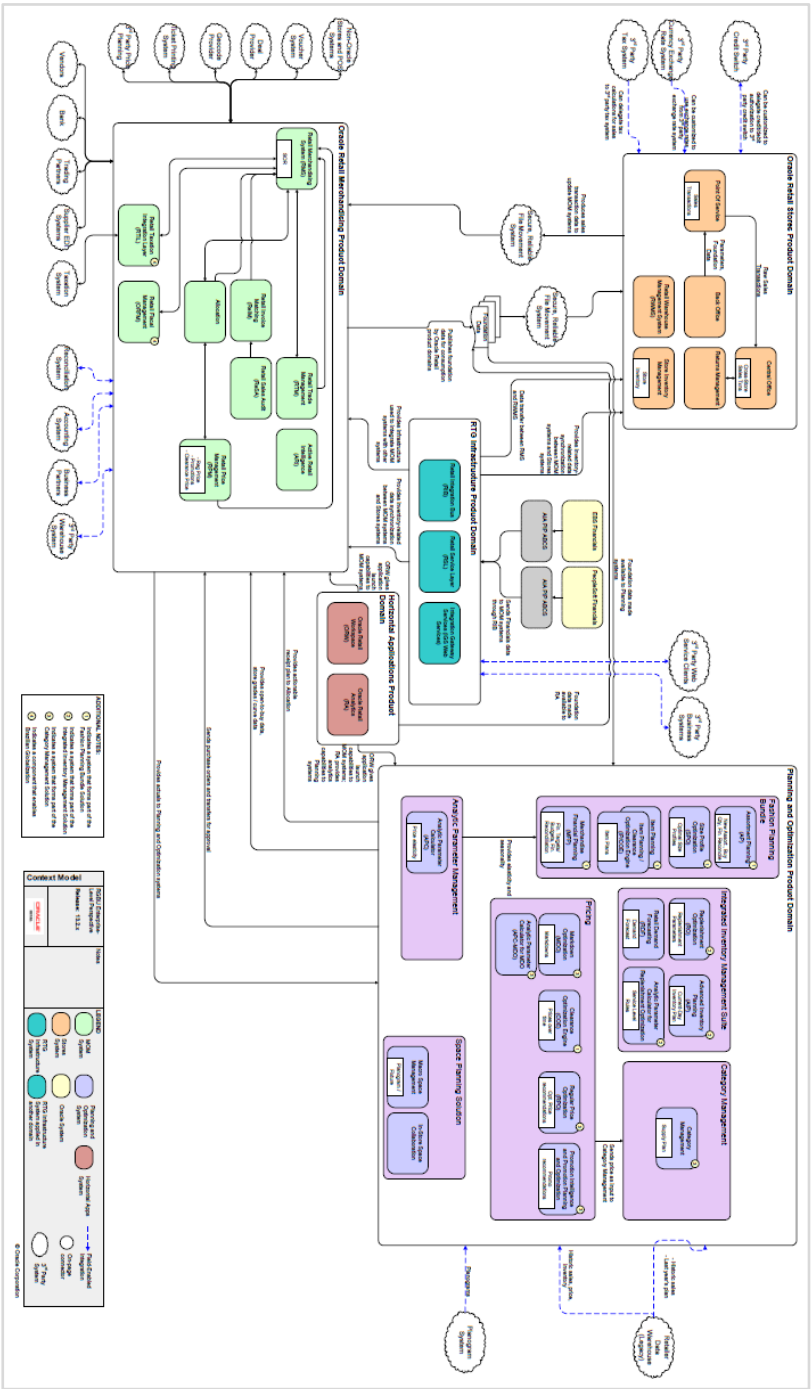


Figura 35 – Domínios de produtos
(Imagem de: Oracle. 2011. Oracle Retail Reference Architecture, p. 3)

Anexo III – Modelo de dados

Os modelos de dados relacionais (Figura 36) das diferentes aplicações de retalho foram objeto de estudo deste problema, de forma a tornar possível o ciclo de vida de um utilizador no sistema de retalho, sem causar impactos para o negócio.

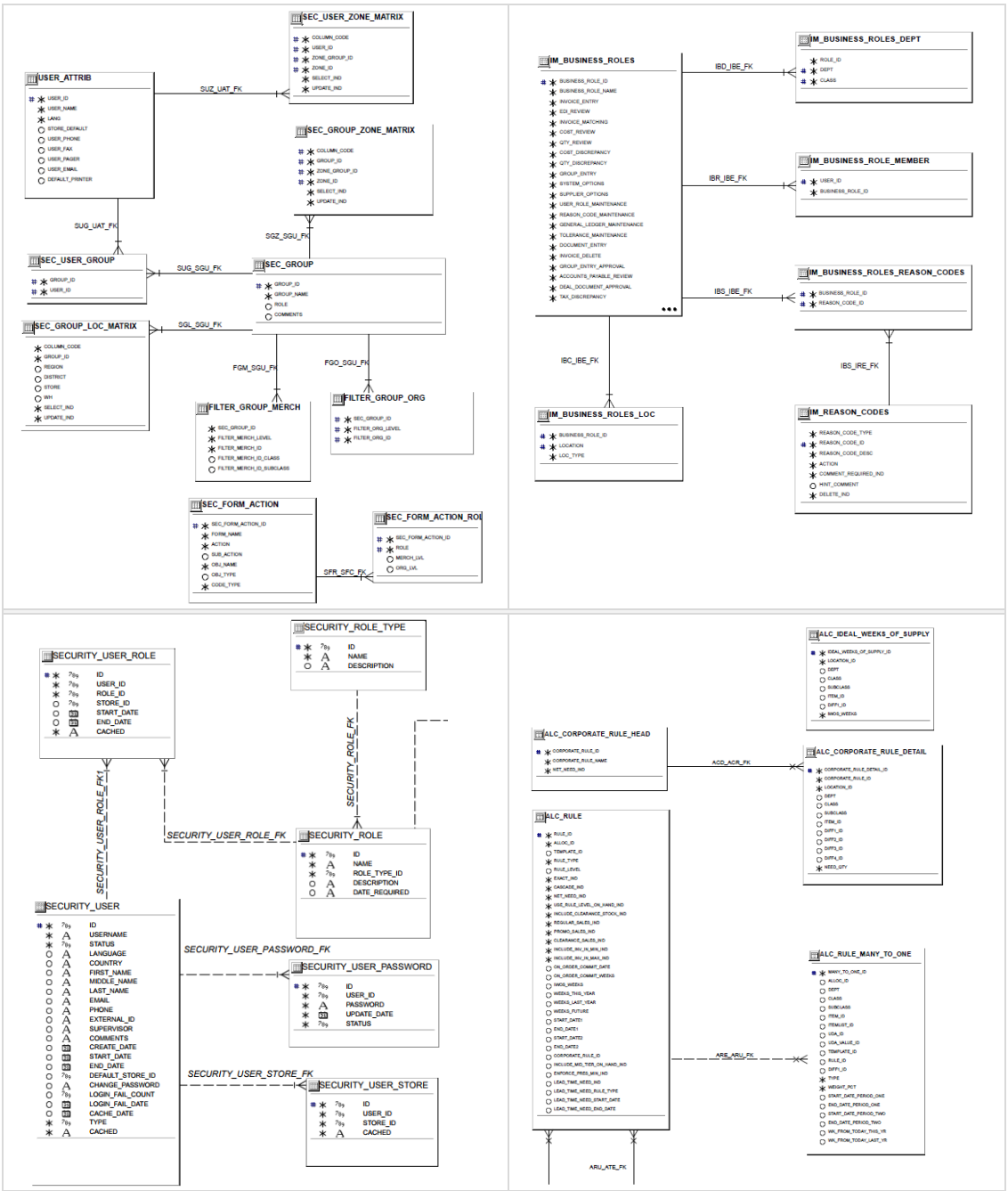


Figura 36 – Estudo do modelo de dados

(Imagem de: Oracle. 2012. RMS, ReIM, SIM, ALLOC Data Model)[12]

[12] Http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html

Anexo IV – Operações dos Adaptadores Lógicos

Tabela 11 – Adaptadores lógicos

Adaptador	TIM operação	Descrição
OID (LDAP)	Adicionar	Criar o utilizador com as classes de objetos e atributos específicos. Associar as permissões de acesso, quer aos grupos referentes ao Portal (WebCenter), quer aos grupos de acesso aos Reportes (BIP)
	Modificar	Alterar utilizador e os grupos associados
	Eliminar	Eliminar o utilizador e todas as referências associadas
	Suspender	Inativar o utilizador
	Reativar	Ativar o utilizador
	Reconciliar	Reconciliar o utilizador com os grupos associados
	Alterar palavra-passe	Modificar a palavra-passe do utilizador
OID RAD (LDAP)	Adicionar	Criar o RAD do utilizador com os detalhes de ligação e a mesma palavra-passe do utilizador criado na base de dados (RMS)
	Modificar	N/A
	Eliminar	Eliminar o RAD do utilizador
	Suspender	N/A
	Reativar	N/A
	Reconciliar	Reconciliar as entradas do RAD
	Alterar palavra-passe	Modificar a palavra-passe do RAD e invocar o adaptador RMS Base de Dados para executar a mesma operação
RMS Base de Dados	Adicionar	Criar utilizador de base de dados, conceder privilégios de sistema e atribuir funções de negócio
	Modificar	Alterar as funções de negócio atribuídas
	Eliminar	Eliminar utilizador de base de dados
	Suspender	Inativar o utilizador de base de dados
	Reativar	Ativar o utilizador de base de dados

	Reconciliar	Reconciliar o utilizador com as funções de negócio atribuídas
	Alterar palavra-passe	Modificar a palavra-passe do utilizador de base de dados e invocar o adaptador RAD para executar a mesma operação
RMS Tabelas	Adicionar	Inserir registos do utilizador das tabelas de autorização
	Modificar	Alterar registos do utilizador aos grupos associados
	Eliminar	Eliminar registos do utilizador aos grupos associados
	Suspender	N/A
	Reativar	N/A
	Reconciliar	Reconciliar o utilizador com as tabelas de autorização
	Alterar palavra-passe	N/A
ReSA Tabelas	Adicionar	Inserir registos do utilizador das tabelas de autorização
	Modificar	Alterar registos do utilizador das tabelas de autorização
	Eliminar	Eliminar registos do utilizador das tabelas de autorização
	Suspender	N/A
	Reativar	N/A
	Reconciliar	Reconciliar o utilizador com as tabelas de autorização
	Alterar palavra-passe	N/A
RPM Tabelas	Adicionar	Inserir registos do utilizador das tabelas de autorização
	Modificar	N/A
	Eliminar	Alterar registos do utilizador das tabelas de autorização com uma data de fim
	Suspender	N/A
	Reativar	N/A
	Reconciliar	Reconciliar o utilizador com as tabelas de autorização
	Alterar palavra-passe	N/A

ReIM Tabelas	Adicionar	Inserir registos do utilizador das tabelas de autorização
	Modificar	Alterar registos do utilizador das tabelas de autorização
	Eliminar	Eliminar registos que fazem a associação entre o utilizador e a função de negócio
	Suspender	N/A
	Reativar	N/A
	Reconciliar	Reconciliar o utilizador com as tabelas de autorização
	Alterar palavra-passe	N/A
ALLOC Tabelas	Adicionar	Inserir registos do utilizador das tabelas de autenticação e autorização
	Modificar	Alterar registos com os departamentos associados ao utilizador
	Eliminar	Eliminar registos com os departamentos da tabela de autorização e alterar a palavra-passe do utilizador com um valor nulo
	Suspender	N/A
	Reativar	N/A
	Reconciliar	Reconciliar o utilizador com os departamentos da tabela de autorização
	Alterar palavra-passe	N/A
WMS Tabelas	Adicionar	Inserir registos do utilizador das tabelas de autenticação e autorização
	Modificar	Alterar registos do utilizador das tabelas de autorização
	Eliminar	Eliminar registos do utilizador das tabelas de autorização
	Suspender	Alterar palavra-passe na tabela de autenticação
	Reativar	Alterar palavra-passe na tabela de autenticação
	Reconciliar	Reconciliar o utilizador com as tabelas de autorização
	Alterar palavra-passe	Alterar palavra-passe no serviço de diretórios e sincronizar na tabela de autenticação
Argws Tabelas	Adicionar	Inserir registos do utilizador das tabelas de autenticação e autorização

	Modificar	Alterar registos do utilizador das tabelas de autorização
	Eliminar	Eliminar registos do utilizador das tabelas de autorização
	Suspender	Alterar palavra-passe na tabela de autenticação
	Reativar	Alterar palavra-passe na tabela de autenticação
	Reconciliar	Reconciliar o utilizador com as tabelas de autorização
	Alterar palavra-passe	Alterar palavra-passe no serviço de diretórios e sincronizar na tabela de autenticação

Anexo V – Questionário Wipro CSAT

1. Did the project deliver the RESULTS and the QUALITY that were promised?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

2. Were key project deadlines met?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

3. Was day to day discipline and direction provided in regards to approach, scope & schedule?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

4. Did the project team produce as well as guide; be total team players and focus on delivering results?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

5. The project PROCESS (approach, communication, and staffing) was:

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

6. Was there open, honest and timely communications, with no surprises, acting as one project team?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

7. Were the right personnel assigned consistently throughout the project life-cycle?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

8. Did the project team bring an outside perspective to bear, and also demonstrate creative and flexible approaches in meeting project objectives?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

9. Did the project team listen, learn, and then execute an approach to solve business problems?

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

10. The OVERALL SERVICE for the project was:

○ NA	○ Extremely dissatisfied	○ Dissatisfied	○ Somewhat dissatisfied
○ Neutral	○ Somewhat satisfied	○ Satisfied	○ Very satisfied

Overall Comments: