FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

MODELO DE GESTÃO DE IDENTIDADES E ACESSOS

Vitor João Constantino Madureira

Mestrado Integrado em Engenharia Informática e Computação

Orientador: Raul Moreira Vidal

28 de Junho de 2010

Modelo de Gestão de Identidades e Acessos

Vitor João Constantino Madureira

Mestrado Integrado em Engenharia Informática e Computação

Aprovado em provas públicas pelo Júri:

Presidente: João Pascoal Faria (Professor Auxiliar)

Vogal Externo: Luís Borges Gouveia (Professor Associado da Universidade Fernando Pessoa)

Orientador: Raul Fernando de Almeida Moreira Vidal (Professor Associado)

Resumo

Uma definição estratégica de gestão de identidades e acessos deve ser desenvolvida, numa perspectiva de aumentar a segurança nos sistemas de informação da organização e obter uma gestão de utilizadores eficaz de forma a reduzir toda a complexidade envolvida.

A definição de um modelo de gestão de identidades e acessos é um passo importante para obter uma gestão de utilizadores eficaz.

A forma, como vão ser identificados os utilizadores e controlados os seus acessos aos recursos são os desafios que se colocam. Neste contexto, um levantamento do estado actual a nível de utilizadores e acessos deve ser prioritário antes de começar este processo com alguma complexidade. Posteriormente, deve ser definida pelo menos uma forma de identificação dos seus utilizadores e um ou vários modelos de controlo de acesso devem ser implementados.

Quando se tratam de organizações com grandes números de utilizadores, onde a sua criação não seguiu nenhuma regra e a atribuição de acessos não foi controlada, o trabalho de revisão destes utilizadores torna-se complexo e essencialmente muito longo.

Abstract

A definition of strategic identity and access management should be developed, with a view to increase security in the information systems of the organization and supported by an effective user management to reduce all the complexities involved in.

The definition of an Identity and Access Management model is an important step to getting an effective management of users.

The way how the users will be identified and their access to resources will be controlled are the challenges to achieve. In this context, a survey of current state-level of users and access must be given priority before beginning this process with some complexity. Afterwards, it must be defined at least one type of identification of their users and one or more control access model must be implemented.

When dealing with organizations with a large number of users where their creation did not follow any rules and assignment of access was not controlled, the work of revising these users becomes complex and too long.

Agradecimentos

Inicialmente gostaria de agradecer à SONAE por ter proporcionado a realização desta dissertação nas suas instalações.

Ao responsável da área de Segurança da Informação Carlos Fernandes, com quem tive o privilégio de trabalhar e evoluir muito profissionalmente dada a sua competência e experiência profissional.

Ao orientador Raul Vidal, por ter aceitado orientar esta dissertação assim como pela sua disponibilidade, pelo seu profissionalismo e dedicação durante todo o meu percurso na Faculdade de Engenharia.

Um agradecimento muito forte e especial para os meus pais, que sempre me apoiaram em todos os desafios.

Conteúdo

Capítulo 1 Introdução 15
1.1. Contexto/enquadramento 17
1.2. Motivação e objectivos 18
1.3. Estrutura da Dissertação 21
Capítulo 2 Gestão de Identidades e Acessos 22
2.1. Introdução 22
2.2. Gestão de Identidades e Acessos (IAM) 23
2.2.1. Gestão de identidades 27
2.2.2. Gestão de acessos 28
2.2.2.1. Modelos de Controlo de Acesso 29
Mandatory Access Control (MAC) 30
Discretionary Access Control (DAC) 31
Role Based Access Control (RBAC) 32
Generalized Role Based Access Control (GRBAC) 43
2.3. Conclusões 46
Capítulo 3 Descrição do Problema e Situação Actual 48
3.1. Introdução 48
3.2. Descrição do Problema 48
3.3. Caracterização da situação actual 49
3.4. Conclusões 52
Capítulo 4 Desenvolvimento do Projecto 54
4.1. Introdução 54
4.2. Definição do Modelo 55
4.2.1. Gestão de identidades 55
4.2.2. Gestão de acessos 56
4.3. Implementação do modelo 60
4.3.1. Procedimento de gestão de utilizadores 60
4.3.2. Identidades 61

4.3.3. Acessos 61
4.4. Conclusões 61
Capítulo 5 Conclusões e trabalhos futuros 63
5.1. Conclusões 63
5.2. Trabalho futuro 65
Referências 67
Anexos 70
Anexo I 70
Anexo II 73

Lista de Figuras

Figura 1 - Norma ISO/IEC 27001 18
Figura 2 - Gestão de identidades e acessos 23
Figura 3 - Relação conceitos IAM 24
Figura 4 - Arquitectura de um Sistema IAM 26
Figura 5 - Gestão de Identidades 28
Figura 6 - Modelo MAC 30
Figura 7 - Modelo DAC 31
Figura 8 - Elementos RBAC 33
Figura 9 - Role 33
Figura 10 - Múltipla Role 34
Figura 11 - Básico RBAC 36
Figura 12 - Hierarquia RBAC 36
Figura 13 - Hierarquia Básica 37
Figura 14 - Hierarquia Múltipla 38
Figura 15 - Hierarquia Limitada 38
Figura 16 - Restrições RBAC - Estáticas SOD 40
Figura 17 - Restrições RBAC - Dinâmicas SOD 41
Figura 18 - Simetria RBAC - Estática SOD 42
Figura 19 - Simetria RBAC - Dinâmica SOD 42
Figura 20 - Modelo GRBAC 45
Figura 21 - Gestão de utilizadores actual 50
Figura 22 - Aplicação método identificação 55
Figura 23 - Utilizadores genéricos 56
Figura 24 – Níveis perfilagem 57
Figura 25 - Perfil Estruturas Centrais 57
Figura 26 - Perfis Lojas 58
Figura 27 - Perfil Temporário 59
Figura 28 - Gestão DAC centralizada 61
Figura 29 - Solução ORACLE 66
Figura 30 - Áreas de negócio 70
Figura 31 - Perfil Corporativo 71
Figura 32 - Organigrama DSI 72
Figura 33 - Domínios ISO/IEC 27001 74
Figura 34 - Modelo PDCA 76
Figura 35 - Core Publications ITIL 78

Lista de tabelas

Tabela 1 - Estrutura do relatório 21
Tabela 2 - Níveis RBAC 43
Tabela 3 - Relação UNIFO - RH 50
Tabela 4 - Universo Unifo 51
Tabela 5 - RH e UNIFO 51
Tabela 6 - Valores finais estado actual 51
Tabela 7 - Valores finais 51
Tabela 8 - Matriz RBAC 59
Tabela 9 - Valores actuais da Implementação 62
Tabela 10 - Dominios detalhados ISO/IEC 27001 74
Tabela 11 - Modelo PDCA 77

Abreviaturas e Símbolos

COBIT - Control Objectives for Information and related Technology

CRM - Customer Relationship Management

DAC - Discretionary Access Control

DSI - Departamento de Sistemas de Informação

ERP - Enterprise Resource Planning

IAM - Identiy and Access Management

ISO - International Organization for Standardization

LDAP - Lightweight Directory Access Protocol

MAC - Mandatory Access Control

MC - Modelo e Continente

RBAC - Role Based Access Control

RH - Recursos Humanos

SSO - Single Sign On

SGSI - Sistemas de Gestão de Sistemas de Informação

UNIFO – Sistema de Informação das lojas

check-in - Processo de entrada de um colaborador

check-out - Processo de saída de um colaborador

Front - Office - Parte da aplicação à qual o utilizador final tem acesso

Operations - Uma acção ou operação sobre determinado recurso

Object - Um objecto do sistema, pode ser um recurso qualquer da rede

Password - senha de acesso

Permission – Permissões

Role - Regra, conjunto de permissões

Username - nome de utilizador

User - Utilizador

Workflow - fluxo de trabalhos, tarefas de determinado processo

Capítulo 1

Introdução

A informação é um dos activos mais importantes nas organizações que é essencial no desenrolar dos seus negócios e consequentemente, necessita ser adequadamente protegida de acordo com a sua classificação.[FNL09] Isto torna-se especialmente importante dado que os ambientes de negócio estão cada vez mais interligados e dispersos geograficamente. Como resultado desta crescente interligação, a informação está agora exposta a um número cada vez maior e a uma ampla variedade de ameaças e vulnerabilidades. O dinamismo do mercado ao qual as empresas estão sujeitas actualmente, obriga acessos a informação de extrema confidencialidade, que não estando devidamente protegida, uma oportunidade de mercado, ou mesmo um nicho de mercado pode ser perdido e explorado por uma organização concorrente.

Quando se fala em segurança da informação, estamos a referir-nos a tudo, cultura, procedimentos, regras, normas, sistemas de informação, etc. [CarnFCA] Os sistemas de informação que estão associados às organizações, devem ter mecanismos de segurança de forma a manter e proteger a informação pela qual é responsável.

Com o crescimento das empresas, não é só a informação que aumenta, os sistemas de informação ou os colaboradores também incrementam de acordo com as necessidades das organizações. As empresas adquirem diversos sistemas como ERP's, CRM's, sistemas operativos e outras aplicações. São gerados vários repositórios de utilizadores para autenticação e autorização nos mesmos, incorrendo assim numa administração descentralizada e susceptível a erros. Utilizadores que deviam estar sem permissões em vários sistemas, recursos ou aplicações após cessação ou alteração de funções dentro da organização podem continuar com acesso activo o que abrirá oportunidades de fraude.

A maioria dos danos que podem recair sobre um SI são ao nível dos dados e da informação, quando acedidos por pessoas não autorizadas. Motivadas por acessos mal atribuídos, identificadores genéricos, partilhados e todo um ciclo de gestão de identidades e acessos ineficiente e por vezes, não existente.

Com foco especial nos sistemas de informação, a segurança a nível de gestão de identidades e acessos torna-se uma prioridade em qualquer organização.

Numa perspectiva de aumento de segurança, uma definição estratégica de gestão de identidades e acessos deve ser desenvolvida, acompanhada com a implementação de um correcto e adequado modelo de gestão de identidades e acessos para obter uma gestão de utilizadores eficaz reduzindo toda a complexidade envolvida. Apresenta-se assim a necessidade de restringir acessos, assegurar que a utilização dos dados por parte do utilizador sigam os procedimentos correctos, que a informação esteja disponível e somente disponível a quem tem autorização para aceder à mesma e esta seja recebida integralmente.

O ponto inicial e mais prioritário na maioria dos SI é a identificação[1] dos utilizadores, verificação e confirmação dos seus níveis de acesso, autorização e finalmente a autenticação[2] da sua identidade. Estes dois conceitos encaixam na definição de um modelo de gestão de identidades e acessos.

A nível de autenticação do utilizador, existem várias técnicas de forma a garantir perante o sistema que é quem diz ser.

A nível de autorização, a gestão de acessos deve seguir processos de gestão de utilizadores, revisão periódica de acessos e procedimentos de onboarding[3] e offboarding[4].

As formas de acessos aos dados e à informação devem seguir vários modelos de controlo de acesso, essa escolha deve ser feita de acordo com o cenário onde se pretende implementar um sistema que faça essa gestão.

Uma das formas de acesso pode ser controlada através da função ou papel do utilizador na organização. Por exemplo, os direitos de acesso atribuídos a um líder de projecto e a um programador diferem. Assim, estamos perante uma atribuição de direitos de acesso de acordo com a função que o colaborador desempenha na organização. Todos estes direitos de acesso devem seguir determinadas regras e algumas até são limitadas.

Acessos de acordo com a localização e horários também são atribuídos. Por exemplo, situações em que o acesso é permitido em determinadas horas ou dias da semana. [CarnFCA]

Já as modalidades de acesso estão relacionadas com o tipo de permissões que o utilizador tem sobre os recursos e informação do SI. Estas podem ser, leitura, escrita, execução, criação, pesquisa ou todas as anteriores.

O auxílio de software de controlo de acesso torna-se necessário e revela-se de grande utilidade dado que implementa mecanismos para validações de identidades, relatórios, rotinas de segurança e gestão de acessos.

A implementação destas soluções de gestão de identidades e acessos precisam de uma análise inicial acerca da situação actual da organização. Para perceber como são reconhecidas as identidades, quais os identificadores e como os acessos são e estão atribuídos actualmente. Cada organização tem requisitos e necessidades diferentes.

[1] Momento em que o utilizador se dá a conhecer ao SI
[2] Análise e verificação que o SI realiza relativamente a uma identificação
[3] Processo de entrada de um colaborador
[4] Processo de saída de um colaborador

1.1. **Contexto/enquadramento**

A segurança de informação, tem como seus principais objectivos garantir 3 princípios:

- **Confidencialidade** - assegurar que a informação é acedida apenas pelas pessoas autorizadas.
- **Disponibilidade** - assegurar que os utilizadores autorizados têm acesso à informação sempre que dela necessitarem.
- **Integridade** - salvaguardar a fiabilidade e a totalidade da informação.

Boas práticas de mercado e normas internacionais de segurança da informação devem ser adoptadas. Entre as várias destacam-se as seguintes: ISO/IEC 27001 que é uma norma que faz uma abordagem ao processo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o Sistema de Gestão de Segurança de Informação (SGSI.)

Control Objectives for Information and related Technology (COBIT), diponibiliza uma *framework* para manter práticas e processos que estão relacionados com a infra-estrutura de sistemas, redes e dispositivos utilizados pela empresa.

E por fim, Information Technology Infrastructure Library (ITIL), trata-se de um guia de boas práticas para a gestão de serviços em TI. Este guia promove uma gestão mais focada no cliente e na qualidade dos serviços de TI. Ver mais detalhes das normas no anexo II.

A norma ISO/IEC 27001 apresenta uma estrutura baseada em onze domínios, cada um com os seus objectivos que deverão usar um ou mais controlos para os atingir. Os domínios[5] são ilustrados na seguinte figura.

[5] Ver Anexo II

Figura 1 - Norma ISO/IEC 27001

O foco desta investigação incide sobre o domínio, **Controlo de Acessos**, que tem como principais objectivos, assegurar acessos a utilizadores autorizados, e prevenir acesso não autorizado a sistemas de informação.

Esta dissertação foi realizada na SONAE[6] na área de retalho.

1.2. **Motivação e objectivos**

A Segurança da Informação é uma área que ultimamente tem merecido uma atenção especial por parte das organizações. Neste sentido, vários projectos exigentes e de dimensões consideráveis têm presença no dia-a-dia das empresas.

Dada a complexidade da área e aplicação em todos os sectores das organizações, a possibilidade de efectuar uma investigação mais focada e na criação de soluções diferentes torna-se um desafio constante. Mais especificamente, a criação de uma solução viável para a resolução de um problema em particular com base em fundamentos e conceitos teóricos, torna-se essencial para uma investigação teórica e prática com sucesso. A possibilidade desta incidir sobre um projecto de grande dimensão mas ainda numa fase embrionário revela-se de uma importância elevada, na medida em que, a continuidade do projecto é uma certeza assim como o seu amadurecimento durante os próximos anos.

Os principais objectivos são:

- Aumentar a segurança;
- Reduzir a complexidade de gestão dos utilizadores

[6] Ver anexo I

- Automatizar o processo de gestão de utilizadores
- Definir uma estratégia para a gestão de identidades e acessos

Aumentar a segurança

- Atribuição correcta de acessos, para evitar acessos indevidos à informação.
- Mecanismos de autenticação eficazes, de modo a certificar a identidade.
- Revisões periódicas a nível de acessos.
- Registos das transacções efectuadas pelos utilizadores
- Procedimentos de segurança.

Reduzir complexidade de gestão de utilizadores

- Gestão de identidades que trate de toda a informação relacionada com a identificação do utilizador, funcionalidades de criação, modificação, suspensão e re-certificação de utilizadores.

Automatizar o seu processo de gestão de utilizadores

- Criação de mecanismos que quando é efectuada qualquer alteração essa seja propagada pelos vários sistemas.
- Workflows de aprovação
- Inactividade de utilizadores
- Gestão de passwords

Definição estratégica da gestão de identidades e acessos

- Definição de regras para criação de utilizadores
- Regras para atribuição de acessos
- Formas para facilitar a identificação das identidades e dos acessos dos utilizadores.

Abordagem

Análise e estudo dos I&AM

Inicialmente será feita uma análise às soluções de gestão de identidades e acessos. Nesta análise serão efectuados estudos teóricos a nível de identidades e de controlo de acessos tendo em conta os seus modelos.

Definição de políticas e procedimentos de segurança

Definição de políticas e procedimentos de segurança que determinam a importância da informação e como esta deve ser protegida, disponibilizada e tratada.

Tipificação dos perfis funcionais e aplicacionais

Criação de perfis aplicacionais de acordo com as funções operacionais dos colaboradores.

Definição do modelo de gestão de identidades e acessos no Sistema UNIFO

O modelo deve ser definido de forma a garantir uma gestão optimizada e segura dos utilizadores e dos acessos. Com a definição de regras de gestão de utilizadores e acessos controlados através dos vários modelos de controlo de acessos existentes actualmente.

Implementação do modelo no sistema UNIFO

Implementação do modelo no sistema UNIFO, aplicando as novas regras que o modelo define.

Revisão e limpeza dos utilizadores no sistema UNIFO

A revisão e limpeza dos utilizadores no sistema UNIFO torna-se inevitável de forma a adicionar e implementar as novas regras do modelo criado anteriormente. Neste contexto, todos os utilizadores serão revistos.

1.3. **Estrutura da Dissertação**

Este relatório de dissertação encontra-se organizado em 5 capítulos, a descrição do conteúdo de cada um deles está descrito na seguinte tabela.

Tabela 1 - Estrutura do relatório

Nome do Capítulo	Descrição
Capítulo 1	Capitulo presente composto por uma introdução, motivação e o contexto da dissertação e seus objectivos.
Capítulo 2	São apresentados conceitos teóricos a nível de gestão de identidades e acessos e modelos de controlo de acesso. No fim são apresentadas as conclusões do Capítulo.
Capítulo 3	Neste Capítulo é feita uma descrição do problema, análise detalhada com o levantamento de informações do estado actual e apresentadas as conclusões do Capítulo.
Capítulo 4	É definido o modelo de gestão de identidades e acessos no UNIFO e sua implementação. No final são apresentadas as várias conclusões do Capítulo acompanhadas com os resultados da implementação.
Capítulo 5	Este é o último Capítulo onde são referidas as conclusões principais de todo projecto e trabalho futuro.

Capítulo 2

Gestão de Identidades e Acessos

2.1. **Introdução**

Quando se fala numa solução para gerir eficazmente identidades e acessos, está-se a falar de todo um processo que envolve dois conceitos principais são eles, identidades e acessos. Cada um deles tratado separadamente, no entanto, só fazem sentido quando relacionados um com o outro.

A Gestão de Identidades relaciona-se com todo o ciclo de vida de um utilizador na organização. Todas as informações de identificação dos utilizadores estão incluídas nesta gestão.

A Gestão de Acessos relaciona-se com o controlo de acessos dos utilizadores após a sua autenticação no sistema. Esta gestão trata de todos os acessos que os utilizadores têm sobre os recursos da empresa, o que pode fazer com eles e durante quanto tempo.

Mais detalhes são apresentados no seguinte esquema:

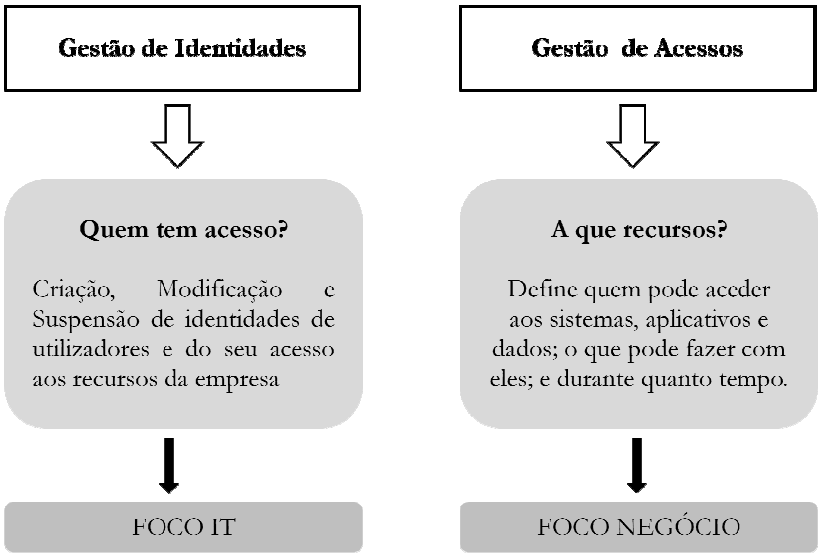

Figura 2 - Gestão de identidades e acessos

2.2. **Gestão de Identidades e Acessos (IAM)**

Um sistema de IAM trata-se de um processo complexo que consiste em várias políticas, procedimentos, actividades e tecnologia que requerem coordenação com muitos grupos da organização como recursos humanos e departamento de TI.[GartnerPA08] Os conceitos envolvidos neste sistema de gestão de identidades e acessos, fundamentalmente servem para responder a questões como:

- Quem tem acesso e a que informação?
- Os acessos atribuídos são apropriados à função que o colaborador desempenha na organização?
- Os acessos e as actividades são monitorizados, registados e reportados apropriadamente?

Com um IAM robusto permite que a organização obtenha várias informações e respostas às perguntas anteriores. Dado que, tem toda a informação de uma identidade e também a gestão dos acessos aos recursos e aplicações.

Também é possível saber se os acessos atribuídos estão de acordo com a sua função na empresa e se os acessos possibilitam agregação de direitos. Ou seja, incompatibilidade com outras funções.
O último ponto refere-se ao facto que com um sistema de IAM há a possibilidade de todo o fluxo de informação ser devidamente documentada, registada, monitorizada e reportada apropriadamente.

Este processo deve ser desenhado de forma a iniciar, modificar, registar e terminar identificadores específicos associados com cada conta, humanos ou não humanos. Como resultado deve ser desenhado de forma a incorporar as aplicações que o utilizador precisa ter acesso e como o identificar (caso sejam aplicações diferentes são associadas com o utilizador). [REY07] A forma como os vários conceitos de um IAM se relacionam, estão apresentados na seguinte figura.

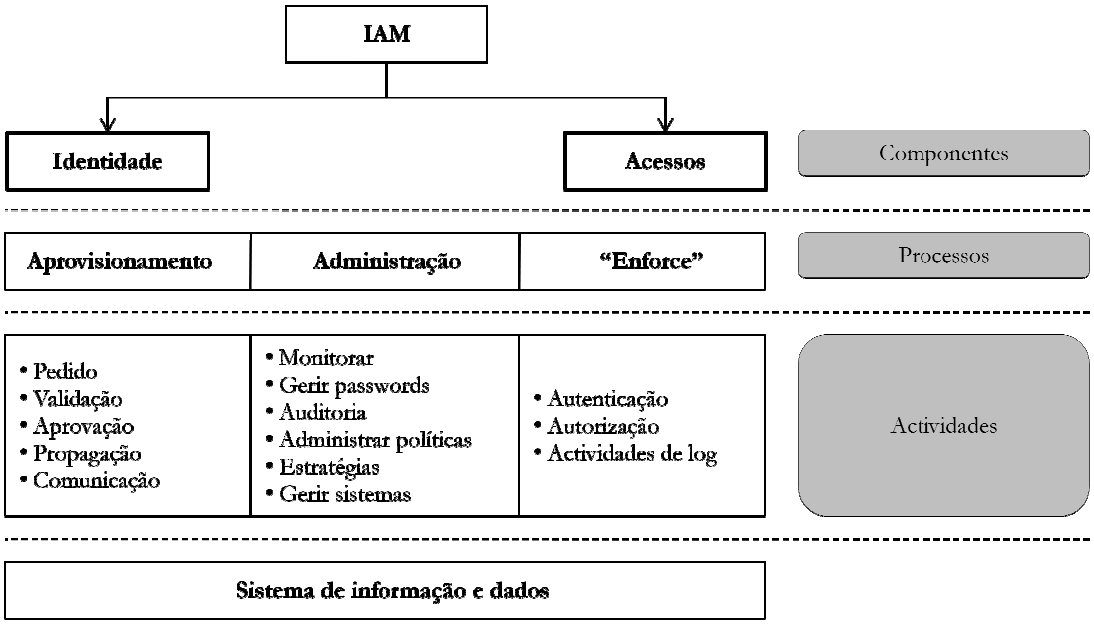

Figura 3 - Relação conceitos IAM

Identidade

Trata-se de um conjunto de atributos que identificam unicamente uma entidade[7] na rede.
O conceito de identidade não se aplica só aos humanos, aplica-se a todos os recursos do sistema de forma a identificá-los. [CernPace08]

[7] Uma entidade numa rede pode ser de vários tipos, dispositivo, uma aplicação, um utilizador ou outro tipo qualquer de recurso que necessite de interagir com toda a rede ou todo o sistema.

Acessos

Contém informação que apresenta os acessos e direitos de acesso que determinada identidade possui, ou tem privilégios para aceder aos recursos.

Aprovisionamento

O aprovisionamento está relacionado com o ciclo de vida de uma identidade, desde a sua criação, alteração, validação, aprovação, remoção, propagação e comunicação. Este processo varia com as necessidades da organização.

Administração

Este é um processo que permite toda a administração do sistema de IAM, desde monitorizar, gerir *passwords*, auditorias, administrar políticas, estratégias e gerir sistemas.

Enforcement

O *enforcement* dos direitos de acesso primeiramente ocorre através de processos ou mecanismos automatizados. [REY07] Inclui a **autenticação**, **autorização** e ***actividades de log*** das identidades que são usadas nos sistemas de TI na organização.

Autenticação - Serviço que garante a identificação inequívoca de uma pessoa que está ligada ao sistema de informação. A identificação deve apontar para uma base de dados onde todos os potenciais utilizadores do sistema de informação possam ser identificados. Isto significa que todo o processo, modificação e acção feita no sistema de informação tem uma "*tag*" com o nome da pessoa que está por detrás da acção pedida. São muitas as tecnologias que implementam um serviço de autenticação. As mais tradicionais são baseadas no par *username/password*, onde a password é secretamente comunicada durante o processo inicial de validação de identidade. Mas também existem outros métodos de validação de identidade, baseados em certificados electrónicos, tokens, reconhecimento biométrico, etc. [CernPace08] [iSMGSS09].

Autorização - Este serviço, garante que aquela determinada pessoa autenticada tem as permissões adequadas para desempenhar uma função específica ou aceder a determinado recurso no sistema de informação.

Actividades de log - Este serviço regista todas as transacções feitas no sistema de informação. Aqui é possível saber quem, quando, onde e ao que, determinada identidade acedeu no passado. Em alguns casos, até é permitido o *rollback* de algumas acções. Com este serviço é possível verificar se houve algum tipo de fraudes. São guardadas todas as operações efectuadas por esta conta no sistema de informação. Logicamente que não pode

ser feito o *rollback* em todas as transacções, situações que tiveram impacto no Mundo real. Por exemplo, pagamentos indevidos, fugas de informação confidencial, etc. [CernPace08] [Orac03]

Arquitectura IAM

A nível de arquitectura de um sistema de IAM, este permite a integração de várias informações dos vários sistemas da empresa. Como vemos na seguinte figura, a gestão de identidades e acessos e o Single Sign-On[8] são centrais. Os conectores fazem as ligações dos vários recursos ou sistemas da empresa. Podemos verificar que com um sistema de IAM, a informação é adquirida dos recursos humanos, e posteriormente é feita a gestão da identidade dos seus acessos. [TechIAM07] Permitindo assim uma gestão central de utilizadores com a ligação aos vários sistemas da empresa.

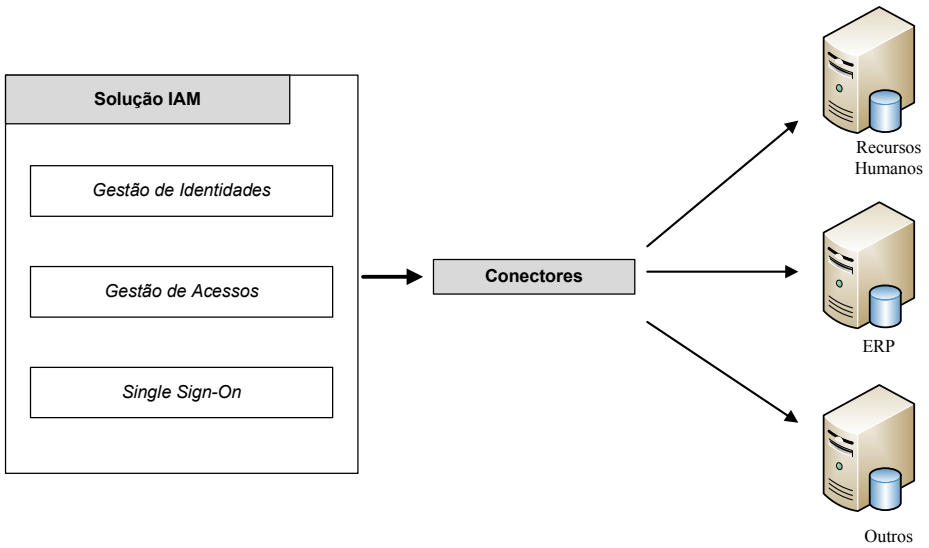

Figura 4 - Arquitectura de um Sistema IAM

[8] Login único para aceder aos vários recursos da empresa

2.2.1. GESTÃO DE IDENTIDADES

Gestão de Identidades

A gestão de identidades pode ser definida como a informação ou o conjunto de fluxos que são suficientes, para identificarem quem é a entidade que tem acesso ao sistema de informação. Trata-se assim, de um processo pelo qual através de uma aplicação as identidades dos utilizadores são definidas e geridas no ambiente da organização, ou seja, como é gerido todo o seu ciclo de vida (criação, suspensão, alteração e remoção). Mais especificamente são tratados os seguintes pontos:

- Identidades dos utilizadores são provisionadas e coordenadas
- Aprovisionamento da conta do utilizador é automatizado
- Regras dos utilizadores
- Administradores delegam responsabilidades
- Os utilizadores podem alterar algumas preferências e *passwords*
- Os utilizadores têm acesso SSO (Single Sign On)

Um sistema integrado de gestão de identidades ajuda as empresas no desempenho dessas operações eficientemente. [Orac03]

Na tentativa de centralizar a administração dos utilizadores, onde cada aplicação, sistema ou recurso possui um determinado interface de administração para o registo de utilizadores, a gestão de identidades visa uma **administração centralizada** e tecnicamente automática, ou seja, só com uma interface administrativa com um repositório central de utilizadores (Metadirectório), que automaticamente ou via aprovações de *workflow*, replica (aprovisiona) dados dos utilizadores para as demais bases de autenticação utilizados pelos recursos disponíveis.

Principais componentes de um sistema de gestão de identidades

- Serviço de directórios, seguro e escalável para guardar e gerir informação do utilizador
- Uma *Framework* de aprovisionamento que pode ser ligado com um sistema de aprovisionamento empresarial, tais como com a aplicação de recursos humanos ou operando mesmo em modo *standalone*
- Plataforma de integração de directórios que activa a conexão do directório do gestor de identidades com o directório específico da aplicação
- Um modelo de autenticação em tempo de execução
- Um modelo de administração delegado que permite/activa que o administrador selectivamente delegue direitos de acesso a um administrador de uma aplicação individual, ou directamente a um utilizador

Fluxo Funcional

Com um sistema de gestão de identidades, várias potencialidades podem ser exploradas, um exemplo de um fluxo funcional está apresentado na figura em baixo, onde demonstra a entrada de um colaborador e todo o seu processo de gestão. Ou seja, a informação relativa ao novo colaborador é enviada ao departamento dos recursos humanos, que por sua vez cria um novo registo com a informação desse colaborador e envia essa informação para o serviço de gestão de identidades. Neste serviço, são aplicadas as várias regras, políticas, workflow e aprovisionamento. No aprovisionamento, as contas são criadas nos vários sistemas de acordo com as informações que foram atribuídas ao colaborador.

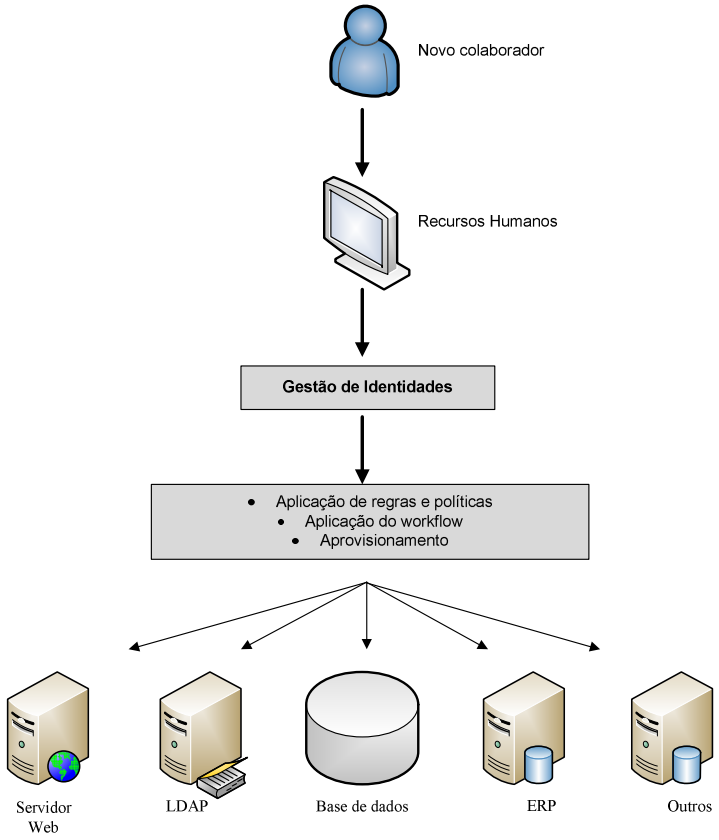

Figura 5 - Gestão de Identidades

2.2.2. GESTÃO DE ACESSOS

A gestão de acessos está relacionada com o processo de atribuir e conceder permissões de acesso aos recursos da empresa, após a respectiva solicitação. Contém a informação que descreve o que o utilizador final pode fazer sobre os recursos do sistema de informação. Essas informações, consistem em associação de direitos de acesso, quem é a

entidade que pode aceder e a que recursos. Estas associações podem ser *time-dependent*[9] ou *location-dependent*[10].[CernPace08].

No controlo de acessos de forma a garantir mais segurança, é seguido um conceito denominado de **princípio de acessos mínimos** que consiste em garantir que não são atribuídos mais acessos que os necessários para desempenhar a sua função. Para garantir o privilégio mínimo de acessos, é necessário perceber bem qual a função do colaborador para criar o conjunto de permissões para o desempenho dessa mesma função. No entanto, as formas como são controlados esses acessos podem ser diferentes. Neste contexto, são abordados os seguintes modelos de controlo de acesso, Mandatory Access Control(MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC) e Generalized Role Based Access Control (GRBAC). Cada um deles é aplicado em situações distintas.

Direitos de acesso (*Entitlements*)

Trata-se de uma colecção ou conjunto de direitos de acesso necessários para executar determinada função. A informação dos direitos de acesso, permite aos utilizadores executarem várias transacções a vários níveis. Alguns exemplos são, alterar, criar e ler determinada informação.

Gestão de direitos de acesso

Permite gerir as permissões de acesso nas contas dos utilizadores. Contudo, a organização deve efectuar as revisões periódicas para detectar situações em que os utilizadores agregam ou acumulam direitos de acesso, que possa abrir espaço a falhas de segurança. As separações de direitos de acesso têm que prevalecer. São as denominadas *Separation of Duties* (SOD). [SSW]

2.2.2.1. Modelos de Controlo de Acesso

É sempre necessário garantir a segurança, mesmo quando em ambientes dinâmicos, de acordo com este cenário torna-se necessário a utilização de alguns modelos de acesso. [CSI08]. São quatro os modelos apresentados, cada um com diferentes características para utilização em cenários distintos. Um modelo MAC[11], consiste em atribuir classificações diferentes aos vários recursos do sistema e as entidades só podem aceder a esses recursos caso tenham autorização ou estejam habilitados a aceder a esse tipo de informação, DAC[12] um modelo onde os acessos podem ser atribuídos livremente e individualmente, RBAC[13] é um modelo orientado à função onde são associados grupos de

[9] Determinada hora ou dias da semana/mês
[10] De acordo com a localização geográfica
[11] Mandatory Access Control
[12] Discretionary Access Control
[13] Role Based Access Control

utilizadores e GRBAC[14] um modelo também orientado à função mas depende de algumas variáveis externas (tempo e local).

Mandatory Access Control (MAC)

O modelo MAC consiste em classificar os vários tipos de informação existentes numa organização. As entidades só podem aceder a essa informação, caso tenham autorização ou estejam habilitados para aceder à mesma.

Este modelo utiliza determinadas disposições ou regras de segurança que são aplicadas a todos os objectos, aplicações e recursos variados. [Crue].

Como exemplo explicativo, considerem-se 3 tipos de informação com a seguinte classificação, *sensitive*, *secret* e *confidential.* Podem eventualmente haver mais categorias, depende de organização para organização. Supondo que um utilizador (Utilizador1) só tem permissão para aceder a informação do tipo *sensitive.* Este utilizador, nunca em nenhum momento pode aceder a outra categoria de informação que não esteja referenciada como *sensitive.* A seguinte figura ilustra um exemplo da utilização do modelo MAC com 3 utilizadores, cada um deles com acesso a classificação de informação diferente.

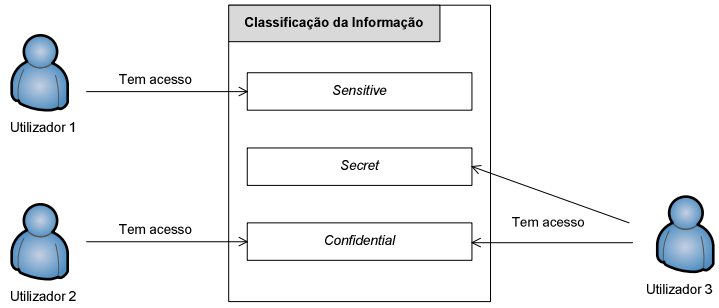

Figura 6 - Modelo MAC

Com a atribuição de permissões de acesso de acordo com a classificação da informação o MAC torna-se assim capaz de lidar com o facto de efectuar uma separação de funções. Algumas implementações deste modelo incluem uma estrutura hierárquica na classificação da informação, neste exemplo considere-se a seguinte hierarquia, *Confidential*, *Secret*, *Sensitive* do nível mais alto da hierarquia para o mais baixo, respectivamente.

Isto significa, um utilizador que tenha acesso a informação classificada como *secret*, tem acesso a dados classificados como *secret*, obviamente, e também classificados como *sensitive*. No entanto este modelo alerta para uma situação, onde a confidencialidade se

[14] Generalized Role Based Access Control

torna muito importante como em departamentos militares, quem tem acesso a informação de um nível mais alto, por exemplo *confidential* só pode aceder a informação de nível inferior para consulta, impedindo a escrita ou alteração de informações nesses níveis. De forma a evitar que quem tem conhecimento de informação *confidential* não tenha a possibilidade ou permissão para passar essa informação para níveis inferiores da hierarquia.

Discretionary Access Control (DAC)

O modelo DAC é um modelo onde os acessos podem ser atribuídos livremente e individualmente. Trabalha de duas formas, pode funcionar como modelo centralizado ou distribuído.

O modelo centralizado é quando um administrador ou grupos de administradores distribuem acessos aos dados, aplicações ou dispositivos da rede. Todos os pedidos para efectuar qualquer tipo de alterações são reportadas a um único departamento que completa as acções requeridas. O que se pode tornar desvantajoso porque em empresas grandes, pode haver um grande consumo de tempo quando os administradores estão fora do local de trabalho ou se trata de um serviço contratado. [Crue]

Um modelo distribuído, delega responsabilidades para os responsáveis de cada "sistema" podendo ser o gestor, o líder de equipa ou supervisor a atribuir as permissões de acesso aos vários recursos inerentes ao sistema que está à sua responsabilidade a nível de controlo de acessos. A vantagem é que pode haver uma redução no tempo de atribuição de acessos dado que essa gestão se torna local. Em contrapartida, se o sistema for muito grande pode-se tornar muito granular e a distribuição e monitorização de acessos pode ser muito demorada. A figura abaixo ilustra os dois modelos centralizado e distribuído que o modelo DAC permite.

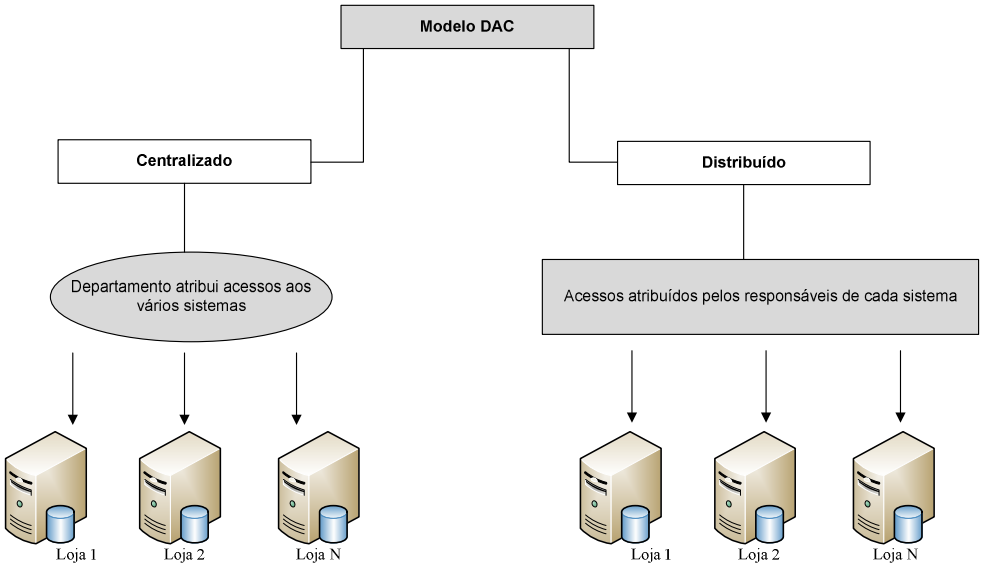

Figura 7 - Modelo DAC

Este modelo permite que se decida os direitos de acesso sobre determinado objecto. Quem o criou pode conceder esses acessos. É um modelo que usa Listas de Controlo de Acesso (ACL) mas estas, são ineficientes no sentido que tipicamente o sistema operativo sabe quem é o utilizador de determinado processo, mas não sabe os direitos que esse utilizador tem sobre os objectos do sistema. ACLs, não são muito utilizadas em sistemas com um número grande de utilizadores ou objectos. [Mat03]

Role Based Access Control (RBAC)

O RBAC é um modelo orientado à função onde as suas decisões a nível de acessos são direccionadas para grupos de utilizadores. [Jun09] [IEEECS07]. Consiste na criação de conjuntos de permissões, são as denominadas *roles* e posteriormente associar a essas *roles* grupos de utilizadores. Evitando assim, atribuição de acessos individuais e as suas complicações que daí advêm em organizações com muitos utilizadores.
Os elementos constituintes deste modelo são utilizadores (*users*), regras (*roles*), permissões (*permissions*), operações (*operations*) e objectos (*objects*). Este modelo tem sido continuamente aperfeiçoado, incrementando novas funcionalidades em cada nível. Desde o seu primeiro modelo base até ao actual, básico-rbac, hierarquia-rbac, restrições-rbac e simétrico-rbac, respectivamente. [SFK] A origem destes vários níveis, consistiram nas necessidades das organizações em conceder e restringir de uma forma adequada as permissões para um utilizador desempenhar a sua ou as suas funções correctamente. Em várias situações a incompatibilidade de funções está presente, obrigando a haver uma separação de direitos ou exclusão mútua de funções. Assim como um limite no número de funções exercidas e por vezes para exercer uma função, esta tem que ser antecedida por outra ou outras funções.

RBAC Elements

O modelo RBAC é constituído por 5 elementos relacionados entre si, são eles *users*, *roles*, *permissions*, *operations* e *objects*. Estes elementos facilitam a administração de acessos aos vários recursos da organização. A forma como estes elementos se relacionam, consiste em utilizadores associados a *roles*, que por sua vez, estas estão associadas a um conjunto de permissões e com essas é possível efectuar determinadas operações sobre os objectos. Este fluxo está ilustrado na seguinte figura.

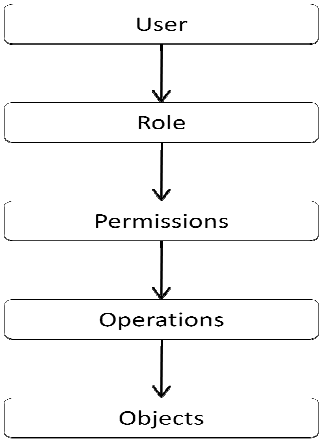

Figura 8 - Elementos RBAC

Users

São os utilizadores do sistema. Tipicamente estes não têm acesso aos recursos, só quando associados a pelo menos uma *role*. Um *user* deve ter uma identificação única no sistema, que com essa informação seja possível saber quem ele é.

Roles

Trata-se de um conjunto de permissões que permitem efectuar transacções sobre determinado ou determinados objectos.

O exemplo de uma *role* está apresentado na figura que se segue, onde estão associados vários membros, utilizadores, e com essa *role* é possível efectuar várias transacções sobre os objectos associados.

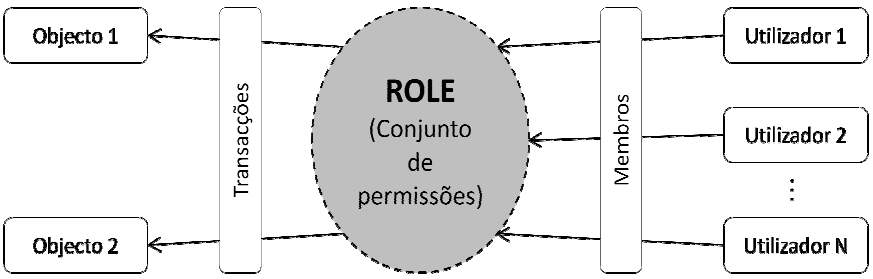

Figura 9 - Role

As roles seguem alguns **princípios básicos** que consistem nos seguintes pontos:

- Atribuição de *roles*
  - Um utilizador só pode efectuar uma determinada transacção se esse utilizador estiver associado a essa *role* que permita efectuar a transacção.
- Autorização de *roles*
  - O utilizador tem que estar autorizado a atribuição dessa *role*.
- Autorização de transacções
  - Um utilizador só pode efectuar uma transacção se essa for permitida pela *role* que está activa no utilizador
- Formas de acesso aos objectos
  - Definem as permissões de acesso aos objectos, leitura/escrita. Pode ser útil em situações que é necessário apenas que a informação seja consultada por vários utilizadores, mas só alteradas por alguns.

Relações múltiplas de roles

Uma utilização de *roles* é a possibilidade de estas serem constituídas por outras *roles*, ou seja, não se torna necessário atribuir todas as permissões a uma nova *role*, se determinada *role* já contém esse conjunto de permissões. Basta associar essa *role* à nova *role* a definir. Um exemplo de regras múltiplas é o que está apresentado na figura abaixo, onde a *role* estagiário tem determinadas permissões sobre objectos, mas quem tem associada a *role* coordenador, tem as permissões da *role* coordenador e estagiário. O mesmo sucede com a *role* Director, tem agregadas as roles estagiário e coordenador, tendo todas as permissões que essas *roles* permitem. [FK92]

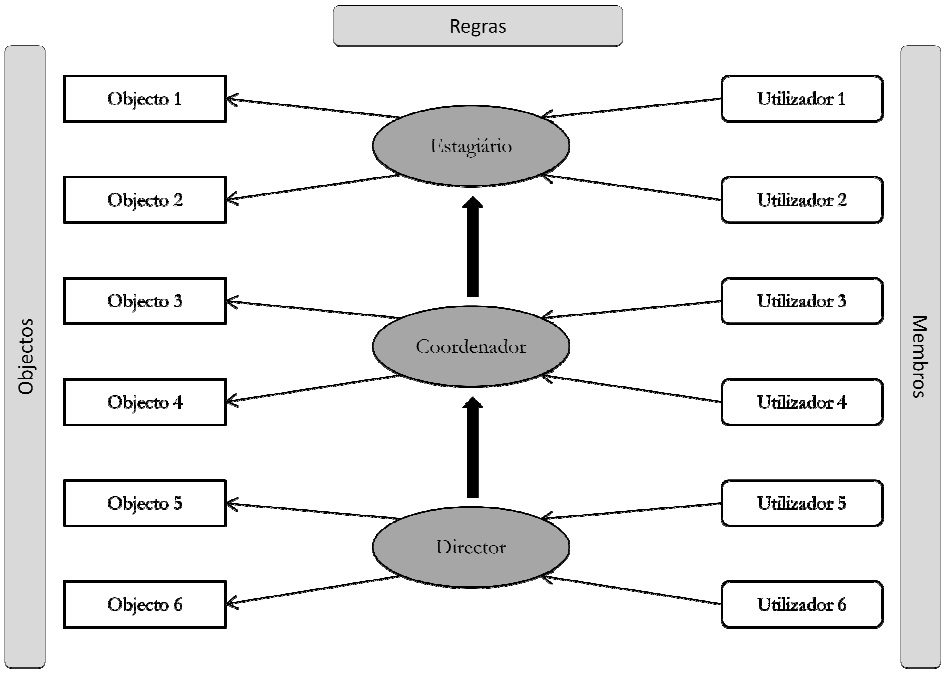

Figura 10 - Múltipla Role

Estas *roles* podem ser organizadas de acordo com a hierarquia da organização. Esta relação **role-role** pode ser de dois tipos exclusão mútua ou herança. Exclusão mútua, quando se pretende que a determinado grupo de utilizadores seja atribuída uma *role*, e não possa ser atribuída outra *role* que permita obter acessos a informação que não seja cruzada. Herança, uma determinada *role* herda outras *roles*.

Permissions/Operations

As *permissions* e *operations* são dois elementos completamente distintos, mas directamente relacionados um com o outro. Ou seja, só é realizada uma determinada operação sobre um objecto se existir permissão para a realizar por parte do utilizador. Neste contexto, as operações tornam-se de um nível mais baixo que as permissões porque estas apresentam um certo domínio sobre as operações. Por exemplo, um utilizador que tenha uma *role* atribuída e que essa *role* contenha permissões para impressão, uma operação possível é imprimir.

Objects

Os objectos estão associados a dados ou informação. Cujo utilizador ou outra entidade queira aceder e tenha permissões para esse fim. De forma a realizar a operação que pretende sobre esse objecto. Vários exemplos de objectos possíveis são, ficheiros, impressoras, outros dispositivos de rede, aplicações ou outro qualquer recurso do sistema.

Níveis RBAC

O modelo RBAC teve várias evoluções onde em cada nível foram incrementadas novas funcionalidades. Como se trata de um modelo orientado à função, novas necessidades emergiram obrigando ao incremento dos vários níveis. [SFK]

RBAC usa 4 níveis em que cada um deles incrementa funcionalidades diferentes são eles:

- Básico RBAC
- Hierarquia RBAC
- Restrições RBAC
- Simétrico RBAC

Básico RBAC

Este é o nível mais básico do modelo RBAC em que os utilizadores estão associados a *roles* sem que estas estejam limitadas. Utilizadores estão associados a *roles* e *roles*

associadas a várias permissões (ver figura em baixo). Estas relações podem ser todas de **muitos para muitos**. Por exemplo, vários utilizadores podem estar associados a várias *roles*. Este modelo opõe-se assim à questão que um utilizador activo só poder ter uma *role* associada, uma solução apresentada por muitos produtos que utilizam o modelo RBAC.
Neste nível não são exploradas todas as funcionalidades possíveis de atribuição de *roles* a grupos, mas sim o básico.

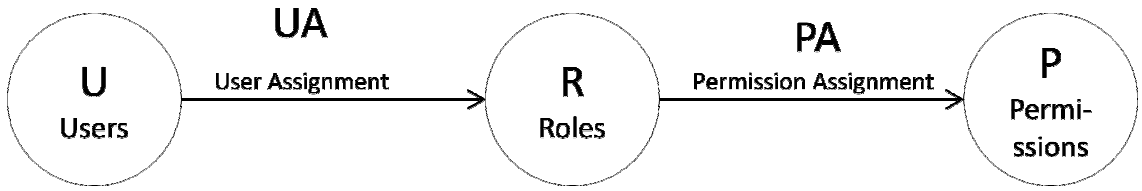

Figura 11 - Básico RBAC

Hierarquia RBAC

A hierarquia de *roles* é uma forma natural de reflectir as posições hierárquicas da organização. [NIST09] Desta forma, respeitam as responsabilidades atribuídas a cada cargo e as permissões que têm sobre membros de nível mais baixo na hierarquia. No entanto, o modelo hierárquico pode assumir várias formas a nível de *roles*, pode ser uma hierarquia **básica**, **múltipla** ou **limitada**. A atribuição de permissões às *roles* e a associação de utilizadores seguem o esquema apresentado na figura abaixo. Neste caso, as *roles* seguem uma hierarquia ao contrário do modelo básico em que não existia nenhuma organização neste sentido. [SFK] [SCFY96].

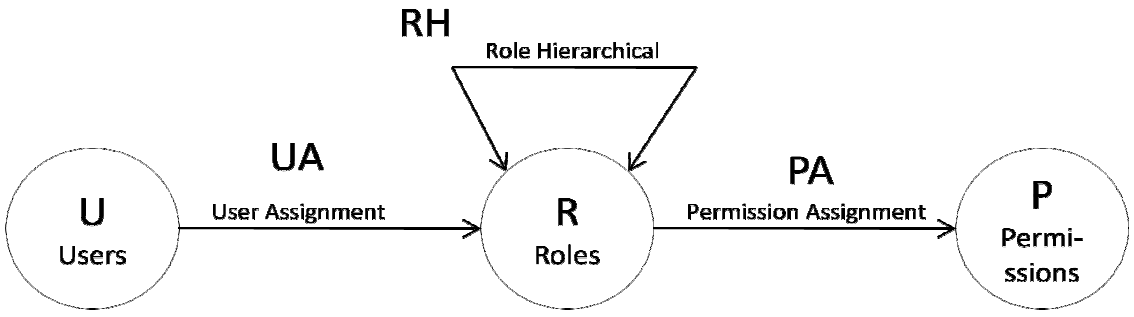

Figura 12 - Hierarquia RBAC

Básica

Consiste numa hierarquia tradicional, ou seja, há uma herança de *roles* e um utilizador que esteja associado a essa *role*, tem os acessos de *roles* inferiores na hierarquia. Um exemplo está apresentado na seguinte figura.

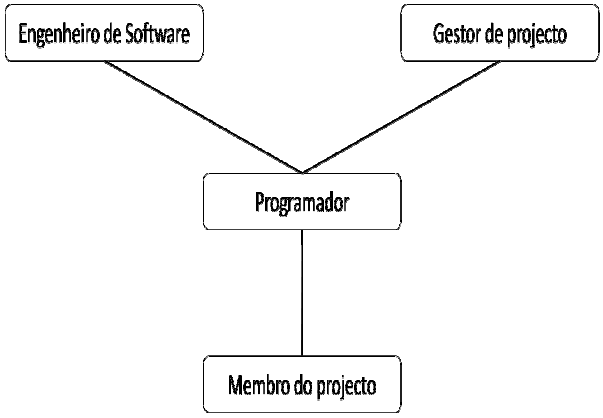

Figura 13 - Hierarquia Básica

A *role* "Engenheiro de Software e Gestor de Projectos" são *roles* diferentes, mas têm os mesmos acessos que as *roles* "Programador" e "Membro de projecto".

Múltipla

A herança múltipla que pode ser útil em algumas situações, mas não permite a exclusão mútua de *roles*. Imaginando agora uma situação em que há várias *roles*, "Engenheiro de Testes" e "Programador" ambas herdam as permissões de "Membro de Projecto". Mas, "Supervisor do Projecto" tem herança múltipla ou seja, tem as permissões de "Engenheiro de Testes" e da *role* "Programador". Esta situação é ilustrada na seguinte figura.

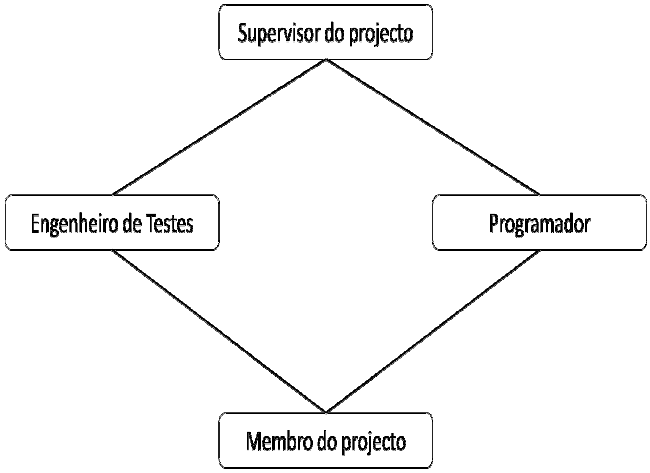

Figura 14 - Hierarquia Múltipla

Quando existem *roles* diferentes mas estas devem ser supervisionadas, a aplicação de uma herança múltipla torna-se uma boa solução.

Limitada

A hierarquia na situação anterior permitia que o Supervisor do Projecto tivesse as mesmas permissões que são atribuídas ao Programador e ao Engenheiro de testes. No entanto, por vezes convém limitar esta herança, ou seja, pretende-se que o engenheiro de testes tenha acesso a outro tipo de recursos que não sejam do interesse do Supervisor do projecto. Nesse caso é criada uma segunda regra baseada na primeira, são as denominadas **private roles** e são mutuamente exclusivas. Na seguinte figura esta situação ocorre com as *roles* Engenheiro de testes' e Programador'.

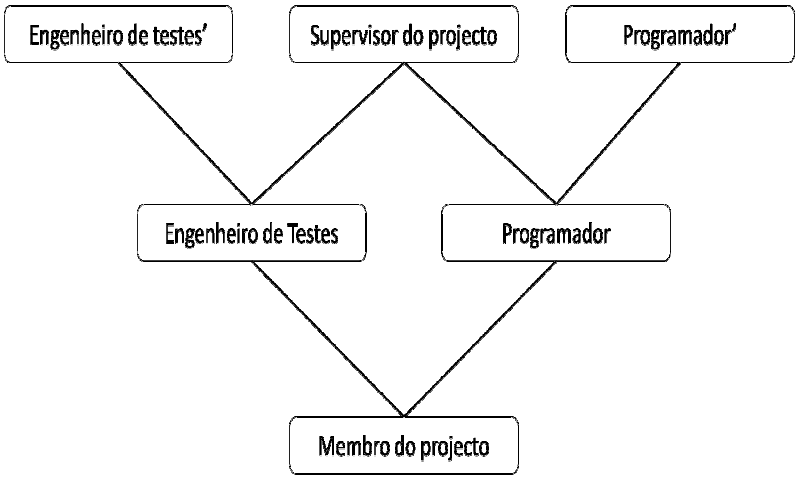

Figura 15 - Hierarquia Limitada

O caso das *roles* Engenheiro de testes e Programador servem como meio de partilha de permissões para o Supervisor do projecto.

Concluindo, o desenho hierárquico permite uma **administração fácil** através da atribuição dos direitos de acesso aos seus subordinados de acordo com a hierarquia da organização. Assim, os utilizadores de nível inferior obtêm os acessos directamente concedidos pelo seu superior hierárquico.

Uma das vantagens desta estratégia de definição de *roles* de uma forma hierárquica é que reduz significativamente o número de *roles* desde que este processo de atribuição de direitos de acesso seja devidamente combinado com a progressão dos direitos de acesso. Outro dos benefícios com a utilização hierárquica é que múltiplas *roles* podem ser associadas umas com as outras de forma a permitir uma melhor funcionalidade para o utilizador final. [NIST03]

Restrições RBAC

Este nível do RBAC capacita o modelo com a utilização de restrições de *roles*. Estas restrições incluem os conceitos de **cardinality**, **prerequisite role** e **separation of duties.**

Cardinality

Cardinality define-se como uma restrição que indica que determinada *role* só pode ter um determinado número máximo de *roles* associadas. Tem dificuldades de implementação.

Prerequisite role

Esta restrição é baseada na competência, em que a determinado utilizador não pode ser atribuído uma *role* B, sem que já tenha sido atribuída a *role* A. Um exemplo, é um colaborador que tenha atribuída uma *role* para desenvolver determinado projecto, posteriormente pode ser-lhe atribuída uma *role* para efectuar os testes. Esta restrição é boa para garantir consistência.

Separation of Duties (SOD)

Esta estratégia consiste na separação de direitos, ou poderes sobre determinados acessos para evitar situações que permitam vários tipos de fraude. Desta forma, são resolvidas questões de impossibilidade de ter determinadas *roles* atribuídas que sejam incompatíveis e não seja permitida a posse das duas. Normalmente, onde estes tipos de estratégias são muito utilizadas são nos departamentos financeiros das organizações onde existem vários

pagamentos e recebimentos e em alguns casos, um mesmo utilizador não pode ter esses acessos ao mesmo tempo. Só em separado. [SSW]
Nesta separação de direitos de acesso à informação, esta é dividida em 2 partes, **SOD estática** e **SOD dinâmica**.

SOD estática

Separação estática, pode ser facilmente determinada, atribuindo *roles* aos utilizadores onde tenham as transacções definidas. Ou seja, numa situação em que determinado utilizador tenha atribuído uma *role*, não pode ter outra associada caso esta seja incompatível. Pode ver-se na seguinte figura como actuam as restrições estáticas. [FK92]. Onde se ilustra que as restrições são aplicadas aos utilizadores respeitando as restrições.

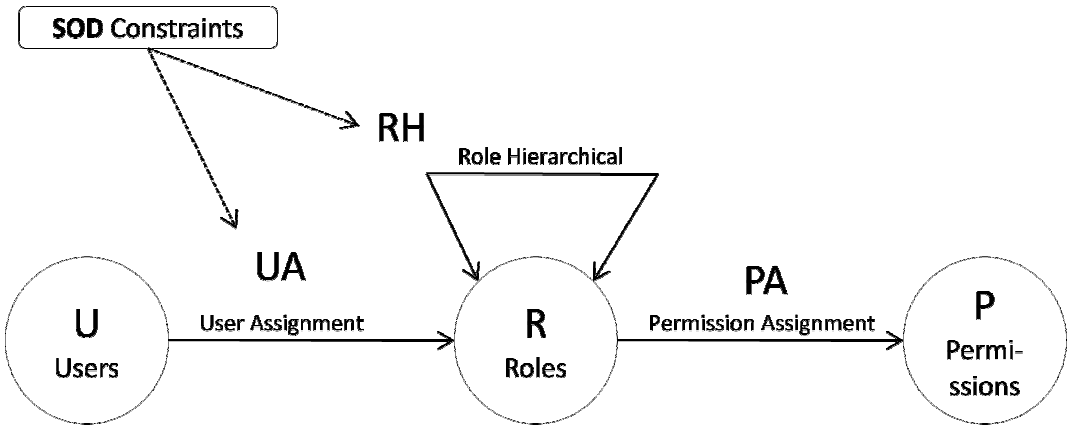

Figura 16 - Restrições RBAC - Estáticas SOD

SOD dinâmica

Supondo agora, que determinado utilizador necessita de estar associado a duas *roles* que são incompatíveis. Esta situação é normal acontecer dadas as funções que alguns colaboradores desempenham no decorrer das suas actividades na organização. Para estes casos, são utilizadas as **SOD dinâmicas.** O objectivo por trás da separação dinâmica consiste em permitir mais flexibilidade nas operações. Ou seja, um utilizador pode ter duas *roles* incompatíveis associadas desde que utilizadas independentemente mas nunca na mesma sessão. Com **SOD Dinâmica** esta situação é possível**.** Como se pode ver na figura em seguinte. Enquanto na separação estática, essa situação seria eliminada logo à partida. Quem tem atribuído determinada *role*, não pode ter acesso a outras. **SOD estática** é uma forma mais rígida a nível de *roles*. [FK92] Esta é a grande diferença entre as **SOD dinâmicas** e as **SOD estáticas**.

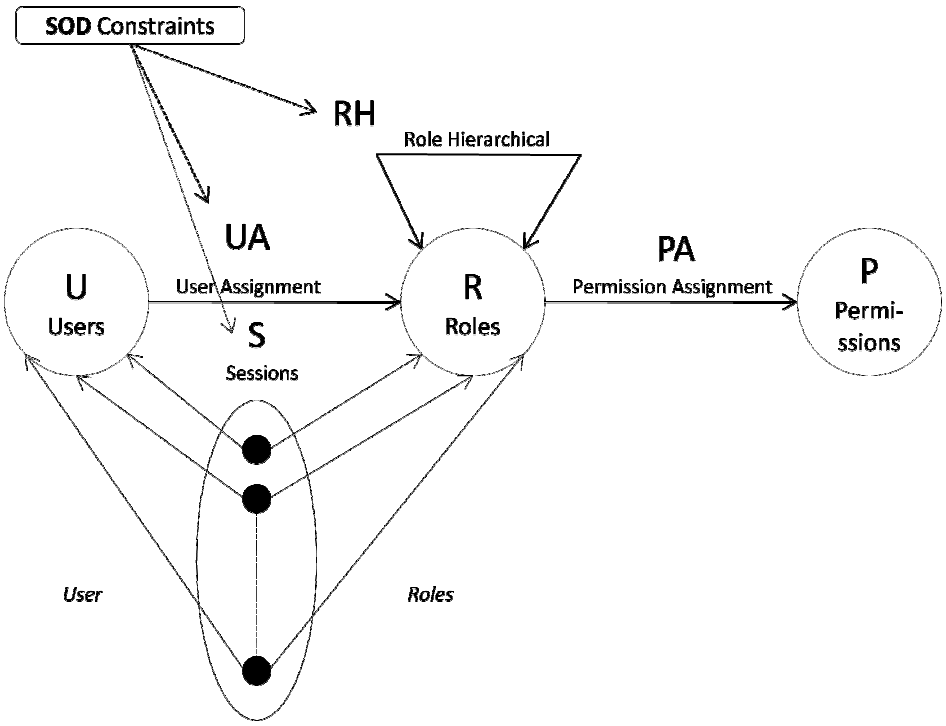

Figura 17 - Restrições RBAC - Dinâmicas SOD

Simétrico RBAC

Este nível funciona da mesma forma que o anterior mas com mais uma funcionalidade, permite a atribuição directa de permissões ao utilizador. Mas não é muito utilizado porque se torna difícil de implementar em sistemas distribuídos de grande escala. Também permite uma separação de direitos mas neste caso, incidem directamente sobre as permissões e não sobre as *roles*. Neste contexto, também há **SOD estáticas** e **dinâmicas.**

SOD estática

No nível simétrico RBAC, o funcionamento é semelhante às restrições RBAC a única diferença é a atribuição directa de permissões. Tanto para **SOD estática** como para **SOD dinâmica.** Este funcionamento é ilustrado nas seguintes figuras.

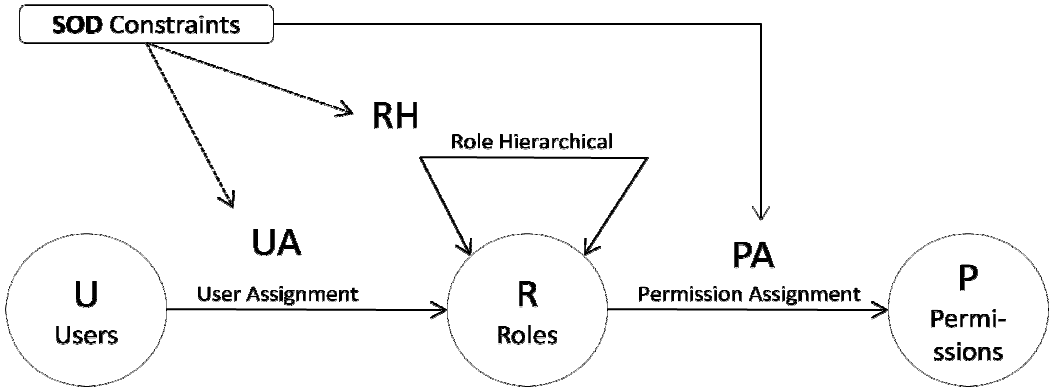

Figura 18 - Simetria RBAC - Estática SOD

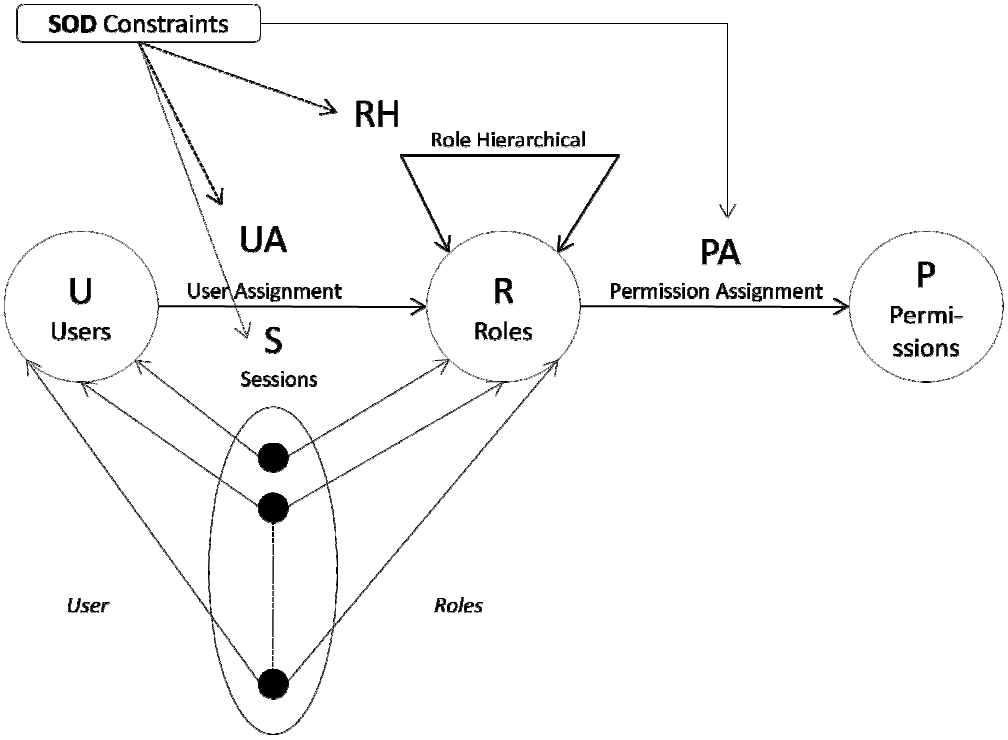

Figura 19 - Simetria RBAC - Dinâmica SOD

A seguinte tabela apresenta um resumo das principais funcionalidades de cada nível do modelo RBAC:

Tabela 2 - Níveis RBAC

Nível	Nome	RBAC Capacidades funcionais
1	**Básico RBAC**	• Utilizadores adquirem permissões através da atribuição de *roles* • Deve suportar a relação muitos-para-muitos na atribuição de *user-role* • Deve suportar a relação muitos-para-muitos na atribuição de *permission-role* • Deve suportar a possibilidade de revisão de user-*role* • Utilizadores podem usar permissões de múltiplas *roles* simultaneamente
2	**Hierarquia RBAC**	Básica RBAC + • Deve suportar hierarquia de *roles* • Nivel 2a requer suporte a hierarquias arbitrárias • Nível 2b apresenta a possibilidade de limitar as hierarquias
3	**Restrições RBAC**	Hierarquia RBAC + • Deve obrigar à separação de deveres (SOD) • Nível 3a requer suporte para hierarquias arbitrárias • Nível 3b denota suporte para hierarquias limitadas
4	**Simetria RBAC**	Restrições RBAC + • Atribuição directa de permissões ao utilizador • Nível 4a, requer suporte para hierarquias arbitrárias • Nível 4b denota suporte para hierarquias limitadas

Conclui-se que o modelo RBAC apresenta vários níveis que se ajustam para determinados problemas específicos.

Generalized Role Based Access Control (GRBAC)

O modelo GRBAC é uma extensão do tradicional modelo de controlo de acessos RBAC. Este modelo visa responder a situações para conceder acesso a determinado utilizador, para aceder aos recursos de acordo com o espaço e tempo. Incorporando assim mais 3 tipos de *roles* que até agora não são suportadas no modelo RBAC. São elas as **subject roles**, **object roles** e **environment roles**.

Subject roles

As *subject roles* que são análogas às tradicionais *roles* do modelo RBAC. A única diferença das *subject roles* em relação às tradicionais do modelo RBAC é a forma que elas usam para tomarem as duas decisões de conceder ou negar o acesso.[CMA09]
No modelo RBAC, as decisões de acesso são inteiramente baseadas nas permissões associadas com o conjunto de *roles* que o sujeito possui. No modelo GRBAC a decisão de acesso não depende apenas das *subject roles*, mas também das *environment roles* e *object roles.*

Environment roles

Estas *roles* são utilizadas de acordo com o contexto em que os recursos são disponibilizados, por exemplo, muitas organizações restringem o acesso a determinados recursos durante a noite ou fim-de-semana. Uma *environment role* é assim baseada num estado do sistema. Torna-se assim possível responder a questões temporárias como por exemplo, "Os gestores só podem editar os dados do salário dos colaboradores apenas na primeira Segunda-feira de cada mês. ". Assim como, a utilização de determinado recurso se estiver em determinado local.

Object roles

Trata-se de *roles* aplicadas aos objectos do sistema, onde estes podem conter vários atributos para os classificar, são eles:

- Data de criação
- Tipo de objecto (imagem, streaming de vídeo, etc…)
- Nível de sensibilidade (secret, top-secret, etc…)
- Informações acerca do conteúdo dos objectos

Com a informação dos atributos, é possível tomar decisões diferentes de acesso de acordo com o tipo de objectos. Suponhamos o exemplo de uma casa de família, onde os pais podem aceder à televisão, mas não querem que os filhos tenham permissões de acesso.

Enquanto no modelo tradicional RBAC se um utilizador S pretendia aceder a um objecto O, bastava que esse utilizador estivesse associado a essa *role* R e que a mesma permitisse a transacção sobre o objecto O. No caso do modelo GRBAC, aumenta a complexidade. Se determinado *subject* S pretende efectuar uma transacção T sobre um objecto O, já é diferente. O *subject* S possui um conjunto de roles são as *subject roles* Rs e o objecto possui um conjunto de *object roles* Ro. Adicionalmente, o sistema tem um conjunto de *environment roles* Re. Para que o *subject* S possa efectuar a transacção T sobre o objecto O, subject S tem que possuir algumas *subject role* Rs, tais que:

- Existe alguma *object role* Ro, possuída pelo *object* O;
- Existe alguma *environment role* Re que está actualmente activa;
- Existe uma transacção T que permite Rs aceder aos objectos na *role* Ro quando Re está activa:

Na figura está ilustrado o processo, descrito anteriormente, onde um *subject* S quer efectuar uma transacção T sobre o *object* O. [CMA09]

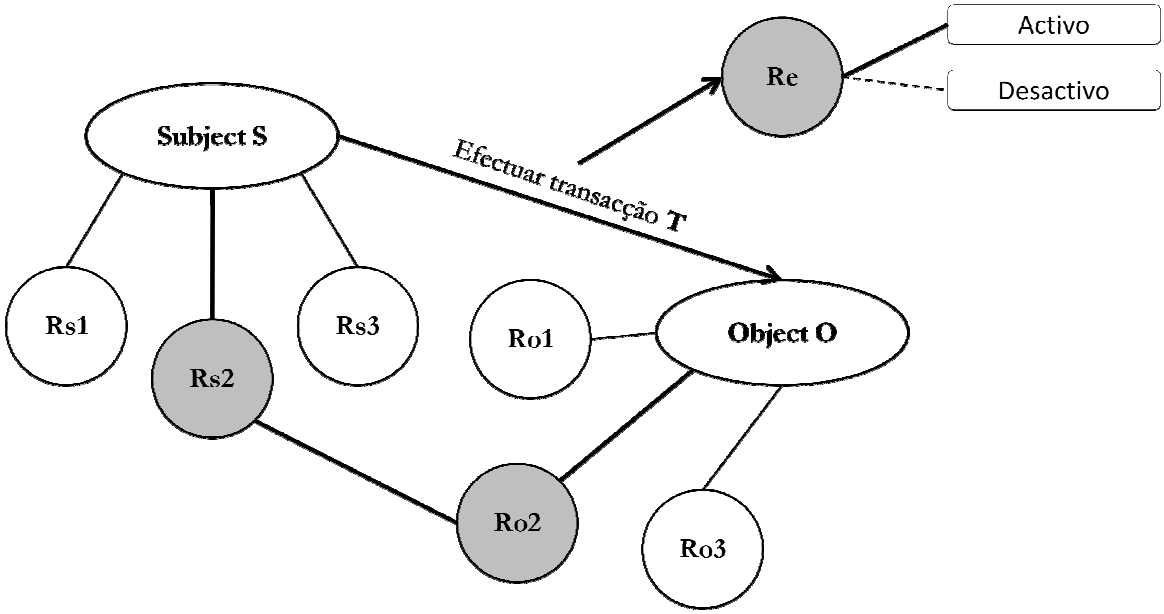

Figura 20 - Modelo GRBAC

2.3. **Conclusões**

Numa solução de gestão de identidades e acessos dois conceitos principais são tratados separadamente, mas claramente relacionados um com o outro.

A nível de gestão de Identidades são utilizadas várias técnicas de identificação dos utilizadores de forma a validar a sua identidade. Podem ser através de algo que o utilizador saiba, por exemplo *username* e *password*, alguma coisa que o utilizador possua, exemplo cartão de identificação, ou alguma coisa que o utilizador seja, exemplo, análise biométrica. Várias tecnologias auxiliam neste sentido. Esta gestão trata de todo o ciclo de vida de um utilizador no sistema, possibilitando a propagação de alteração, criação ou remoção do utilizador.

A nível de gestão de acessos está é tratada com o objectivo de ter um controlo de acessos eficaz sobre os utilizadores após estes se identificarem no sistema. Os vários modelos desenvolvidos são adaptados de acordo com o cenário.

O modelo MAC identifica-se como um modelo onde a confidencialidade é o seu principal objectivo. Tendo vários benefícios, a impossibilidade de desclassificação de informação porque se trata de um modelo especialmente focado em confidencialidade, um bom modelo para sistemas comercias que operam em ambientes hostis. A implementação do modelo evita erros administrativos porque as regras definidas são *hard coded*. No entanto, este modelo também apresenta alguns problemas, a sua implementação é difícil e como as regras são *hard coded*, quando a necessidade de alteração de alguma regra torna-se uma tarefa complexa. A diminuição na produtividade também se verifica dadas as rígidas protecções de confidencialidade.

O modelo DAC tem duas formas de funcionamento centralizado ou distribuído, no entanto é caracterizado como um modelo livre na atribuição de acessos, a diferença consiste em ter um departamento responsável por essa atribuição ou um responsável local em cada sistema. É um modelo com uma implementação fácil e de baixo custo. Apresenta como principais desvantagens a manutenção e a verificação dos princípios de segurança é extremamente difícil porque são utilizadores que controlam os acessos dos seus próprios objectos e a impossibilidade de administração central.

O modelo RBAC é um modelo à função onde permite agrupar vários grupos de utilizadores. Como benefícios, tem uma facilidade de administração [LZM01], pois só basta associar o utilizador a uma role, sem que seja necessário ter preocupação com as permissões, estas já foram definidas anteriormente. As transacções baseadas em direitos permite controlarem não apenas os recursos que são acedidos assim como quem acedeu, é aplicado o conceito dos privilégios mínimos, permite separação de direitos e uma facilidade de atribuição de utilizadores a grupos. No entanto como principal desvantagem, a administração em sistemas grandes continua a tornar-se complicada a nível de herança de roles, a necessidade de conceder privilégios mais específicos torna-se de administração mais difícil porque se trata de um modelo à função. [Crue]

O modelo GRBAC é uma extensão do modelo RBAC, funciona de uma forma semelhante, no entanto acrescem mais as variáveis externas, a nível de espaço e tempo.

Em suma, é aconselhada a utilização do modelo DAC em utilizadores particulares ou em pequenos negócios onde o número de utilizadores seja reduzido. O modelo MAC é

um modelo apropriado para um grupo especial de utilizadores que tenham em comum as mesmas necessidades. De referir, que este modelo torna-se pouco apropriado para ambientes muito dinâmicos onde existam muitas alterações de regras dada a sua segurança extremamente rígida. O modelo RBAC é mais utilizado onde o número de utilizadores é elevado, há muitos grupos de utilizadores e as funções não mudam frequentemente. [SMJ01] [iSMGCS09]. O modelo GRBAC é utilizado pelos mesmos motivos que o RBAC mas quando a necessidade de conceder acessos a determinada informação depende da localização ou durante um determinado tempo.

Capítulo 3

Descrição do Problema e Situação Actual

3.1. **Introdução**

Dada a crescente preocupação na área de Segurança, questões relacionadas com a confidencialidade da Informação e que a mesma apenas esteja acessível a quem dela necessite, as organizações sentem uma forte necessidade de saberem quem tem acesso à informação, porquê, por quanto tempo e quem autorizou. Neste contexto, deparam-se com o desafio de gerir eficaz e eficientemente a atribuição de utilizadores e perfis, dado o contínuo aumento do número de utilizadores em ambientes de sistemas heterogéneos e em múltiplos países. A falta desta gestão de acessos potencia o risco de exposição de informação crítica a utilizadores não autorizados, ou mesmo o risco de fraude, com impacto negativo na imagem da empresa. As falhas agregadas à falta de um modelo de gestão de identidades e acessos eficaz, são variados.
Na perspectiva de perceber e analisar melhor o problema em causa, alguns detalhes serão apresentados que foram avaliados segundo um levantamento do estado actual a nível de gestão de utilizadores.

3.2. **Descrição do Problema**

Com foco na área Operacional, pretende-se gerir e minimizar o risco da existência das seguintes situações:

- **Utilizadores genéricos e partilhados** - dada a natureza do negócio, em determinados processos, são utilizados *usersid* genéricos à função e partilhados, com *passwords* do conhecimento de um elevado número de colaboradores, não permitindo assim garantir o principio de não repúdio.

- **Aplicações com regras e passwords não robustas** - A existência de aplicações que não garantam a existência de regras de construção de *passwords* complexas potencia o acesso a funções de negócio e a informação por pessoas sem autorização para tal.
- **Gestão de utilizadores descentralizada no UNIFO** - A existência de um legado de aplicações com repositórios de utilizadores autónomos, não se encontrando integradas num repositório central de utilizadores, dificulta a gestão nos processos de check-in, transferência de funções e check-out de utilizadores.
- **Utilizadores "fantasmas"** - a existência de utilizadores que não são utilizados por um período alargado de tempo, por mudança ou cessação de funções, potencia a sua utilização para acções fraudulentas.
- **Utilizadores duplicados** - A utilização de *usersid* diferentes por aplicação que pertencem ao mesmo colaborador dificulta os processos de identificação e gestão dos mesmos.
- **Mudanças regulares de funções** - Alguns colaboradores desempenham funções diferentes durante o seu ciclo de vida na empresa, nesse contexto as suas permissões de acesso a determinadas aplicações devem acompanhar essa mudança com o objectivo de garantir o princípio que um colaborador apenas deve ter acesso à informação necessária para o exercício da sua função.
- **Perfis não alinhados com funções de negócio** - Como algumas atribuições são atribuídas a pedido, por exemplo, por motivos referidos anteriormente em que determinado funcionário muda de funções. Não existem em várias situações perfis definidos com as novas funções a desempenhar.
- **Processo de atribuição moroso** - A existência de múltiplas aplicações e a não integração total da atribuição de acessos no Sistema Central de Gestão de Utilizadores obriga a um conjunto de autorizações/validações que torna o processo de atribuição de acessos moroso e de elevado esforço manual. Não existe uma solução que automatize este processo, torna-se necessário recorrer a vários processos para que determinado colaborador tenha os acessos disponíveis em tempo útil.

3.3. **Caracterização da situação actual**

Uma das fases da componente prática da dissertação consistiu em obter informação mais detalhada sobre o estado actual. Neste contexto, foi feita uma avaliação a nível de gestão de utilizadores, actuais utilizadores e acessos.

Gestão de utilizadores

A gestão de utilizadores definida actualmente apresenta-se descentralizada, a loja tem total autonomia na gestão dos mesmos e atribuição de acessos.
Esta situação está ilustrada na seguinte figura.

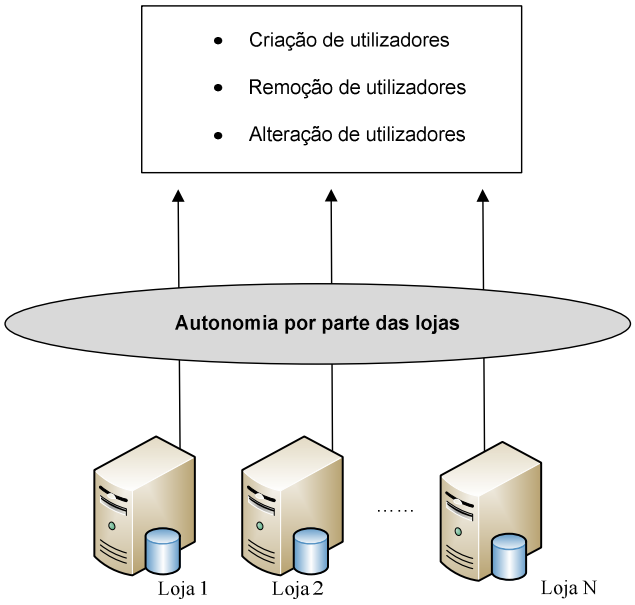

Figura 21 - Gestão de utilizadores actual

Identidades

Outro levantamento necessário foi a nível de utilizadores nas lojas para perceber a relação deles com uma identidade. Foi um processo que consistiu na aplicação de um mecanismo que compara informações provenientes dos recursos humanos e do actual sistema implementado nas lojas, o UNIFO.
Para isso, foram recolhidas duas listas, uma com os actuais colaboradores da sonae e outra com os utilizadores que estão cadastrados no UNIFO para conseguir identificar os utilizadores. Com a aplicação do mecanismo aplicado, é possível verificar se é um utilizador válido ou não.
Considera-se um utilizador válido quando todos os requisitos do mecanismo aplicado são satisfeitos. Todos os outros casos são para tratar. Esta situação está exemplificada na seguinte tabela.

Tabela 3 - Relação UNIFO - RH

LISTA	Requisitos mecanismo	Acção
RH / **UNIFO**	Satisfaz todos os requisitos	**Válido**
RH / **UNIFO**	Satisfaz um ou mais requisitos mas não todos	**Tratar (com ligação RH)**
RH / **UNIFO**	Não satisfaz nenhum requisito	**Tratar (sem qualquer ligação com RH)**

Após esse levantamento verificou-se que **84%** dos utilizadores satisfazem pelo menos um requisito do mecanismo, os outros **16%** não satisfazem qualquer requisito pelo que não têm qualquer ligação com os valores dos Recursos Humanos. Estes valores são apresentados na seguinte tabela.

Tabela 4 - Universo Unifo

UNIFO com correspondência em RH	UNIFO sem qualquer correspondência em RH
84%	16%

Dos **84%** dos utilizadores resultantes da correspondência UNIFO-RH, conclui-se que **93%** são utilizadores válidos (Todos os requisitos do mecanismo são satisfeitos), os outros **7%** indicam que só são satisfeitos um ou mais requisitos mas não todos, pelo que será necessário rectificar a situação recorrendo a informações provenientes das lojas, ou mesmo das estruturas centrais. Estes valores são apresentados na seguinte tabela.

Tabela 5 - RH e UNIFO

RH e UNIFO	
Validos	Tratar
93%	7%

Com os valores totais do universo UNIFO, no final obtêm-se **78%** de utilizadores válidos, de acordo com o mecanismo aplicado. Valores para tratar com correspondência em RH e sem correspondência com RH, obtém-se os valores de **6%** e **16%**, respectivamente. Estes valores são ilustrados na seguinte tabela.

Tabela 6 - Valores finais estado actual

Valores finais do estado actual		
Válidos	Tratar RH e UNIFO	Tratar UNIFO
78%	6%	16%

No final obtemos um total de **78%** de utilizadores válidos e **22%** para tratar. Ver a seguinte tabela. No entanto, todos os utilizadores marcados como válidos têm que ser validados com as lojas.

Tabela 7 - Valores finais

Valores Finais	
Total Válidos	Total Tratar
78%	22%

Acessos

A nível de perfis de acesso, a avaliação consistiu essencialmente em obter uma percepção de como os acessos eram atribuídos e que tipos de acessos existiam, quem tem acesso e a que informação. Esta avaliação incidiu sobre todos os utilizadores do UNIFO.

Como resultado desta avaliação verificou-se que existem **3 perfis** principais (Administrador, Operador e Consulta). Para cada perfil, foi contabilizado o número de utilizadores que estavam associados a esse perfil.

Concluiu-se que para o perfil de administrador estão associados um número elevado de utilizadores, o que indicia que uma grande maioria de utilizadores possui acessos excessivos em relação à função que executa.

3.4. **Conclusões**

A identificação de falhas ou problemas nos sistemas de informação, por si só, não apresentam todos os detalhes do verdadeiro problema a resolver. Neste sentido, um levantamento do estado actual permitiu obter mais informações até agora desconhecidas. Identificaram-se vários problemas a nível de actual gestão de utilizadores, identidades e acessos.

A actual gestão de utilizadores é descentralizada, sendo a mesma da responsabilidade de cada loja. Os problemas desta gestão incidem sobre a falta de controlo de acessos e identificação dos seus utilizadores.

Muitos utilizadores foram criados nas várias lojas sem nenhum tipo de regra consistindo na dificuldade em obter a sua identidade. Utilizadores desconhecidos mesmo até para a própria loja, login diferente para várias lojas tratando-se da mesma identidade e no caso da saída de um colaborador o utilizador continuava registado e com os acessos activos.

A nível de perfis verificaram-se só 3 perfis de acesso e com funcionalidades, ou muito limitadas ou com acessos excessivos. Um perfil de administrador, tem total acesso aos recursos disponibilizados pelo sistema, ao contrário dos outros dois perfis, operador e consulta. Caso um utilizador necessitasse de aceder a mais alguns recursos para desempenhar a sua função, a solução era atribuir perfil de administrador. Mas esta situação vai contra um dos conceitos principais de atribuição de acessos, denominada privilégios de acessos mínimos.

Com este levantamento, verificou-se que há muitos utilizadores onde não é possível identificá-los e muitos com acessos não adequados à função que desempenham. Esta situação é um reflexo de uma gestão descentralizada de um grande número de utilizadores.

Capítulo 4

Desenvolvimento do Projecto

4.1. **Introdução**

Na definição de um modelo de gestão de identidades e acessos os conceitos envolvidos devem ser tratados separadamente, inicialmente identidades e posteriormente os acessos.

A gestão de identidades deve ter em conta por qual ou quais atributos determinada identidade deve ser reconhecida no sistema. De forma a criar um identificador único.

A gestão de acessos, tem como principal objectivo gerir todos os acessos a atribuir aos utilizadores, concedendo as permissões necessárias para o desempenho das suas funções. Este controlo de acessos segue o modelo RBAC que é o que mais se enquadra com a actual situação. Vários perfis são criados para conceder as permissões necessárias aos vários grupos de utilizadores.

Durante o processo de implementação, alguns procedimentos a nível de gestão de utilizadores foram criados e alterados, mesmo que temporários.

4.2. **Definição do Modelo**

4.2.1. GESTÃO DE IDENTIDADES

A nível de gestão de identidades foi definido um identificador único para cada utilizador, através dele é sempre possível saber qual a identidade do utilizador que está a aceder ao sistema.

Como forma de autenticação de um utilizador no sistema será através de algo que ele conheça, neste caso, o uso tradicional do par *username* e *password.*

Os utilizadores do sistema UNIFO serão de dois tipos, denominados utilizadores genéricos e utilizadores únicos. Utilizador único corresponde à utilização por um única identidade. Utilizadores genéricos serão utilizados por mais que uma identidade.

A criação dos utilizadores genéricos é uma necessidade de forma a facilitar as operações nas lojas.

Utilizadores únicos

Para a definição das identidades para acesso ao sistema UNIFO, foi definido uma forma que permite identificar univocamente qualquer utilizador que está a aceder ao sistema UNIFO. Esta situação está apresentada na seguinte figura, onde um utilizador tem acesso através do seu login único, às lojas 1 e 2, e não tem acesso à loja 3.

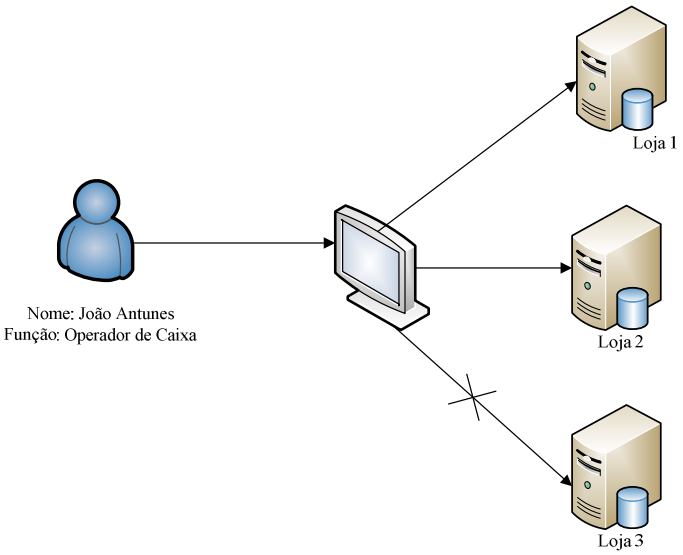

Figura 22 - Aplicação método identificação

Utilizadores genéricos

Estes utilizadores apesar de não serem identificados univocamente os acessos a eles atribuídos não implicam um risco elevado para a organização. Mas, para estes utilizadores também foram definidas regras para a sua criação. Um exemplo é ilustrado na seguinte figura.

99	Número de Loja

Figura 23 - Utilizadores genéricos

4.2.2. GESTÃO DE ACESSOS

A nível de gestão de acessos com fundamento nos modelos de controlo de acesso estudados, o que melhor se aplica a esta situação é um modelo de gestão de perfis, ou seja, um modelo à função. O modelo RBAC dadas as suas funcionalidades de lidar bem com grandes grupos de utilizadores e com funções que não tenham grandes alterações ao longo do tempo é o mais indicado. Como os acessos não precisam ser controlados de acordo com o tempo ou localização do utilizador, o modelo GRBAC pode ser excluído que é o outro modelo também orientado à função.

Os perfis mencionados na caracterização do estado actual, não se adequavam à realidade, nesse sentido, foram criados mais perfis aplicacionais de acordo com a sua função na empresa.

Cada perfil aplicacional tem acessos e formas de acesso diferentes às funcionalidades do UNIFO de acordo com os privilégios mínimos para o colaborador desempenhar com sucesso as suas funções. No entanto, nesta definição foram criadas excepções e alguns perfis têm mais acessos do que os necessários, mas isso não implica um risco considerado grave. Estas excepções foram feitas de forma a conseguir agregar um maior número de utilizadores num determinado perfil e limitar o número de perfis.

Perfilagem

No processo de perfilagem para a criação de mais perfis, foram consultadas as funções que podiam e não podiam desempenhar os colaboradores nas lojas. Para a definição correcta dos perfis e ajustar as permissões adequadas a cada um. Foi feita uma separação em 3 níveis: estruturas centrais; lojas; e temporários, como estão apresentados na seguinte figura:

Figura 24 – Níveis perfilagem

Estruturas Centrais

Nas estruturas centrais estão colaboradores que trabalham para as lojas, mas não nas lojas. Ou seja, departamentos financeiros, equipas de suporte, directores de operações, etc. Este grupo de utilizadores tem muitas funções em comum, no entanto algumas têm que ter acessos diferentes. No caso do financeiro. Foram criados os seguintes perfis para as estruturas centrais, **Serviços Financeiros**, **Consulta e Suporte Aplicacional** como se pode ver na figura seguinte.

Figura 25 - Perfil Estruturas Centrais

Os perfis foram definidos de acordo com as funções que os colaboradores desempenham na empresa, não foi feito um mapeamento directo com a sua posição hierárquica na empresa, porque originava muitos perfis, e como referido anteriormente a possibilidade

de conceder mais acessos (limitados) não incorre num risco grave para a organização. Assim, foi possível reduzir o número de perfis e homogeneizar cada um deles. Para cada perfil foram associadas várias permissões/acessos para que todos os utilizadores que estejam associados aquele grupo, possam desempenhar o seu papel. Há vários perfis com acessos em comum e outros que só estão associados a alguns perfis.

Loja

Os perfis de loja englobam todos os colaboradores que trabalham directamente na loja, directores de loja, operadores, supervisores, etc. Seguindo o mesmo princípio que nas estruturas centrais, o risco de atribuição de acessos é controlado. Desta definição resultaram 4 perfis, que estão ilustrados na seguinte figura.

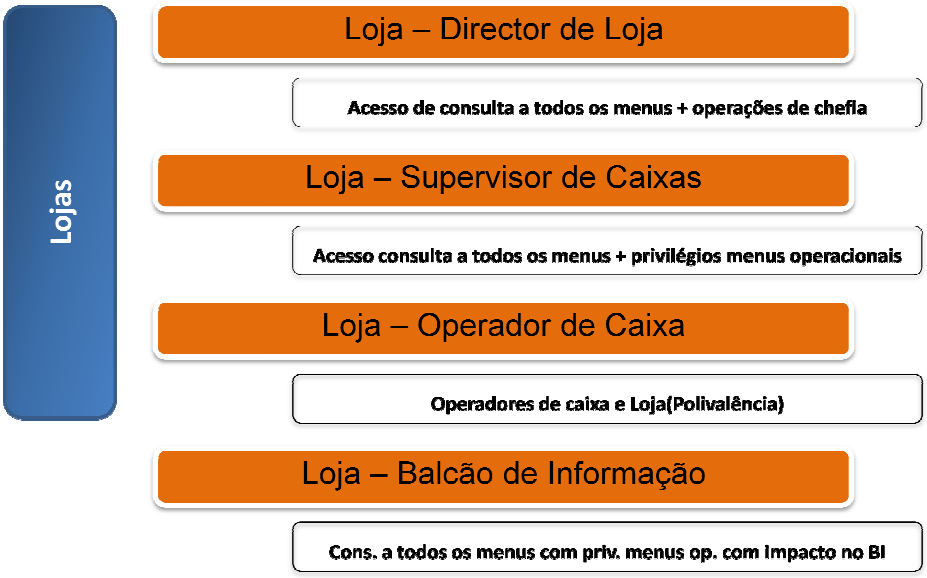

Figura 26 - Perfis Lojas

Temporários

Durante o processo de migração para uma nova *release* da aplicação UNIFO que suporta novas funcionalidades de perfilagem, houve a necessidade de manter os perfis actuais, criando assim 3 perfis temporários para serem utilizados no decorrer do processo de migração para os novos perfis.
Esta necessidade surge para minimizar os impactos da migração, dado tratar-se de um trabalho de grande dimensão, que tem que ser feito de forma faseada e gradual.
Os perfis temporários criados estão ilustrados na seguinte figura:

Figura 27 - Perfil Temporário

Estes perfis, serão eliminados quando finalizada toda a implementação.

Com toda a análise feita anteriormente, foi criada uma matriz, denominada **matriz RBAC** onde são apresentados todos os acessos atribuídos a cada perfil, assim como o tipo de acesso. Esta matriz, foi transportada para a nova versão do UNIFO. De seguida está apresentada a forma como foi criada a matriz, por motivos de confidencialidade não é possível disponibilizar a totalidade da matriz.

C – Consulta
X – Sem acesso
T – Acesso Total

Tabela 8 - Matriz RBAC

	Central			**Loja**			
	Serviços Financeiros	Suporte Aplicacional	Consulta	Director de Loja	Supervisor de Caixas	Operador de caixa	Balcão de Informação
Funcional.	**Tipos de acesso**						
Func. 1	C	T	C	C	T	X	C
Func. 2	C	T	C	C	T	X	T
Func. 3	C	T	C	C	C	X	C
Func. 4	C	T	X	X	C	X	X

4.3. **Implementação do modelo**

Para a implementação do modelo no sistema UNIFO, inicialmente foi alterado o procedimento de gestão de utilizadores de forma a centralizar esta gestão. Como forma de evitar a continuidade de aparecimento de mais problemas detectados na caracterização do estado actual.

A nível de identidades, as lojas foram notificadas através de um procedimento onde constam indicações do processo que está a decorrer, as novas regras para a gestão de utilizadores e as regras definidas no modelo a ser seguidas.

A nível de acessos, os perfis atribuídos foram os temporários durante o processo de migração para a nova versão do UNIFO.

4.3.1. PROCEDIMENTO DE GESTÃO DE UTILIZADORES

Este procedimento alterou a forma como estavam a ser geridos os utilizadores, retirando a total autonomia das lojas sobre a gestão dos seus utilizadores. Esta responsabilidade passou para uma equipa de suporte UNIFO, tendo agora uma gestão de utilizadores central, estamos perante um modelo DAC centralizado. Uma loja que pretenda criar um novo utilizador não pode fazê-lo de uma forma autónoma, mas sim, efectuar os pedidos ao *helpdesk*, que por sua vez a equipa de suporte trata dos mesmos. Esta situação é ilustrada na seguinte figura:

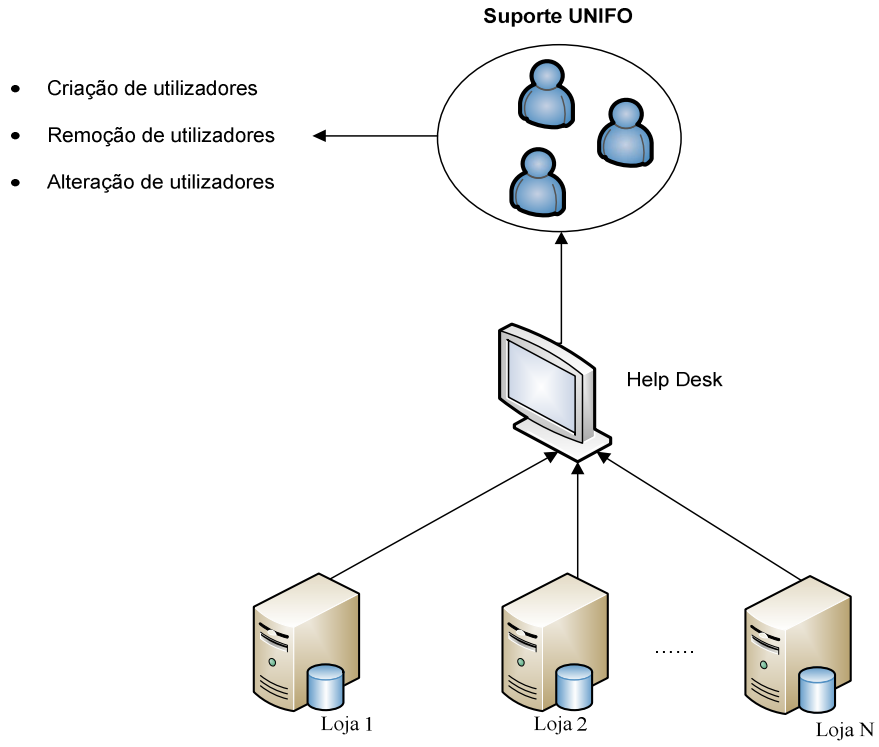

Figura 28 - Gestão DAC centralizada

4.3.2. IDENTIDADES

Durante o processo de revisão e limpeza dos utilizadores no UNIFO após envio do novo procedimento de gestão de utilizadores UNIFO às lojas, como forma de acelerar todo o processo de tratamento das identidades foi criada uma excepção, para comunicação com as lojas. Quando as lojas necessitam de alterações ou eliminação dos seus utilizadores no âmbito do processo de revisão e limpeza dos utilizadores, não precisam seguir o procedimento normal implementado para a gestão central de utilizadores. Foi criada uma caixa de correio electrónico criada especialmente para este processo para não sobrecarregar a equipa de suporte e as lojas terem uma resposta mais breve.

Todos os utilizadores resultantes do levantamento do estado actual efectuado anteriormente têm que ser validados com as lojas. Apesar de estarem de acordo com o mecanismo aplicado, essa validação é sempre obrigatória, porque muitos utilizadores já alteraram as suas funções e não devem de ter acessos a essas lojas.

Assim, todos os utilizadores do sistema UNIFO, no final desta revisão ficam de acordo com as regras definidas no modelo.

4.3.3. ACESSOS

Os novos perfis são atribuídos aos utilizadores das lojas se houver confirmação por parte das lojas dos perfis operacionais dos colaboradores e se a nova versão do UNIFO já foi instalada no sistema daquela loja. Caso a loja não confirme, são atribuídos os perfis temporários criados para o efeito.

4.4. **Conclusões**

Neste capítulo definiu-se um modelo para a gestão de identidades e acessos para um sistema específico, o UNIFO.

A nível de identidades a forma de identificação recaiu sobre algo que o colaborador conheça neste caso o tradicional par *username* e *password*. Um identificador único no sistema UNIFO foi definido para que seja sempre possível identificar qualquer utilizador único.

A nível de acessos chegou-se à conclusão que o modelo de controlo de acessos mais indicado é o RBAC. Porque se trata de um universo de utilizadores grande e há a possibilidade de divisão em vários grupos. Esta divisão é possível porque muitos

utilizadores têm as mesmas funções operacionais. Neste sentido, foram definidos mais perfis que os identificados no levantamento do estado actual.

Iniciou-se assim uma divisão em 3 níveis, estruturas centrais, lojas e temporários. Para cada nível foram definidos vários perfis, que estes serão posteriormente utilizados para atribuir aos vários grupos de utilizadores.

Nesta definição de perfis alguns têm permissões em comum, e outros têm essas mesmas permissões mas com tipos de acesso diferentes. Esta criação de mais perfis foi necessária e essencial para obter um alinhamento correcto entre os perfis aplicacionais e operacionais.

Após a definição do modelo, foram alterados alguns processos e criados procedimentos de forma a apoiar a implementação. Durante esta fase foi alterado o processo de criação de utilizadores, uma gestão centralizada implementada com um departamento responsável por toda a gestão dos utilizadores.

Um procedimento foi enviado para as lojas com as novas alterações da gestão de utilizadores e o processo de revisão que está em curso.

Como resultados da implementação, actualmente **45%** dos utilizadores do UNIFO já estão resolvidos, isto é, validados com as lojas. Destes 45%, **40%** mantiveram-se sem qualquer tipo de alteração, **5%** eliminados porque não estavam de acordo com as regras e **0,5%** foram alterados. Todos os valores resultantes da implementação estão apresentados na seguinte tabela, com valores detalhados e acções realizadas sobre esses utilizadores.

Tabela 9 - Valores actuais da Implementação

Resultados actuais da implementação				
Status/Acção	**Ok**	**Eliminados**	**Alterados**	**Total**
Resolvidos	40%	5%	0,5%	45%
Não resolvidos	37%	13%	5%	55%

Capítulo 5
Conclusões e trabalhos futuros

5.1. **Conclusões**

Para obter uma melhor gestão de identidades e acessos dos utilizadores aos sistemas de informação da empresa, na área operacional, uma gestão centralizada deve existir, seja esta apoiada por um departamento responsável por essa gestão ou uma solução comercial de gestão de identidades e acessos (IAM). Assim como, deve ser seguido um modelo que defina as regras de identificação e controlo dos acessos, dos utilizadores aos sistemas de informação.

De acordo com o problema proposto[15], foram identificadas lacunas na gestão de utilizadores e respectivos acessos devido à falta de regras de identificação e atribuição de acessos. A necessidade da criação de um modelo para a gestão de identidades e acessos é assim essencial.

No entanto, como passo inicial procedeu-se a um levantamento do estado actual[16] a nível de perfis actuais e quais as permissões de acesso de cada perfil. O mesmo foi feito relativamente aos utilizadores de forma a identificá-los.

Neste contexto, verificou-se que a alteração de alguns procedimentos de gestão de utilizadores se tornou necessária para não continuar com o processo de gestão descentralizado que estava em curso até à data. Foi então alterado o processo de gestão de utilizadores, para uma gestão centralizada com um departamento responsável por todo o ciclo de vida dos utilizadores nas lojas. Com este procedimento, foi retirada a autonomia às lojas e foi possível ter mais controlo sobre o ciclo de vida dos utilizadores.

[15] Descrição do problema (secção 3.2)
[16] Caracterização do estado actual (secção3.3)

Para a definição do modelo de gestão de identidades e acessos que seja adequado ao sistema UNIFO, inicialmente foram tratadas as identidades e posteriormente os acessos. Concluiu-se que a forma de validação de identidade mais adequada ao sistema de informação era a forma tradicional, a utilização do conjunto *username* e *password* para poder aceder ao sistema. Onde o *username* é um identificador único no sistema UNIFO de forma a ser sempre possível saber a identidade de qualquer utilizador do sistema.

A nível de acessos, vários modelos de controlo de acessos foram abordados. O modelo *Mandatory Access Control (MAC)* é um modelo que consiste em atribuir classificações diferentes aos vários recursos do sistema e as entidades só podem aceder a esses recursos caso estejam autorizadas ou habilitadas para acesso a essa informação. É um modelo muito utilizado em situações que se pretende um grau de confidencialidade muito elevado. Na área operacional pretende-se ter uma produtividade elevada e não se pode permitir que as regras rígidas de segurança impeçam esse rendimento, logo o modelo MAC não é o mais indicado para a actual situação.

O modelo *Discretionary Access Control (DAC)* é um modelo cujos acessos podem ser atribuídos individualmente e livremente. Este modelo, quando utilizado no seu modo distribuído não é eficiente para um universo de muitos utilizadores, prova disso foi a situação actual encontrada. Este modelo quando usado em modo centralizado, apresenta-se como uma boa solução mas como temporária, porque o excesso de pedidos sobrecarrega a equipa responsável pela gestão de utilizadores, assim como alguma dependência.

O modelo *Role Based Access Control* (RBAC) é um modelo orientado à função para vários grupos de utilizadores. Trata-se de um modelo indicado para grupos grandes de utilizadores, onde as funções às quais os utilizadores estão associados não sofrem grandes alterações e a administração de utilizadores é fácil.

O modelo *Generalized Role Based Access Control* (GRBAC) também é um modelo orientado à função mas com mais variáveis externas, tempo e local em que a necessidade de ter acessos a determinada informação pode depender da localização ou durante determinado tempo. Este modelo também foi considerado porque agrega todas as vantagens do modelo RBAC, no entanto a necessidade de permitir acessos de acordo com a localização geográfica ou temporal do utilizador não é uma realidade para os utilizadores na área operacional do universo UNIFO.

Concluí-se assim que o modelo mais ajustado à realidade do problema apresentado é o RBAC. Dado que estamos perante uma área com um grande número de utilizadores e podem ser divididos em vários grupos que desempenham as mesmas funções e estas não mudam frequentemente.

Após a definição do modelo, procedeu-se à sua implementação sendo esta efectuada paralelamente com uma revisão e limpeza de utilizadores, para resolver os vários problemas identificados[17]. Inicialmente foram tratadas as identidades onde todos os utilizadores tiveram que ser validados com as lojas, independentemente de estes estarem identificados nos recursos humanos. Resolvendo assim alguns acessos mal atribuídos, situações como por exemplo, utilizadores que alteraram funções e não precisam de ter acesso a determinadas lojas. A atribuição dos novos perfis de acesso inicialmente estava

[17] Ver Capítulo 3

previsto ocorrer posteriormente ao tratamento das identidades, mas como se trata de um universo muito grande de utilizadores está a decorrer em paralelo sempre que possível.

Dado o universo de utilizadores ser demasiadamente grande e o curto espaço de tempo não é possível apresentar mais resultados da implementação do modelo. A revisão é um processo para continuar nos próximos projectos até estarem todos os utilizadores alinhados com as regras definidas e perfis correctamente atribuídos.

Ainda muito trabalho tem que ser desenvolvido a fim de terminar todo este processo a nível de identidades e acessos.

Ficou definida uma estratégia de gestão utilizadores de forma a reduzir a sua complexidade de gestão e posteriormente automatizar todo o seu processo de gestão com a implementação de uma solução de IAM.

Apesar de a implementação de uma solução de IAM não estar alocada a este projecto, foi feita uma abordagem teórica e é apresentada uma solução para trabalho futuro.

5.2. **Trabalho futuro**

Este projecto é uma parte integrante dum projecto de grande dimensão que prevê futuramente mais fases de forma a alcançar outros objectivos. Neste contexto, a continuidade da revisão e limpeza de utilizadores é um trabalho que terá continuidade para além deste projecto. Quando este processo terminar, o trabalho fica completo para que possa ser aplicada uma solução de gestão de identidades e acessos que consiga gerir eficazmente e automatizar processos de gestão de utilizadores. A solução que se pretende implementar vai fazer uma gestão de identidades e acessos correcta. Porque tem ligação com vários sistemas e assim, gere centralmente todo o ciclo de vida do utilizador. Nesta solução são definidas as várias regras. Prevê-se que esta implementação decorra durante os próximos anos. Na seguinte figura, está apresentada a arquitectura como uma solução de IAM será utilizada.

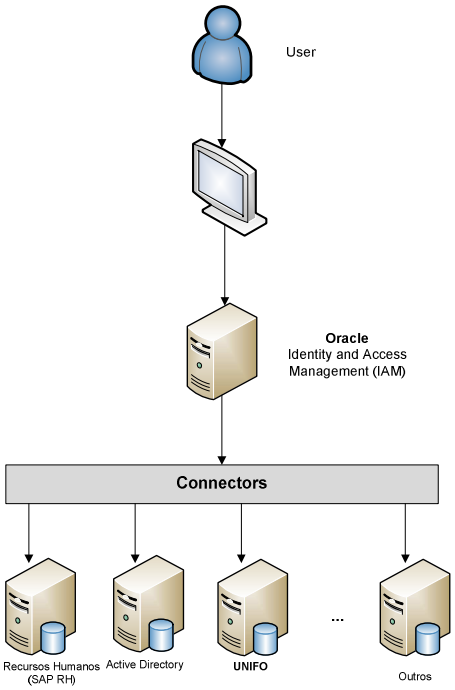

Figura 29 - Solução ORACLE

Esta solução, apresentada pela Oracle, permite obter uma gestão centralizada de utilizadores, onde é possível ter uma administração central dos utilizadores e usufruir das vantagens[18] da mesma. Neste contexto, quando há alguma alteração a nível de utilizador e dos seus acessos, esta é propagada por todos os sistemas que estão agregados à solução da Oracle.

[18] Ver secção 2.2

Referências

[CarnFCA]. Introdução à segurança da informação, Alberto Carneiro, FCA

[CernPace08]. International Conference on Computing in High Energy and Nuclear Physics, Journal of Physics, Conference Series, Identity Management, Alberto Pace; Cern, Geneva, Switzerland.

[CMA09]. Generalized Role-Based Access Control for Securing Future Applications, Michael J. Covington, Matthew J. Moyer and Mustaque Ahamad, July 2009

[Cob09]. CobitV4.0.

[Crue]. Methods for Access Control: Advance and Limitations, Ryan Ausanka-Crues, Harvey Mudd College, 301 Platt Blvd Claremont, California

[CSI08]. CIS/CSE 785:Computer-Security(Syracuse University),23 October 2008

[FK92]. Role-Based Access Controls,15th National Computer Security Conference (1992), David F. Ferraiolo and D. Richard Kuhn, National Institute of Standards and Technology.

[FNL09]. Classificação da informação de acordo com norma ISO/IEC 17999:2005, João Carlos Ferreira, Ennisten Neto e Ricardo Leite

[GartnerPA08]. A Decision Framework for Initial Identity and Access Management Planning, Earl Perkins, Ant Allan, 29 January 2009

[IEEECS07]. Emerging Standards, RBAC Standard Rationale, publish by the IEEE Computer Society, November/December 2007

[iSMGSS09]. iSMG- Security Strategies july 2009 (The Latest Information Security News, Technology and Insights) - It's all about Access - IAM Trends & Solutions

[iSMGCS09]. iSMG Information Security Media Group, Case Study:People's United Bank Saves Time, Cost through Identity and Access Management, 2009

[ISO10b]. Normas ISO, http://www.27000.org/iso-27001.htm

[ISO05]. La norme Internationale ISO/IEC 17799:2005

[ITIL10a]. ITIL, http://www.itil.org/en/vomkennen/itil/index.php

[Jun09]. Introduction to Role based Access control (RBAC) model, Oulu University, The Department of information Processing Science, Marja Junno, 31March 2009

[LZM01]. Malasyan Journal of Computer Science, Vol. 14 No.2, December 2001, pp. 20-25, Rola-Based Access Control in Kidney Dialysis Information System, Boon Peng Lim, Omar Zacaria and Mustaffa Kamal Mohd Nor

[Mat03]. Cristiano Matos, *Sentinel:um engenho Java para controle de acesso RBAC,* Tese de Mestrado, Universidade Federal de Pernambuco, Agosto 2003

[NIST03]. Role Based Access Control: NIST Solution, SANS Institute 2003

[NIST09]. Role-Based Access Control(RBAC): Features and Motivations, November 2009

[OECG10c].OECG,http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html

[Orac03]. Oracle Identity Management Concepts and Architecture, An Oracle White Paper, December 2003

[PDAC10d]. Modelo PDAC, http://www.asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html

[REY07]. Global Technology Audit Guide, Identity and Access Management, Project Leader, Sajay Rai, Ernst&Young LLP, November 2007

[SCFY96]. IEEE Computer, Volume 29, Number 2, February 1996, pages 38-47, Role-Based Access Control Models, Ravi S.Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman

[SFK]. The NIST Model for Role-Based Access Control: Towards A Unified Standard, Ravi Sandhu, David Ferraiolo and Richard Kuhn

[SMJ01]. The Role-Based Access Control System of a European Bank: A Case Study and Discussion,Andreas Schaad, Jonathan Moffett, Jeremy Jacob, 2001

[SSW]. A case Study of Separation of duty properties in the context of the Australian "eLaw" process, Andreas Schaad&Pascal Spadone, Helmut Weichsel

[TechIAM07]. Technology Brief: Identity and Access Management, An integrated Architecture for Identity and Access Management, CA, Transforming IT Management

Anexos

Anexo I

A Sonae é uma empresa de retalho fundada em 18 de Agosto de 1959, com duas grandes parcerias ao nível dos centros comerciais e telecomunicações. Esta tem várias áreas de negócio como são ilustradas na seguinte figura.

Figura 30 - Áreas de negócio

Sonae MC

A Sonae MC é responsável pela área de retalho alimentar da Sonae e é hoje uma referência no mercado, após ter iniciado uma verdadeira revolução nos hábitos de consumo e no panorama comercial português, com a implementação do primeiro hipermercado em Portugal, em 1985 (Continente de Matosinhos).

A Sonae MC é líder de mercado nacional, no retalho alimentar, com um conjunto de formatos distintos que oferecem uma variada gama de produtos de qualidade superior, aos melhores preços: Área Saúde (parafarmácias), Bom Bocado (cafeterias), Book.it (livraria/papelaria), Continente (hipermercados) e Modelo (supermercados).

Organigrama estrutural

A Sonae como dito anteriormente está dividida em várias áreas de Negócio e o trabalho desenvolvido nesta tese foi efectuado na Sonae MC. A nível de perfil corporativo é o seguinte:

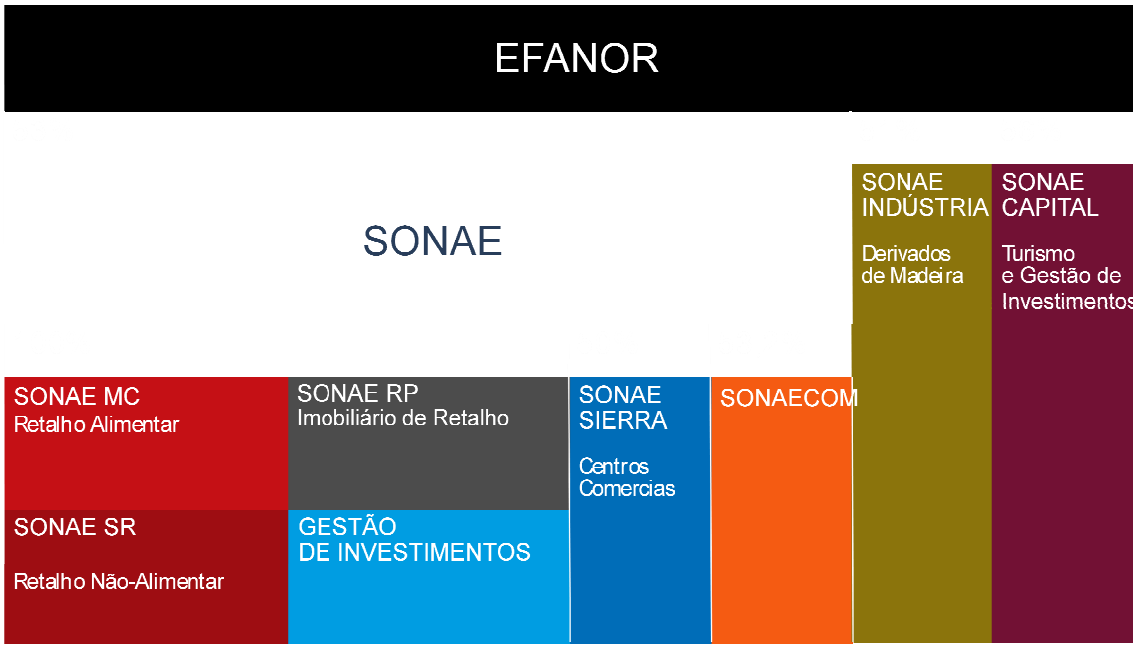

Figura 31 - Perfil Corporativo

A SONAE MC é composta por vários departamentos. O DSI (Departamento de Sistemas de Informação) é o responsável por toda a vertente informática da empresa. O Organigrama estrutural do DSI é o representado de seguida.

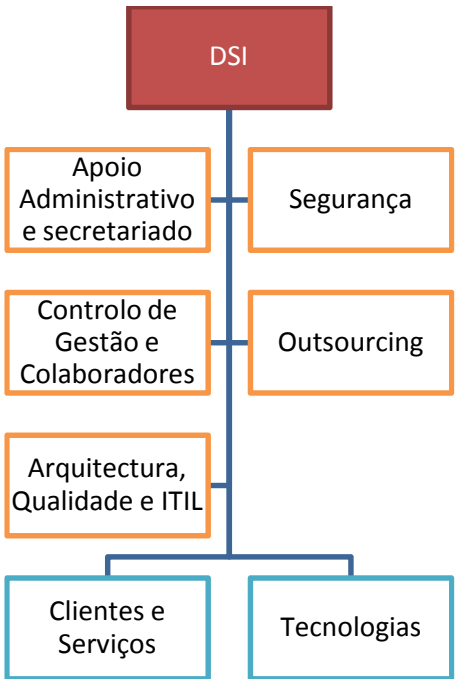

Figura 32 - Organigrama DSI

A área da segurança é uma área que está presente em toda a estrutura da DSI, de forma a resolver todo o tipo de problemas relacionados com segurança. Tentando minimizar qualquer impacto que possa condicionar o correcto funcionamento de todo o negócio da SONAE MC.

Anexo II

Normas internacionais

Iso/IEC 27001 (International Organization for Standardization)

A norma ISO/IEC 27010 trata-se de um padrão internacionalmente reconhecido para a segurança da informação constituído por várias regras de forma a garantir a segurança em todo o ciclo de negócio de uma organização. Através desta norma é possível certificar um sistema de gestão de segurança da informação (Information Security Management System - ISMS), desde o planeamento de novas funcionalidades nos sistemas, passando pelo cumprimento das leis e regulamentações, identificação contínua de riscos, aplicação de controlos tecnológicos e físicos, continuidade do negócio e recuperação de desastres, sensibilização contínua de pessoas sobre os temas de segurança, entre diversos outros aspectos.

O objectivo desta norma é proporcionar um modelo para a criação, implementação, operação, monitorização, análise, manter e melhorar um Sistema de Gestão da Segurança da Informação.

A norma define uma abordagem ao processo, como a aplicação de um sistema de processos dentro de uma organização, juntamente com a identificação, interacções desses processos e da sua gestão. [ISO10b]
A estrutura deste standard contém onze domínios, cada um com o seu objectivo e com vários controlos a ser usados para os atingir. Os domínios estão apresentados na seguinte figura:

Figura 33 - Domínios ISO/IEC 27001

Cada domínio tem um objectivo diferente como estão apresentados na seguinte tabela[ISO05].:

Tabela 10 - Dominios detalhados ISO/IEC 27001

Domínio	Objectivos
Política de segurança	• Fornecer orientação e apoio à gestão da segurança da informação em conformidade com os requisitos de negócio, leis e regulamentos
Organização da Segurança Informática	• Gerir toda a segurança informática a nível interno da organização. • Manter a segurança das informações da organização e as instalações de processamento de informações que são acedidas, processados, comunicados, ou geridas por terceiros
Gestão de Activos	• Alcançar e manter a protecção adequada dos activos da organização, • Classificar a informação, garantir que esta quando recebida esteja com um apropriado nível de protecção.
Controlo de Acessos	• Controlar o acesso à informação • Garantir o acesso do utilizador autorizado e prevenir acesso não autorizado a sistemas de informação. • Impedir o acesso de utilizadores não autorizados, e

	comprometimento ou roubo de informações e de instalações de processamento de informações. • Impedir o acesso não autorizado aos serviços de rede. • Impedir o acesso não autorizado aos sistemas operativos. • Impedir o acesso não autorizado às informações mantidas nas aplicações de sistema. • Garantir a segurança da informação quando se utiliza a computação móvel e instalações de teletrabalho.
Conformidade	• Evitar a violação de qualquer lei, regulamentação ou obrigações contratuais e de quaisquer requisitos de segurança. • Assegurar a conformidade dos sistemas com as políticas e normas de segurança organizacional
Segurança RH	• Garantir que os funcionários, fornecedores e terceiros percebam quais as suas responsabilidades e se estão a desempenhar correctamente as funções que lhes foram atribuídas. • Reduzir o risco de roubo, fraude ou usos indevidos. Garantir que desempenham o seu trabalho durante o desempenho de funções na organização e quando alteração de funções, estas sejam geridas de forma apropriada.
Segurança Física	• Prevenir acessos não autorizados aos recursos físicos, de forma que não sejam danificados. • Prevenir falhas e roubos para que não comprometa o normal funcionamento das actividades na organização
Aquisição, Desenvolvimento e Manutenção de SI	• Garantir que a segurança é parte integrante dos sistemas de informação. • Evitar erros, perdas, modificação não autorizada ou utilização indevida de informações em aplicações. • Proteger a confidencialidade, autenticidade ou integridade das informações por meio de criptografia. • Garantir a protecção dos ficheiros de sistema. • Reduzir os riscos resultantes da exploração de vulnerabilidades técnicas
Gestão de Operações e Comunicações	• Garantir o funcionamento correcto e seguro das instalações de processamento de informação, • Implementar e manter um nível adequado de segurança de informação e prestação de serviços em consonância com terceiros, • Minimizar o risco de falhas do sistema, proteger a integridade do software e da informação, • Back-up. • Assegurar a protecção das informações em networks e a protecção das infra-estruturas de apoio.

	• Evitar a divulgação não autorizada, modificação, remoção ou destruição de bens e interrupção das actividades. • Manter a segurança de informações e troca de software dentro de uma organização e com qualquer entidade externa. • Garantir a segurança dos serviços de comércio electrónico • Detectar actividades não autorizadas de processamento de informação
Gestão de Incidentes de Segurança	• Garantir que eventos de segurança da informação e fragilidades associadas aos sistemas de informação são comunicadas de forma a permitir acções correctivas para estas serem tomadas em tempo útil. • Garantir uma abordagem coerente e eficaz aplicada à gestão de incidentes de segurança da informação
Continuidade de Negócio	• Neutralizar as interrupções de actividade empresarial • Proteger os processos críticos de negócio dos efeitos principais, deficiências dos sistemas de informação ou de desastres e assegurar a sua retomada em tempo útil.

Esta norma encontra-se alinhada com o modelo PDCA Plan-Do-Check-Act [PDAC10d] que é um modelo para estruturar processos e reflecte os princípios estabelecidos nas directrizes OECG. [OECG10c] Este modelo consiste em 4 passos que são executados repetidamente de forma a ter um melhoramento contínuo ao longo de todo o processo. A seguinte figura ilustra as várias fases e todo o processo.

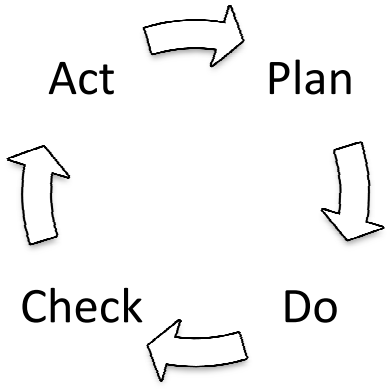

Figura 34 - Modelo PDCA

Cada uma das fases tem tarefas específicas como são apresentadas resumidamente na seguinte tabela.

Tabela 11 - Modelo PDCA

Fases	Descrição
Plan	Estabelecimento de políticas, objectivos, processos e procedimentos para a gestão de risco e melhoria da segurança da informação
Do	Implementação das políticas, controlos, processos e procedimentos.
Check	Avaliar, medição do desempenho de determinado processo. Analisar os resultados e identificar o que foi aprendido.
Act	Acções correctivas e preventivas, baseadas nos resultados da auditoria interna do ISMS.

Relativamente à sua aprovação, esta deve ser uma decisão estratégica. Além disso, a concepção e implementação de um SGSI da organização são influenciadas pelas suas necessidades e objectivos, requisitos de segurança e estrutura da organização.

ITIL (Information Technology Infrastructure Library)

O ITIL trata-se de um guia de boas práticas para a gestão de serviços em TI. Este guia promove uma gestão focada no cliente e na qualidade dos serviços de TI. As estruturas dos processos são orientadas para a gestão de uma organização de TI apresentando um conjunto abrangente de processos e procedimentos de gestão, organizados em disciplinas, com os quais uma organização pode fazer a sua gestão táctica e operacional de forma a alcançar o alinhamento estratégico com os negócios. [ITIL10a]

ITIL contém uma série de vários manuais de apoio para a gestão de serviços de TI. Actualmente, o ITIL já se encontra na versão 3.0, contando esta com uma estrutura que apresenta manuais distribuídos em 3 áreas:

- ITIL Core Publications
- ITIL Complementary Guidance
- ITIL Web Support Services

Considerando o ITIL Core Publications como o mais relevante, este será o único apresentado. Trata-se de um conjunto de 5 manuais (Sevice Strategies, Service Design,

Service Transition, Service Operation e Continual Service Improvement). Este modelo é ilustrado na seguinte figura.

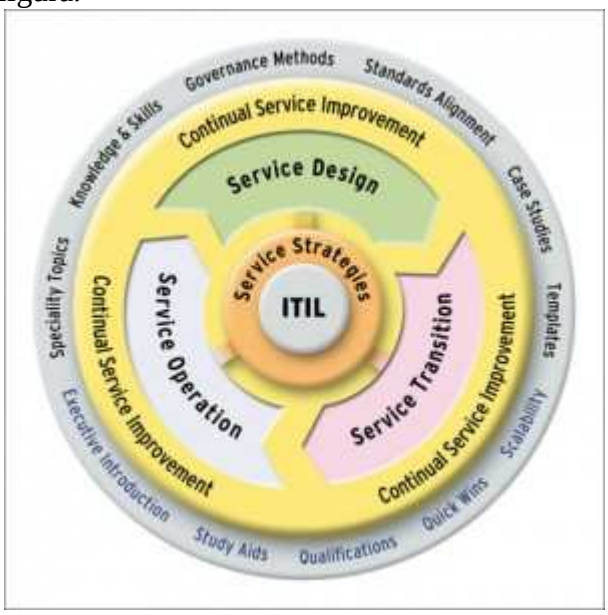

Figura 35 - Core Publications ITIL

Service Strategies

O manual Service Strategies estabelece uma estratégia global para serviços de TI e serviços de gestão de TI. Fornece instruções de como posicionar e definir os serviços como activos estratégicos.

Service Design

O manual de Service Design fornece orientações para a concepção e desenvolvimento de serviços e processos de gestão de serviços. O volume inclui princípios de concepção e métodos para a realização dos objectivos estratégicos em portfolios de serviços e bens de serviços. No entanto o âmbito do projecto não se limita só a novos serviços. Ele também contém conselhos sobre as mudanças e melhorias necessárias para melhorar ou manter o valor adicionado dos serviços em todo o ciclo de vida individual, garantir a sua continuidade, atingir os níveis de serviço e cumprir os requisitos em conformidade. Também é revista uma organização de serviço com conselhos valiosos sobre a questão de como os recursos de design para a gestão de serviços podem ser desenvolvidos e adquiridos.

Service Transition

O manual de Service Transition trata-se de um guia para desenvolver e melhorar as competências necessárias para a transição de serviços novos ou modificados em funcionamento. Este publicação fornece instruções de como os requisitos do Service Strategy pode ser devidamente implementado nos packages Service Design dentro do Service Operation e como o risco de erros e falhas pode ser minimizado. Práticas para a gestão de versões gestão de programas e gestão de risco são combinadas e formadas

dentro de um serviço de gestão num contexto baseado na prática. Também são fornecidas ferramentas para controlar a transferência dos serviços entre o cliente e o prestador de serviços.

Service Operation

O manual descreve práticas para a gestão do Service Operation. Isso inclui instruções sobre a eficácia e eficiência das entregas, bem como de apoio aos serviços, a fim de assegurar o real valor acrescentado para o cliente e consequentemente também o prestador de serviços. O manual contém instruções sobre como manter a estabilidade do serviço e permite mudanças nas áreas de design, escala, âmbito e nível de serviço.

Continual Service Improvement

O manual de Continual Service Improvement fornece instruções de uma forma instrumentalizada para a criação e manutenção de clientes de valor acrescentado em forma de melhorias no design de serviços, implementação e operação. Ele combina os princípios, práticas e métodos de gestão da qualidade, gestão de mudanças e melhorias do processo a fim de optimizar a qualidade do serviço. Estas instruções estão directamente ligadas durante as fases do Service Strategy, Design e Transition.

Para o leitor mais interessado, pode consultar mais detalhes acerca do ITIL em [ITIL10a].

(COBIT) Control Objectives for Information and related Technology

O COBIT tem como principal missão a pesquisa, o desenvolvimento, publicação e promoção de um determinado conjunto de padrões internacionais que sirvam de apoio às boas práticas referentes ao uso das TI. [Cob09].

O principal objectivo da *framework* disponibilizada pelo COBIT consiste em manter práticas e processos que estão relacionados com a infra-estrutura de sistemas, redes e dispositivos utilizados pela empresa. A análise destes processos deve orientar a organização na decisão de novos projectos e como utilizar as tecnologias neles, considerando também a evolução tecnológica, sistemas já existentes, integração com fornecedores, atendimento ao cliente (externo e interno), custo da tecnologia e retorno esperado. A necessidade de integração de sistemas e a evolução tecnológica são fundamentadas nos processos da metodologia, criando-se métricas para auditoria e medição da evolução das actividades destes processos.

Domínios de processos do COBIT

O COBIT está organizado em quatro categorias para a definição de um modelo para os processos de TI. Estas categorias são caracterizadas pelos seus processos e actividades executadas em cada fase de implementação de IT.

Planeamento e Organização (PO)

Define as questões estratégicas ligadas ao uso da TI em uma organização.

Aquisição e Implementação (AI)

Define as questões de implementação da TI conforme as directivas estratégicas e de projectos pré-definidos no Plano Estratégico de Informática da empresa, também conhecido como PDI (Plano Director de Informática).

Entrega e Suporte (DS)

Define as questões operacionais ligadas ao uso das TI para atendimento dos serviços para os clientes, manutenção e garantias ligadas a estes. O momento destes domínios é após a activação de um serviço e da sua entrega ao cliente, que pode operar ou utilizar os serviços da empresa para operação terciarizada.

Monitorizar e Avaliar (ME)

Define as questões de auditoria e acompanhamento dos serviços de TI, sob o ponto de vista de validação da eficiência dos processos e evolução dos mesmos em termos de desempenho e automação.

As áreas de Governance de foco do CoBiT são as seguintes:

- Strategic alignment - para assegurar a ligação do negócio com os planos de TI;
- Value delivery – Assegurar que as TI entreguem os benefícios definidos na sua estratégia
- Resource management – optimização do investimento e da gestão de recursos críticos de TI
- Risk management – trata dos riscos aos quais a empresa está sujeita
- Performance measurement – monitorização e acompanhamento das estratégias de implementação, dos projectos realizados, recursos usados, performance dos processos e da entrega de serviços