Departamento de Ciências e Tecnologias da Informação

[Escola de Tecnologias e Arquitectura]

Delegação de Gestão de Identidades

Pesquisa Aplicada a um Caso Prático na Administração Pública Portuguesa

David Diogo Ralo

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Informática e Gestão

Orientadora:

Profª. Doutora Isabel Machado Alexandre,

ISCTE-IUL

Co-Orientadora:

Mestre Maria Henriqueta Almeida,

GeRAP, EPE

Setembro, 2011

Agradecimentos

... A Carlos Rosa, meu pai, a Luísa Ralo, minha mãe, e a Carolina Rosa, minha irmã, pelo apoio ininterrupto e fé inabalável, e também pelos dias em que tive de os negligenciar para concluir a tese.

... À minha namorada, Nádia Fernandes, pela paciência, compreensão, apoio e força que sempre me ofereceu e por ser, para mim, uma inspiração.

... À Professora Isabel Alexandre pela constante preocupação e pela melhor orientação que eu poderia ter desejado.

...À Dra. Henriqueta Almeida pelos sábios conselhos que me ajudaram a não me desviar do caminho do sucesso.

... À GeRAP e a todos os seus colaboradores que contribuíram directa e indirectamente para este projecto pelos meios técnicos e pessoais e pela permanente disponibilidade e apoio que tornaram este trabalho possível.

... Ao André Barbosa, ao Ricardo Lopes, ao Miguel Gamanho, à Isabel Vala e ao Filipe Correia pela permanente disponibilidade e amizade com que me acompanham desde a licenciatura.

... À Clarisse Carriço, minha mentora, por tudo o que sei de ABAP até hoje e sem a qual não teria os conhecimentos para avançar.

Resumo

A gestão de utilizadores e perfis de autorização numa empresa, também denominada gestão de identidades, é uma actividade com uma importância crescente. Se, por um lado, um utilizador espera poder desempenhar as suas funções num sistema sem quaisquer problemas, por outro lado a empresa a que esse utilizador pertence espera que estejam implementadas e actualizadas todas as medidas de segurança necessárias para que ele possa executar apenas as actividades a que deve ter acesso.

Esta preocupação com a gestão de identidades é tanto maior quanto maior o número de sistemas a que um utilizador deve ter acesso, especialmente se esses sistemas estiverem ligados entre si.

Este trabalho pretende descrever um cenário em que, num sistema de recursos partilhados usado por diversos organismos da Administração Pública Portuguesa (APP), a gestão de identidades possa ser feita pelos próprios utilizadores através de um processo definido, transparente e controlado pela entidade central que assegura a manutenção do sistema.

Palavras-chave: gestão de identidades, recursos partilhados, processo definido e transparente para o utilizador final.

Abstract

The user and authorization profile management within a company, also known as identity management, is an activity with increasing importance. If, on the one hand, a user expects to be able to perform his job activities within a system without any problems, on the other hand the employing company expects that all necessary security measures are implemented and up to date in order to ensure that he can execute only the activities he's supposed to.

This concern with identity management increases when users need to have access to several systems, especially if those systems have some kind of relation.

This work intends to describe a scenario in which, within a shared resources system used by several organisms from the Portuguese Public Administration, the identity management can be done by the users themselves by means of a defined and transparent process controlled by the central entity that maintains the system.

Keywords: *identity management, shared resources, defined process and transparent to the end-users.*

Índice

Índice de Tabelas

Índice de Figuras

Abreviaturas e Siglas

APP – Administração Pública Portuguesa.

AD - (inglês) *Active Directory* → Directoria Activa. Tipo de Directoria (ver Glossário) usado no âmbito do projecto.

Backoffice – (inglês) → Trabalho de manutenção de um sistema que não tem visibilidade directa para o utilizador final.

Debug – (inglês) → Modo de execução de um programa no qual o código pode ser executado linha a linha.

et al. – (latim) E outros.

Flag – (inglês) – Mecanismo de sinalização técnico.

iView SAP – Janela em que o sistema SAP é embebido e utilizável num portal Web.

Phishing (termo técnico com base em inglês) - forma de fraude electrónica, caracterizada por tentativas de adquirir dados pessoais, na qual o agente fraudulento se faz passar por uma pessoa fiável ou uma empresa.

RFC – (inglês) *Remote Function Call* (ver Glossário).

SOA – (inglês) *Service Oriented Architecture*.

SP – (inglês) *Service Provider* → Prestador de Serviço.

SSO - (inglês) *Single Sign-On* → (ver Glossário).

Glossário

Os conceitos deste glossário têm na sua maioria por base as definições apresentadas pela empresa Hitachi ID Systems, Inc. (Hitachi, 2011) no âmbito das suas pesquisas e desenvolvimento de produtos na área da gestão de identidades.

Quando aplicável foram cruzadas essas definições com a ideia de outros especialistas.

As definições citadas encontram-se a itálico, sendo complementadas com considerações do autor apresentadas com um tipo de letra normal.

Sistemas

Sistema financeiro – portal Web partilhado pelos organismos da Administração Pública Portuguesa para a realização das suas actividades financeiras. Este portal, em tecnologia MS SharePoint, é a ferramenta visível para o utilizador final de uma arquitectura orientada a serviços (SOA), com sistemas de gestão de processos e de serviços, cujo sistema operacional é o SAP.

Directoria - *Serviço em rede que lista os participantes nessa rede: utilizadores, computadores, impressoras, grupos, com a intenção de ser um mecanismo robusto e conveniente para publicar e consumir informações sobre esses participantes*.

Na figura abaixo estão representados os utilizadores U1, U2 e U3, os grupos G1 e G2 e os organismos O1 e O2, num exemplo em pequena escala do modo como a *Active Directory* está organizada. Existem duas pastas principais: a de utilizadores e a de organismos, ambos considerados como objectos da Directoria.

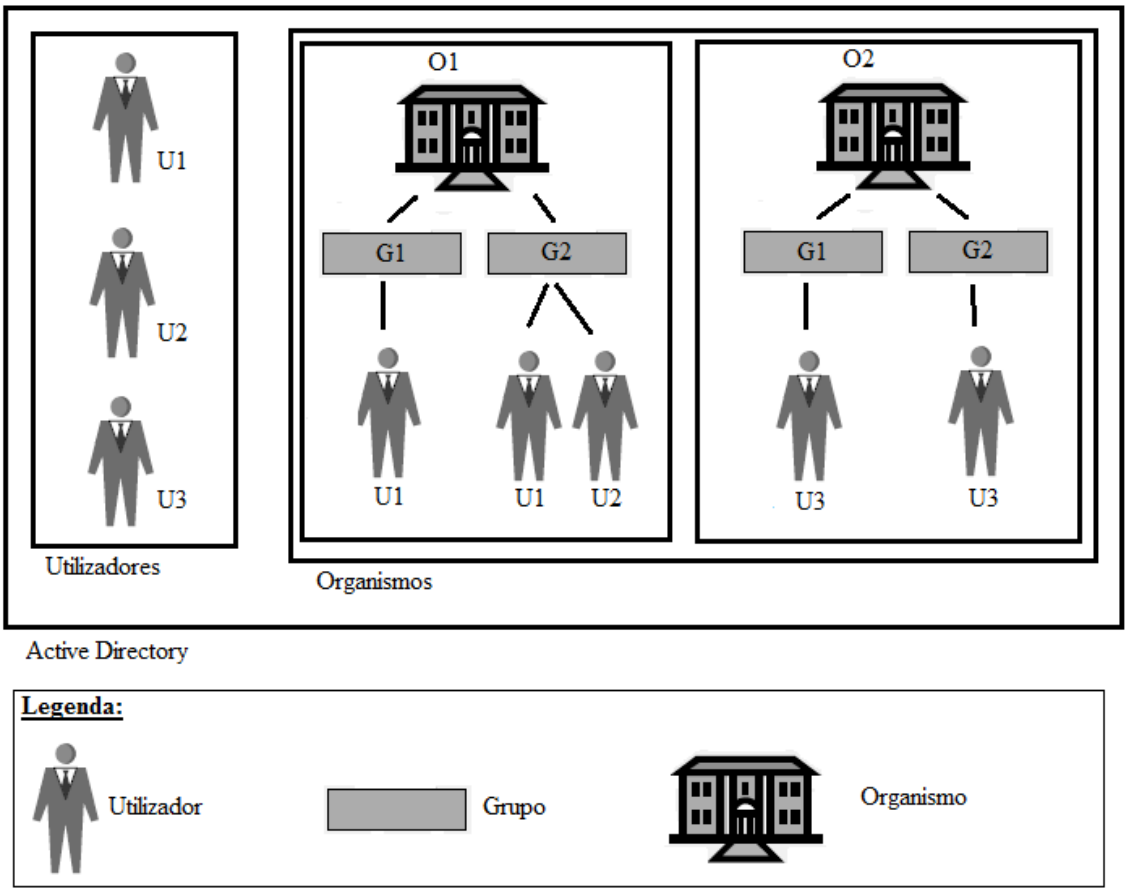


Figura de Glossário 0-1 - Active Directory (pequena escala)

Objecto de Directoria - *Algo que é guardado numa directoria e que pode ser armazenado numa hierarquia e conter atributos de identidade*.

Dentro de cada organismo encontra-se um conjunto de grupos de segurança, replicados em cada organismo mas diferentes entre si (o grupo G1 do organismo O1 é diferente do grupo G1 do organismo O2, embora ambos os grupos se destinem a oferecer as mesmas permissões para o seu organismo). Por sua vez dentro de cada um desses grupos encontram-se os utilizadores que têm acesso a esse grupo. No exemplo acima pode perceber-se que os utilizadores U1 e U2 pertencem ao organismo O1, estando o utilizador U2 apenas no grupo G2 ao passo que o utilizador U1 está nos grupos G1 e G2. Percebe-se ainda que o utilizador U3 pertence ao organismo O2.

Hierarquia de Directoria - *Uma directoria pode ser organizada em hierarquia de modo a tornar mais fácil a sua navegação e gestão. Esta hierarquia normalmente representa algo no mundo físico, tal como uma hierarquia organizacional ou localização*.

Participantes

Empresa responsável pela manutenção do sistema – apesar de o sistema financeiro em si ser propriedade de um dos organismos da APP, é a empresa em que foi realizado este projecto que é responsável pela sua manutenção.

Organismo da Administração Pública Portuguesa – Quando, neste trabalho, estiver referido um Organismo da APP, essa referência é restrita aos organismos que tenham aderido ao sistema financeiro mantido pela empresa, excepto nos casos em que seja explicitamente mencionado outro significado.

Utilizador - *Pessoa cujo acesso aos sistemas e respectiva informação de identidade deve ser gerido.*

O sistema financeiro gerido pela empresa destina-se apenas aos organismos da APP. Como tal, apenas podem ser utilizadores do sistema as pessoas que pertençam a estes organismos ou que pertençam à empresa responsável pela sua manutenção.

Aprovador - *As alterações a perfis e autorizações dos utilizadores podem estar sujeitas a aprovação antes de serem implementadas. Nestes casos, um ou mais aprovadores podem ter esta responsabilidade.*

Deste modo consegue-se controlar as alterações a efectuar a cada utilizador, uma vez que apenas um número restrito de pessoas tem autoridade para requerer essas alterações.

Actualmente todas as necessidades identificadas e devidamente autorizadas em termos de gestão de identidades são tratadas centralmente pela empresa que mantém o sistema. A implementação da ferramenta deste projecto permite que sejam esses aprovadores dos organismos (ou alguém por eles designado) a fazer essas actividades.

Processos de Negócio

Entrada - *Este é o processo em que os utilizadores entram para uma organização. Pode estar relacionado com novas contratações, subcontratações temporárias ou permissão de acesso a visitantes no sistema.*

Neste projecto em particular a Entrada conforme definida pela Hitachi tem sentido apenas em termos de novos colaboradores que entram para a empresa que mantém o sistema. No caso dos organismos da APP, estes designam um conjunto de trabalhadores que deverão dar Entrada no sistema, apesar de não passarem a pertencer à empresa que mantém o sistema pelo facto de estarem nele criados.

Criação de Utilizador - *Após a entrada na organização é dado a um utilizador o acesso ao sistema e aplicações, bem como um perfil para que consiga fazer o seu trabalho no dia-a-dia.*

Apoio de Acesso - *Os utilizadores podem ter dificuldades relacionadas com as suas permissões de segurança. Nestas situações contactam habitualmente um analista para obterem apoio. Esta pessoa ajustará então as permissões do utilizador conforme necessário.*

Apoio de Autenticação - *Por vezes os utilizadores podem ter dificuldades em entrar num sistema ou aplicação. Isto pode acontecer por esquecimento da sua palavra-chave ou porque activaram um bloqueio contra intrusos. Nestes casos podem contactar um analista para apoio, nomeadamente para recuperação de palavras-chave ou desbloqueio de utilizadores.*

Pedidos de Apoio – Tanto para o Apoio de Acesso como de Autenticação, são feitos pedidos técnicos/funcionais que são encaminhados para a equipa de gestão de identidades da empresa central, através de um processo existente no portal. Em contacto com o utilizador, esta equipa procura então solucionar do modo mais adequado cada situação que surge.

As novas funcionalidades implementadas por este projecto de delegação de gestão de identidades permitem que estas situações sejam resolvidas de modo simples, pelo próprio organismo, com pouca ou nenhuma necessidade de intervenção por parte da equipa central.

Término - *Eventualmente todos os utilizadores deixam a organização. A esta situação dá-se o nome de término, sendo necessário desactivar os acessos do utilizador no sistema.*

Desactivação de Acessos - *Quando ocorre o término de um utilizador, os seus direitos de acesso ao sistema e às aplicações da organização devem ser removidos*.

Pedido de Bloqueio - Outro tipo de pedido que é feito por parte dos organismos está relacionado com a desactivação de utilizadores. Por diversos motivos um trabalhador de um organismo da APP pode deixar de exercer as suas funções, dando-se o seu Término no seio da organização, sendo de importância vital, por questões de segurança, vedar os seus acessos ao sistema. À semelhança dos restantes pedidos, também o bloqueio de utilizadores é tratado a nível central pela equipa de gestão de identidades. Uma das funcionalidades pretendidas deste projecto é precisamente a de permitir aos organismos da APP bloquear os seus utilizadores no sistema.

Identificação e Autenticação

Conta de Acesso - *Sistemas e aplicações nos quais os utilizadores tenham a capacidade de entrar e aceder a funcionalidades e dados, geralmente associam uma conta de acesso a cada utilizador. Estas contas habitualmente incluem um identificador único para o utilizador, meios de autenticação, permissões de segurança e informações específicas do utilizador*.

Os utilizadores com acesso ao sistema são actualmente identificados através de duas vertentes. Por um lado têm o seu utilizador de acesso ao portal Web, guardado num sistema de *Active Directory*. Por outro lado têm um utilizador SAP, guardado no próprio sistema SAP da empresa central. O conjunto formado por "nome de utilizador portal", "nome de utilizador SAP" e "endereço de e-mail" identifica um utilizador univocamente.

Atributos de Identidade / Identificadores - *Cada informação identificativa de um utilizador pode ser vista como um atributo desse utilizador. Estes podem ser guardados num ou mais sistemas de informação*.

Autenticação - *Processo através do qual um utilizador prova a sua identificação a um sistema, normalmente ao aceder a esse sistema*.

Os utilizadores têm apenas acesso às suas credenciais de autenticação no portal Web, sendo a autenticação em SAP feita através de um mapeamento entre o nome de utilizador no portal e o nome de utilizador SAP. O modelo usado para esta autenticação

encontra-se explicado em maior detalhe no capítulo "5.1.3 Modelo de Autenticação Usado no Sistema do Projecto".

Single Sign-On - *O Single Sign-On (SSO) é qualquer tecnologia que substitua múltiplos acessos em sistemas independentes por um único processo de autenticação, para que os utilizadores não tenham de se autenticar várias vezes*.

Perfil de Utilizador - *Conjunto de contas de acesso, atributos de identidade e permissões de segurança associados a um único utilizador*.

Para os utilizadores do sistema a ideia de "Perfil" é a de algo único directamente associado ao seu utilizador e que garante todos os acessos necessários às actividades do portal Web. No entanto, à semelhança da identificação de utilizadores também as permissões são feitas em duas vertentes: portal Web e SAP. As actividades a que um utilizador tem acesso no portal Web dependem da sua associação ao que a Hitachi define como Grupos de Segurança. Estes grupos estão definidos na *Active Directory* e são replicados para cada organismo no sistema.

Grupos de Segurança - *Um grupo de segurança é um conjunto de utilizadores, tendo cada grupo um nome único. São geralmente criados para facilitar a definição de permissões de segurança, permitindo atribuir várias permissões ao grupo em vez de as atribuir a cada utilizador.*

Gestão de Permissões - *Conjunto de tecnologias e processos usados para gerir, de forma coerente, os direitos de segurança numa organização, com o objectivo de reduzir os custos de gestão, melhorar o serviço e assegurar que os utilizadores recebem exactamente as permissões que necessitam. Estes objectivos são alcançados através da criação de processos consistentes e robustos, que fornecem ou retiram permissões em vários sistemas e aplicações:*

1) *Criar e actualizar regularmente uma base consolidada de permissões;*
2) *Definir funções de modo a que as permissões possam ser atribuídas aos utilizadores em moldes compreensíveis pelos próprios;*
3) *Permitir pedidos e aprovações em regime self-service, de modo a que as decisões sobre permissões possam ser feitas pelos utilizadores funcionais com conhecimento do contexto e não por utilizadores mais técnicos;*
4) *Sincronizar permissões entre sistemas, quando apropriado;*

5) *Convidar periodicamente especialistas para reverem as permissões e funções associadas aos utilizadores de modo a identificar situações que já não sejam apropriadas e tenham de ser revistas ou removidas.*

Controlo de Acessos Baseado em Funções

Função Simples - *Conjunto de permissões definidas no contexto de um único sistema. Normalmente são usadas para simplificar a gestão da segurança em sistemas e aplicações ao encapsular conjuntos de permissões comuns e atribui-los como um pacote.*

Além da vertente de grupos de segurança na *Active Directory,* que está directamente relacionada com o portal Web, cada utilizador tem associado ao seu utilizador SAP um conjunto de funções que dão acesso às transacções SAP com diferentes graus de liberdade (entre exibição, modificação e criação de dados). Apesar do que o nome indica, no contexto da empresa, as funções SAP não correspondem a funções desempenhadas mas sim a processos e actividades. A título de exemplo existem determinadas funções que permitem a consulta de dados, dividindo-se entre orçamentais, tesouraria, contas a pagar/receber, etc., abrangendo todos os módulos financeiros contemplados no portal.

Alteração de Função - *Processo de negócio no qual as funções de trabalho de um utilizador mudam e, consequentemente, o conjunto de funções e permissões que tem associadas deve também mudar. Pode ser necessário retirar antigas permissões, manter algumas e acrescentar novas.*

Gestão de Funções - *As funções num sistema e a sua atribuição dificilmente se manterão estáticas por muito tempo. Por essa razão devem ser geridas tanto a nível das permissões que lhes estão associadas como dos utilizadores a que estão atribuídas.*

Pedido de Alteração - *Consiste numa ou mais propostas de alteração a perfis de utilizador, tais como a criação de novos perfis, acrescento de novas contas a perfis já existentes ou alteração de atributos de identidade. Estes pedidos podem estar sujeitos a aprovação.*

Uma vez que, para os utilizadores, a dupla vertente de perfis (o sistema mantido pela empresa tem permissões diferentes mas interligadas no portal Web e em SAP) é

transparente, os pedidos de apoio técnico/funcional que chegam até à equipa de gestão de identidades têm de ser cuidadosamente analisados para se determinar a que nível é necessário agir.

Administração Consolidada - *Um sistema de administração consolidada permite a um administrador de permissões criar, modificar e apagar registos de utilizadores em vários sistemas em simultâneo. O objectivo é tornar mais eficiente a gestão de utilizadores em oposição a várias ferramentas de gestão independentes em cada sistema.*

Dada a transparência da camada SAP para o utilizador, pretende-se que a gestão de identidades feita pelos organismos através do portal Web tenha efeitos tanto sobre a camada de grupos de segurança que afectam directamente o portal Web como na camada de funções SAP sem que os utilizadores se apercebam directamente disso. Consegue-se assim uma Administração Consolidada de todos os sistemas num único processo.

Administração Delegada - *Um sistema de administração delegada permite que alguns utilizadores administrem as contas de outros utilizadores em alguns sistemas. A intenção é retirar a gestão de utilizadores de uma equipa técnica central e descentralizá-la de modo a que esta gestão seja feita por uma equipa técnica ou funcional mais directamente ligada aos utilizadores.*

Conceitos Técnicos

Uma vez que o projecto tem uma vertente técnica, nomeadamente de SAP, é conveniente definir dois conceitos que serão relevantes nesta tese, de acordo com a própria empresa (SAP, 2011):

RFC (SAP) – *"Remote Function Call" é o protocolo usado pela SAP para comunicação remota, ou seja, entre sistemas independentes. Estes podem ser dois sistemas SAP distintos ou mesmo um sistema SAP e um sistema não-SAP.*

BAPI (SAP) – *"Business Application Programming Interfaces" são conjuntos de métodos para trabalhar e manipular os objectos de negócio SAP. Além de poderem ser usadas independentemente, os módulos de função por trás das BAPIs podem ser usadas*

dentro de uma RFC. Isto oferece uma razoável estabilidade uma vez que só a SAP pode criar BAPIs, sendo consideradas programação Standard.

1. Introdução

A tendência actual nas empresas é no sentido de consolidar e integrar a gestão dos seus utilizadores num sistema central, permitindo reduzir custos operacionais e de apoio, ao mesmo tempo que aumentam a segurança relacionada com a gestão de identidades e acessos (Berndt *et al*, 2005). Esta gestão de identidades tem, precisamente, vindo a tornar-se um tópico chave quando se fala em segurança de informação, nomeadamente pelo aumento nos roubos de identidade (Ian Grant, 2007).

Este trabalho baseia-se num projecto dentro de uma empresa de gestão de recursos partilhados nos sistemas da Administração Pública Portuguesa (APP). Esta empresa disponibiliza um sistema aos vários organismos da APP para que, através de um portal padrão comum a todos os organismos, realizem as actividades necessárias de âmbito financeiro. A gestão de utilizadores neste sistema é feita de forma centralizada. No entanto, o aumento progressivo do número de organismos utilizadores do sistema (que se pretende no futuro abranger toda a APP) torna necessária uma revisão e evolução do método de gestão de identidades usado, para o tornar escalável sem implicar um aumento proporcional de recursos afectos a essa gestão.

A intenção é oferecer aos organismos utilizadores do sistema, ferramentas de criação e edição dos seus próprios utilizadores, guardando os dados correspondentes de forma centralizada, através de um fluxo de processos previamente delineado e implementado. Pretende-se com esta mudança que o foco dos gestores de identidades da empresa seja mais em questões de fundo (como a manutenção e evolução do processo de gestão de identidades) e menos dedicado a pequenas necessidades locais de cada organismo. Com a existência de processos para o efeito, estas passam a ser resolvidas também a nível local.

Apesar da base da prestação de serviços de recursos partilhados desta empresa ser um sistema SAP, e de muitas das actividades financeiras dos organismos serem ainda executadas directamente em SAP mediante *iViews* (ver Abreviaturas e Siglas), a tendência é para que todas as actividades passem a ser executadas através de processos simplificados via portal Web. Seguindo esta lógica, também a gestão de identidades, que tem repercussões noutros sistemas além do próprio SAP, se pretende

completamente transparente para os utilizadores dos organismos, fazendo-se apenas através do portal Web no qual se baseia o sistema de gestão de recursos financeiros.

2. Gestão de Identidades

É importante perceber o que faz da gestão de identidades uma área com uma importância crítica, bem como o que pode motivar um gestor de identidades a procurar meios de colocar essa gestão nas mãos dos próprios utilizadores. Neste problema em particular há que ter em conta que as tarefas de gestão de identidades ocupam períodos consideráveis de tempo a um gestor central, que tenha de dar resposta às solicitações dos diversos organismos. Apesar disto, para cada organismo individualmente, os resultados produzidos são difíceis de identificar e quantificar, estando o foco na resolução rápida dos problemas. No fundo, os utilizadores de um sistema numa organização esperam *a priori* que o seu trabalho nesse sistema decorra sem problemas, raramente tendo noção do trabalho de "bastidores" que essa estabilidade exige (ver *backoffice* em Abreviaturas e Siglas).

Por outro lado, em sistemas tão críticos para o país como os de gestão financeira da APP, com particular relevo num período em que as Contas Públicas serão alvo de um apertado controlo por parte de instituições internacionais (Memorando de Entendimento, 2011), seria inconcebível delegar totalmente a gestão de identidades nos organismos e permitir aos utilizadores o livre acesso à edição das suas permissões. Com este projecto pretende-se resolver o problema da delegação da responsabilidade de gestão de identidades, sem descurar o problema de controlar quais os utilizadores que podem fazer essa gestão e até que limites. Para responder a esta questão da limitação de poderes, a intenção é conceber processos de gestão, apoiados num portal Web e com acesso a editar apenas o necessário, permitindo aos utilizadores executar esses processos mediante uma validação das suas permissões.

Convém ainda clarificar que, no âmbito deste sistema em particular, os utilizadores do portal Web precisam de possuir perfis definidos e relacionados em dois grandes níveis:

- Permissão para acesso a funcionalidades do sistema no portal, definidas num sistema de *Active Directory* (ver Glossário);
- Permissão para executar as acções SAP equivalentes a essas funcionalidades, definidas em SAP.

A título de exemplo, um utilizador que tenha permissão de acesso à área de Contabilidade Orçamental no portal terá também de ter permissões SAP que lhe permitam executar acções relacionadas com o Orçamento do seu organismo. De igual modo, um utilizador que tenha permissões SAP para executar acções relacionadas com Tesouraria mas que não tenha acesso à área de Tesouraria no portal não poderá fazer o seu trabalho.

O diagrama abaixo expressa, de forma simplificada, o trabalho que tem de ser actualmente realizado por um gestor de identidades em termos de configurações:

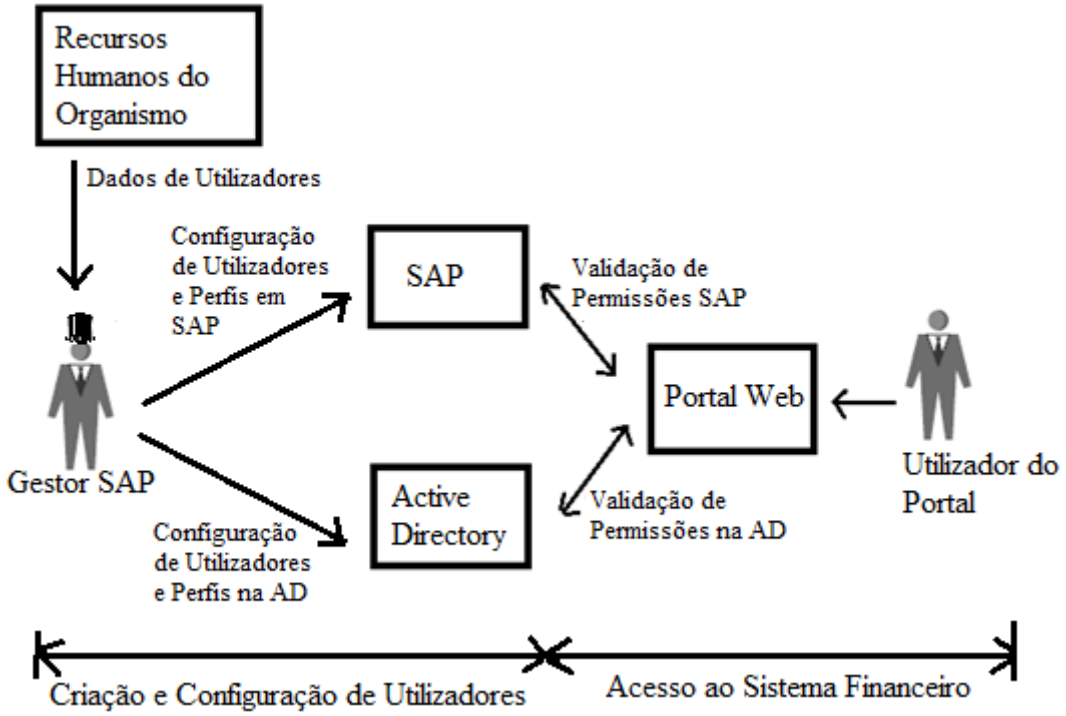


Figura 2-1 Esquema simplificado da gestão de identidades no sistema

Ou seja, o gestor de identidades baseia-se na definição de permissões enviada pelo organismo para configurar os seus utilizadores em SAP e na AD. Deste modo, para que um utilizador tenha acesso às actividades do portal Web, as suas permissões em ambos os sistemas têm de ser validadas.

2.1 Motivação e Justificação

A motivação para a realização deste trabalho passa pela entrada do autor no mercado de trabalho, e pelo facto de ter iniciado precisamente a sua actividade como gestor de identidades. Apesar de ter sido apresentada como uma área bastante crítica, a

morosidade das actividades a ela associadas produzem alguma relutância entre os técnicos SAP em aceitar esta função. Este paradoxo, aliado à continuação do trabalho do autor na área de gestão de identidades e da percepção de que rapidamente o volume de trabalho começa a atingir proporções exponencialmente maiores, acaba por se constituir como uma motivação tanto de interesse pessoal como profissional para a realização deste projecto.

O autor desta tese identifica ainda duas grandes justificações ou pontos de interesse na realização deste projecto.

De um ponto de vista mais científico, a ferramenta que o projecto se propõe conceptualizar e implementar tem uma abordagem inovadora na Administração Pública Portuguesa, permitindo a gestão de identidades num sistema SAP, através de uma interface simples e acessível a utilizadores com diferentes níveis de experiência informática.

Numa vertente mais empresarial este trabalho irá procurar identificar benefícios e riscos da delegação controlada da gestão de identidades nos próprios utilizadores tanto para a empresa que mantém o sistema, como para quem nela gere identidades.

2.2 Objectivos

Perante um cenário de aumento constante do número de utilizadores do sistema financeiro, este trabalho terá como objectivo principal, aliado ao projecto a desenvolver, determinar os factores que levam um gestor de identidades a colocar do lado dos utilizadores, uma parte da sua gestão de identidades.

Dentro deste grande objectivo enquadram-se ainda alguns objectivos mais específicos, nomeadamente:

- Identificar riscos em dar este tipo de poder aos utilizadores;
- Sugerir soluções minimizadoras dos riscos encontrados.

Com o desenvolvimento do projecto de gestão de identidades no portal pretende-se dotar os utilizadores, numa fase inicial, das ferramentas para criar e desactivar utilizadores para o seu organismo. Evoluções posteriores do projecto permitirão uma gestão de identidades através da qual os utilizadores autorizados conseguirão definir

permissões de acesso e restrições para o seu organismo, devendo existir sempre o cuidado de limitar, no sistema central, o âmbito dessas modificações.

2.3 Problema

Tendo por base os objectivos indicados, é possível levantar duas grandes questões:

1. Quais as razões para um gestor de identidades desejar delegar a gestão nos utilizadores?
2. Como pode um gestor de identidades fazer essa delegação com um risco reduzido?

Partindo destas duas questões o problema que se coloca é o seguinte:

- Como pode um gestor de identidades de um sistema financeiro na Administração Pública Portuguesa delegar essa gestão nos utilizadores do sistema, controlando o risco associado a essa delegação?

3. Revisão da Literatura

3.1 Introdução

De acordo com Audun Jøsang e Simon Pope (2005) a gestão de identidades é tradicionalmente vista do lado de quem fornece o serviço. Estas entidades desenham os sistemas de gestão de modo a obterem custos de eficiência e escalabilidade, o que não significa necessariamente uma preocupação com a facilidade de uso por parte do utilizador. No mundo actual em que o crescimento de serviços *online* é exponencial, começa a tornar-se insustentável a memorização de várias credenciais.

Estes autores sugerem, assim, uma visão da gestão de identidades centrada no utilizador e não no prestador de serviço, fazendo a distinção entre o que denominam por Modelos Tradicionais de Gestão de Identidades e os Modelos Centrados no Utilizador.

O âmbito deste projecto não pretende mudar o modelo usado pela empresa responsável pela manutenção do sistema para acesso ao mesmo, que se enquadra num tipo de Modelo Tradicional, mas sim tornar o acesso e utilização mais simples, e parametrizados de modo a poderem ser usados pelos organismos inseridos no sistema.

Audun Jøsang e Simon Pope (Jøsang & Pope, 2005) escrevem que a disponibilização de serviços e recursos através de redes de computadores implica muitas vezes a necessidade de saber quem são os utilizadores e a que serviços têm acesso. Neste contexto, a gestão de identidades tem essencialmente duas fases:

1. A disponibilização ao utilizador de credenciais de identificação e de identificadores únicos perante o sistema (registo);
2. A autenticação dos utilizadores e o controlo dos seus acessos a serviços e recursos com base nas suas credenciais e identificadores.

Esta perspectiva de duas fases aplica-se bem ao sistema em que o projecto se insere embora, até que a ferramenta esteja totalmente implementada, não seja o utilizador a registar-se no sistema, mas sim um gestor de identidades da empresa central a criá-lo e a atribuir-lhe as respectivas credenciais. Numa fase posterior do projecto, passarão a ser os responsáveis de cada organismo a tratar desta criação e da atribuição de credenciais dos utilizadores do seu organismo.

3.2 Delegação

O conceito de delegar pode ser visto como uma distribuição de trabalho, atribuindo tarefas específicas ou responsabilidades a um indivíduo, segundo Jeanne Nyquist (2007). Nyquist diz que a delegação requer *expectativas definidas, comunicação, acompanhamento, monitorização, feedback e confiança* (Nyquist, 2007).

Dentro do conceito alargado de delegação há um mais específico que é o de delegação de autoridade, enunciado por David Chadwick como *permitir a alguém agir em nosso nome para desempenhar tarefas ou consumir recursos que estariam disponíveis apenas para nós* (Chadwick, 2006). No caso deste projecto, é este o conceito que melhor se aplica, uma vez que se pretende passar aos utilizadores dos organismos a autoridade e meios para efectuarem acções que anteriormente eram da responsabilidade da empresa central.

No entanto, Chadwick também refere os perigos de uma delegação de autoridade total em que aqueles sobre quem delegamos a nossa autoridade nos personificam, ficando com acesso a tudo o que nós poderíamos fazer sem possibilidade de controlo adequado. Chadwick apresenta como uma boa solução permitir ao indivíduo em quem se delegou autoridade agir em seu próprio nome e com uma autoridade limitada, contendo apenas uma fracção (necessária) dos poderes de quem delega.

Esta estratégia de delegar apenas alguma da autoridade sobre o próprio utilizador pode ser adoptada, em traços gerais, de duas formas:

1. Indicar explicitamente os utilizadores que devem ter determinadas permissões;
2. Criar conjuntos de permissões agrupados em funções e atribuir essas funções a cada utilizador. Um exemplo prático desta estratégia seria a criação da função de "Gestor de Identidades" que seria depois associada a alguns utilizadores dentro de cada organismo.

3.3 Conceitos de Identidade e Identificação

O projecto FIDIS (Future of Identity in the Information Society) pretende especificar uma conceptualização do domínio de Identidades para ser usado tanto por especialistas na matéria como por curiosos (Nabeth & Hildebrandt, 2005).

Uma das primeiras preocupações do projecto FIDIS foi a de diferenciar as dimensões de identidade e identificação:

- Identidade – *conjunto de características que representam uma pessoa no contexto de actividades práticas*;
- Identificação – *conjunto de termos, conceitos e mecanismos relacionados com a disponibilização de informações sobre uma identidade e com o uso dessas informações. Refere-se ao processo de ligar uma pessoa à sua identidade*.

Outra distinção importante é feita entre as características de uma pessoa e a identidade de uma pessoa (Hildebrandt, 2005; Ricoeur, 1992). O primeiro conceito refere-se a elementos muito constantes e que sofrem apenas alterações pontuais e é aquele que *pode ser explicitamente formalizado e manipulado pelas tecnologias de informação e identificação.* O segundo conceito representa quem a pessoa realmente é de um ponto de vista mais filosófico, sendo frequentemente alterado e difícil de determinar com precisão, *estando fora do âmbito do que pode ser definido pelas tecnologias*.

3.3.1 Identidade

O conceito de identidade intervém em diversos aspectos da vida de uma pessoa, como se pode ver pela Figura 3-1 que relaciona a identidade da Alice com diversos contextos.

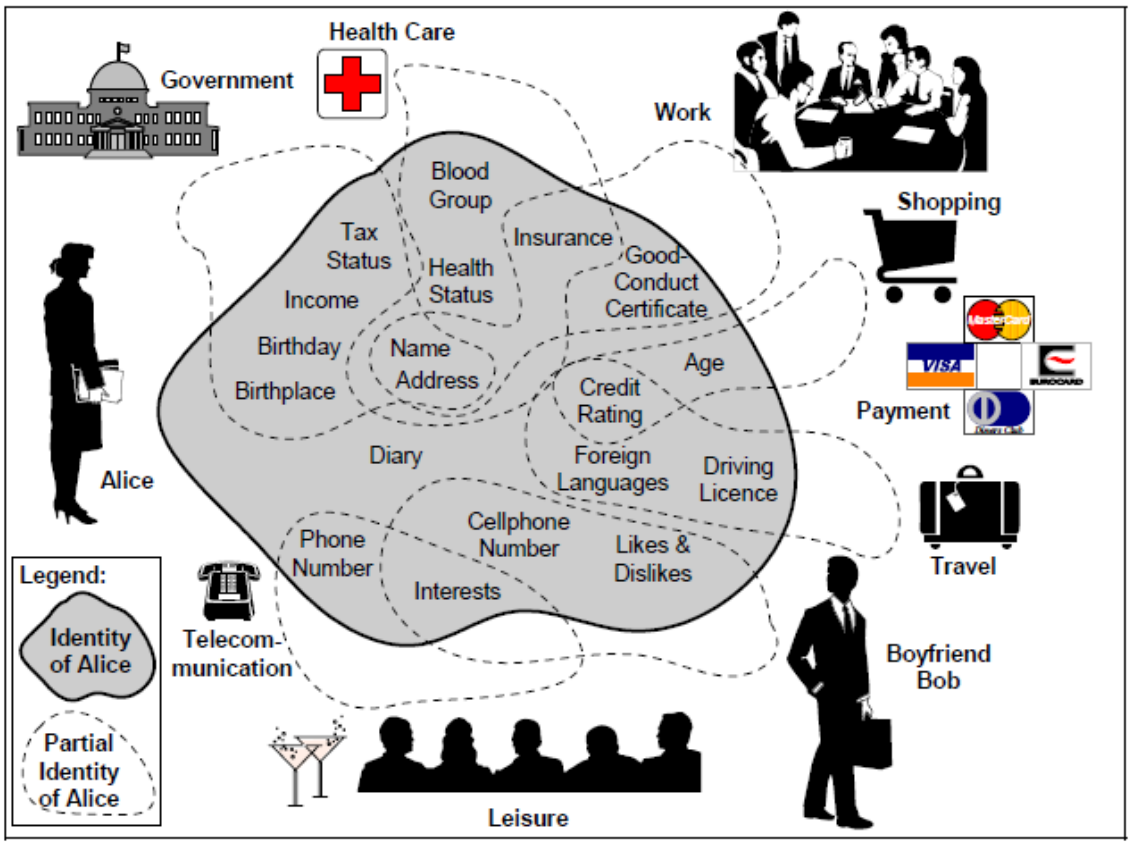


Figura 3-1 Um exemplo das múltiplas facetas da Identidade

(fonte: Alice's Partial Identities (Clauß & Köhntopp, 2001))

Estas identidades parciais, dependentes do contexto em que se inserem, podem incluir características intemporais (nacionalidade, género, …), adquiridas ao longo da vida (diplomas, competências, …) ou correspondentes a uma dada função (posição, autoridade, …).

O projecto FIDIS chama a atenção para o facto de que a "digitalização" da sociedade actual não criou as questões relacionadas com o conceito de identidade, mas veio sim ampliá-las. Hoje em dia torna-se necessário proteger as liberdades de cada um sem descurar o reforço da responsabilização num "terreno digital" em que é difícil estabelecer fronteiras aceites por todos.

Não explorando extensamente definições filosóficas, podem definir-se de forma simples três conceitos interligados:

- O Eu – *Uma perspectiva indeterminada na primeira pessoa*;
- O Eu implícito – *Como uma pessoa se vê a si mesma*;

- O Eu explicito – *Como uma pessoa é percebida pelos outros e qual a imagem que passa para os que a rodeiam*.

Esta categorização é importante para referir as seguintes questões, levantadas pelo projecto FIDIS:

Uma representação de alguém será sempre imperfeita – Uma vez que temos de reduzir uma pessoa a atributos concretos e dependentes de contexto, podem aparecer conflitos entre o modo como uma pessoa se vê e o modo como é vista pelos outros. De modo a manter estes atributos livres de redundâncias e falsas informações, as leis europeias impõem que os detentores de bases de dados de informações pessoais disponibilizem mecanismos que permitam a cada pessoa corrigir as suas informações falsas nessa base de dados.

A questão do controlo – Uma pessoa não controla todos os atributos da sua identidade, sendo que boa parte destes é mantida por governos e outras instituições (ex: segurança social), empresas (ex: bancos, locais de trabalho), lojas (ex: dados de marketing) ou até pela própria opinião pública (ex: jornais). Este problema pode ser combatido através de mecanismos (técnicos, legais, …) que imponham boas práticas quando qualquer entidade acede e gere informações pessoais.

Pessoa Virtual – Muitas vezes não se conhece (nem é esse o objectivo principal) a "pessoa" que pretendemos identificar. Considere-se a pergunta "Quem é o administrador desta rede?". Neste caso o interesse não é em saber o nome da pessoa que administra a rede mas sim a quem nos devemos dirigir quando queremos tratar de assuntos relacionados com a administração da rede, podendo até tratar-se de um grupo de pessoas. Uma pessoa virtual é, assim, *uma máscara que representa uma responsabilidade ou função ou a posse de um determinado conhecimento, e que pode ser usada por um indivíduo ou por um grupo de pessoas*. Apesar desta máscara, é sempre possível identificar e responsabilizar, se necessário, a entidade que usa essa máscara num determinado momento.

3.3.2 Identificação

A Identificação é enunciada pelo projecto FIDIS como sendo o *conjunto de abordagens e mecanismos para descobrir informações de Identidade*. Contém conceitos como:

- Anonimato – *estado de não divulgação de informação de identidade*;
- *Unlinkability* (impossibilidade de ligar) – *propriedade de um sistema de não divulgar informação sobre as relações que possam existir entre diferentes itens*;
- Identificadores – *item de informação que pode ser usado para fornecer um certo nível de autenticação a uma entidade*.

Os usos mais comuns de identificação ocorrem em casos de:

- *Controlo de acessos a recursos/áreas restritos*;
- *Exploração de informação de identidade*;
- *Monitorização para permitir responsabilizar*.

O projecto FIDIS refere ainda os riscos associados ao processo de Identificação, podendo os problemas ter duas grandes causas:

Identificação Incorrecta – *O nível de fiabilidade de uma identificação raramente é absoluto*. São exemplos a facilidade de obter os dados de acesso de terceiros, tentativas de *phishing* (ver Abreviaturas e Siglas) ou páginas falsas na Internet que imitam na perfeição os sites reais. As consequências de uma identificação incorrecta podem ser graves, nomeadamente quando se trata de informações confidenciais que são divulgadas.

Identificação Indesejada – O comércio electrónico ou programas de infiltração de sistemas e registo de credenciais ou de actividades, *tipicamente revelam informação contra a vontade da pessoa e às suas custas, uma vez que essa informação pode ser usada para manipular alguém e levá-lo a efectuar uma compra*. No local de trabalho, a divulgação indesejada da informação de alguém pode ter graves consequências para essa pessoa, incluindo o despedimento. Também enquanto cidadãos, a revelação de informações pessoais pode ter consequências sociais ou legais.

Há ainda dois mecanismos de identificação que são detalhados no projecto FIDIS:

Identificação Explícita – *Processo em que a pessoa está ciente e até coopera com a sua identificação.* São exemplos os ecrãs de acesso a sistemas, o uso de cartões multibanco ou até a apresentação a alguém.

Identificação Implícita – *Processo usado para identificar alguém sem que essa pessoa se aperceba*. Pode ocorrer a partir da análise de ficheiros de registo a partir dos quais a informação pessoal pode ser extraída.

3.4 Modelos de Gestão de Identidades

De acordo com Audun Jøsang e Simon Pope, existem alguns modelos mais usados na definição de estruturas de Gestão de Identidades (Jøsang & Pope, 2005).

3.4.1 Modelo de Identidade Isolada

O modelo mais comum de gestão de identidades consiste em ter os prestadores de serviço a agir tanto como fornecedores de credenciais como de identificadores aos seus clientes. Controlam, assim, o domínio de nomes do seu serviço e atribuem identificadores e credenciais únicas aos utilizadores, que ficam com identificadores e credenciais únicos em cada serviço com o qual mantêm transacções:

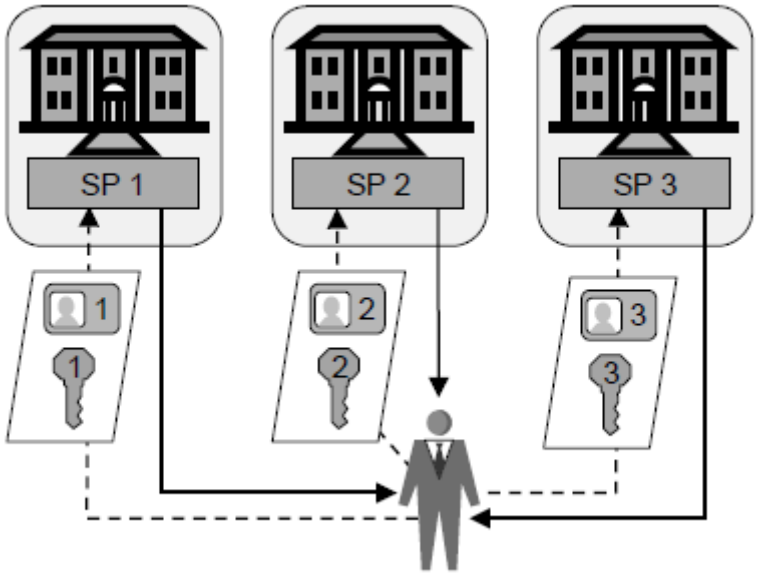


Figura 3-2 Modelo de Identidade Isolada

Esta abordagem actualmente é cada vez menos sustentável para o utilizador dado o crescimento exponencial de serviços que carecem de autenticação.

Para este projecto em concreto este modelo não é muito relevante, uma vez que estamos perante um único local onde o utilizador tem de se autenticar para ter acesso às permissões de dois grandes sistemas. Uma vez que este modelo não apresenta relações

entre as identidades de um utilizador em dois sistemas diferentes, não permite de forma imediata alcançar o pretendido.

3.4.2 Modelo de Identidade Federado

Este modelo pretende colmatar algumas das ineficiências do modelo anterior, ao definir um conjunto de acordos, padrões e tecnologias que permitem a um grupo de fornecedores de serviço reconhecer as identidades de utilizador e permissões dadas por outros fornecedores de serviço no mesmo domínio.

Num domínio de identidades federado é então feito um mapeamento das diferentes identidades de um único cliente, ligando-as para que, ao autenticar-se perante um determinado fornecedor de serviço fique autenticado perante os restantes que pertençam a esse domínio.

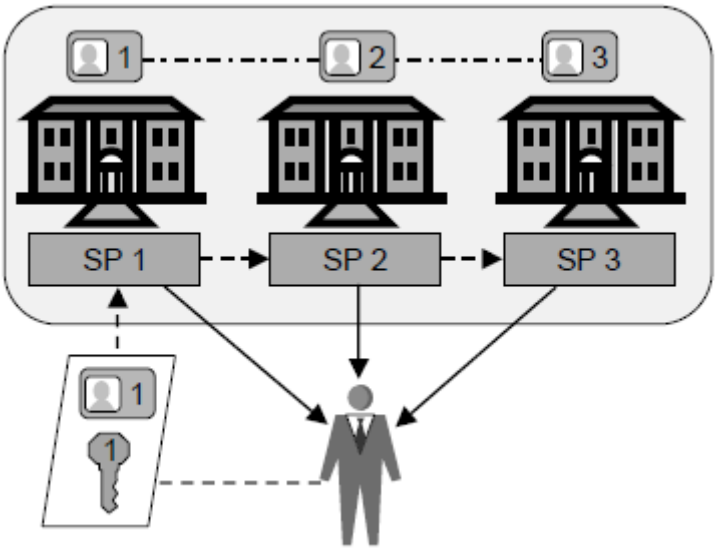


Figura 3-3 Modelo de Identidade Federado

Este modelo dá ao cliente a ilusão de que está perante um domínio de identificação único, apesar de ser possível o utilizador memorizar e autenticar-se com as diferentes credenciais de cada fornecedor de serviço.

No sistema da empresa, o modelo usado usa parte da ideologia de Identidade Federada, embora vedando o acesso à autenticação directa perante o sistema SAP. Esta camada está a tornar-se progressivamente transparente para o utilizador final que cada vez mais interage apenas directamente com o portal Web.

3.4.3 Modelos de Identidade Centralizados

Nestes modelos existe um único conjunto de credenciais que é usado por todos os fornecedores de serviço.

No caso particular do sistema em que se insere o projecto, estes métodos de autenticação não são desejáveis, uma vez que não é pretendido que os utilizadores acedam a SAP directamente.

3.3.3.1 Modelo de Identidade Partilhada

Há uma entidade externa que age como fornecedor de identificadores e credenciais exclusivo para todos os fornecedores de serviço. Pode ser usada, por exemplo, uma Autoridade de Certificados reconhecida por todos os fornecedores de serviços e que baseie os identificadores em endereços de e-mail (que já por si são globalmente únicos).

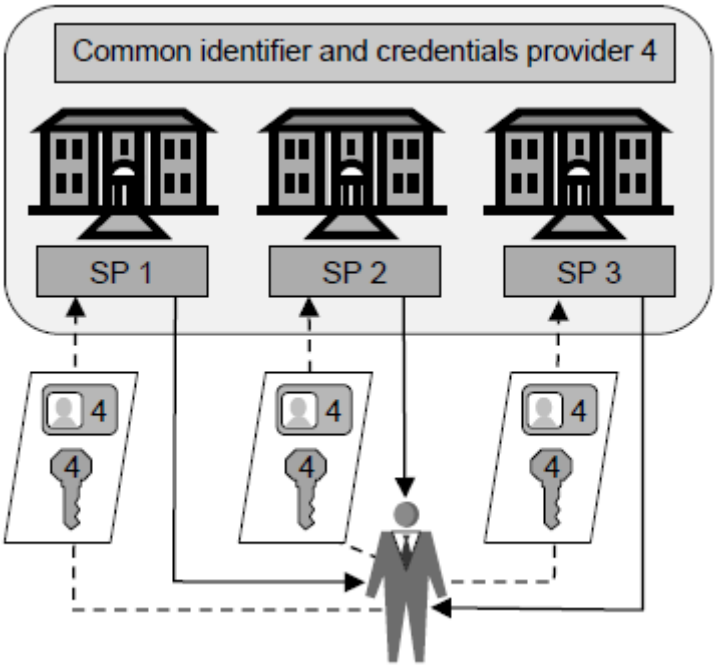


Figura 3-4 Modelo de Identidade Partilhada

3.3.3.2 Modelo de Meta-Identidade

Os fornecedores de serviço podem partilhar certos dados de identidade dos utilizadores num nível comum ou Meta. Isto pode ser implementado mapeando todos os identificadores específicos de cada fornecedor de serviço com um meta-identificador ao qual se pode ligar, por exemplo, a credencial de acesso:

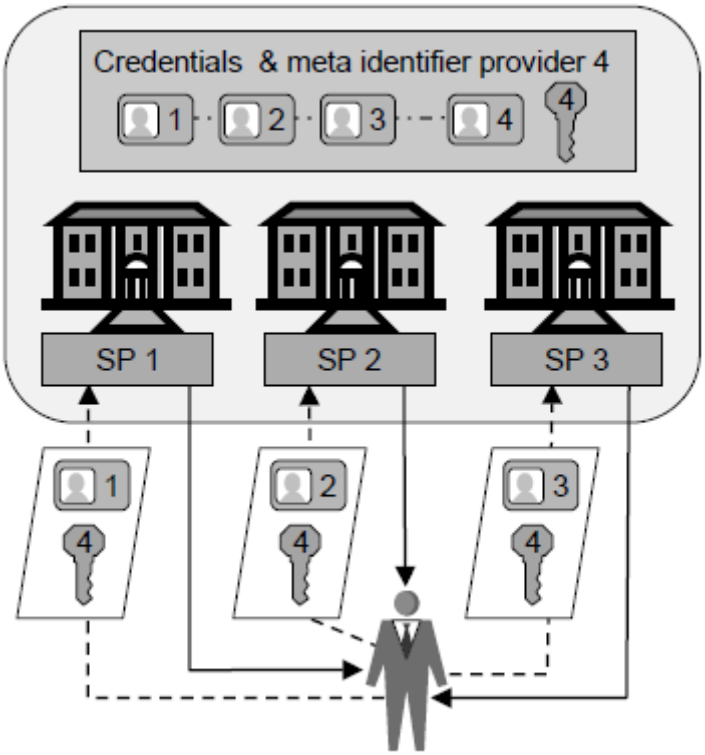


Figura 3-5 Modelo de Meta-Identidade

Este meta-identificador único está geralmente escondido dos utilizadores e é usado apenas internamente para gestão de identidades e coordenação de serviços. Quando um utilizador altera a sua palavra-chave num dado fornecedor de serviço, esta é alterada em todos os restantes.

3.3.3.3 Domínio de Identidades com Single Sign-On

Uma extensão simples dos dois modelos anteriores é a de permitir que um utilizador autenticado num prestador de serviço seja considerado como autenticado por outros prestadores de serviço. Neste caso o utilizador apenas tem de se autenticar uma vez para ter acesso a todos os serviços.

Existe geralmente uma entidade responsável por alocar identificadores e credenciais, bem como fazer a autenticação:

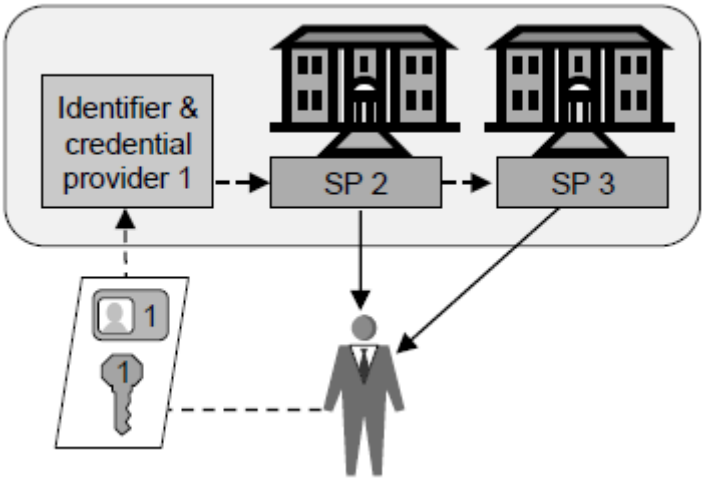


Figura 3-6 Domínio de Identidades com Single Sign-On

Este cenário é semelhante ao modelo de identidade federado com a diferença de que não é necessário mapear identificadores de utilizador, uma vez que é usado um único identificador por todos os fornecedores de serviços.

Apesar de não ser usado apenas um conjunto único de credenciais para todos os serviços, o modelo adoptado no sistema em que o projecto se insere segue uma lógica semelhante à de Single Sign-On, uma vez que o utilizador só se vai autenticar uma vez e sempre no portal para ter acesso a todos os serviços.

4. Metodologia

4.1 Metodologia de Investigação

O conceito de método envolve um conjunto de procedimentos e regras que são seguidos para atingir um resultado pretendido. Podendo adoptar várias perspectivas, os métodos variam consoante os objectivos e a finalidade da pesquisa a que se aplicam.

Para este projecto e de acordo com as definições apresentadas em *Research Methods for Business Students* (Saunders, *et al*, 2009) considerou-se o uso de um Método de Pesquisa Hipotético Dedutivo uma vez que envolve *o desenvolvimento de uma teoria e hipóteses e planeia uma estratégia de pesquisa que testa essas mesmas hipóteses*, ou seja, se a aplicação de gestão de identidades apoiada numa RFC (*Remote Function Call*) SAP consegue dar resposta à necessidade de delegação de gestão de identidades identificada como problema.

Para Edna Lúcia da Silva e Estera Muszkat Menezes (Silva & Menezes, 2001, p. 19) *Pesquisa é um conjunto de acções, propostas para encontrar a solução para um problema, que têm por base procedimentos racionais e sistemáticos. A pesquisa é realizada quando se tem um problema e não se tem informações para solucioná-lo*. Perante esta definição, esta implementação da RFC SAP para uso via aplicação de gestão de identidades e via portal Web, e o âmbito em que esta ferramenta é usada no portal Web pela Administração Pública Portuguesa considera-se, como uma Pesquisa Aplicada, ou seja, *objectiva e que gera conhecimentos para aplicação prática dirigidos à solução de problemas específicos, envolvendo verdades e interesses locais* (Silva & Menezes, 2001, p. 20).

Para a realização desta investigação aplicando o método da Pesquisa Aplicada e de acordo com Hermano Carmo e Manuela Ferreira (Carmo & Ferreira, 1998, p. 213), pode considerar-se esta pesquisa como sendo Descritiva, pois *implica estudar, compreender e explicar a situação actual do projecto de investigação*. Além de explorar a situação actual, procura ainda identificar e caracterizar as razões que estão na base da nova versão da aplicação de gestão de identidades e da futura integração da gestão de identidades no portal. Pretende ainda descrever em que medida essas razões são suficientes para um gestor SAP delegar essa gestão nos próprios utilizadores,

servindo a pesquisa aplicada a um caso prático como um exemplo dos passos para esta delegação.

4.2 Aplicação da Metodologia

Procurou-se dar uma resposta para o problema identificado nos capítulos introdutórios deste documento através do desenvolvimento e aplicação a um caso concreto de uma RFC feita em SAP. Esta deveria permitir não só criar e desactivar utilizadores em SAP, como também alterar as suas permissões e dados gerais. Por constrangimentos temporais, não foi possível desenvolver no portal da empresa a estrutura que faria as chamadas à RFC SAP, dando aos utilizadores as capacidades para verem delegada a sua própria gestão de identidades. O projecto foi então dividido em duas grandes fases:

- Ampliação da ferramenta de gestão de identidades usada pela empresa central para fazer a gestão na *Active Directory* (AD). Esta passaria a ter as funcionalidades necessárias para agir tanto na AD, como em SAP (via RFC);
- Após testes exaustivos e utilização continuada, as potencialidades da RFC SAP estarão provadas e poderá fazer-se a sua adaptação a uma utilização via portal.

Desta forma conseguem-se cumprir os objectivos desta tese, uma vez que só se avançará para uma delegação da gestão de identidades nos utilizadores dos organismos após a ferramenta estar controlada e os riscos da sua utilização identificados e eliminados ou, pelo menos, reduzidos.

O desenvolvimento da própria RFC SAP seguiu igualmente um planeamento de duas fases:

- Criação de um conjunto de macros em MS Visual Basic for Applications (VBA) com suporte num ficheiro de MS Office Excel;
- Criação da RFC em SAP seguindo a lógica das macros VBA criadas.

Ambas as fases foram alvo de testes para validar os desenvolvimentos efectuados.

5. Projecto

5.1 Enquadramento do Projecto

Antes de detalhar o projecto em si, é necessário enquadrá-lo em termos do seu papel na gestão de identidades que tem lugar no âmbito do sistema financeiro em que se insere. Neste ponto é feita uma descrição do sistema da empresa e das várias fases da gestão de identidades e a maneira como se alteraram com o uso da nova ferramenta.

5.1.1 Sistema da Empresa

Na GeRAP (empresa em que se desenvolve o projecto) existem três ambientes distintos:

- Desenvolvimento → neste ambiente são criados os novos programas e funcionalidades do portal Web;
- Pré-Produção → ambiente de testes aos desenvolvimentos que têm lugar no ambiente de Desenvolvimento;
- Produção → ambiente usado pelos utilizadores finais do portal Web.

Estas três vertentes existem tanto para a AD como para SAP.

É importante também referir que os organismos da APP que usam o sistema podem assumir diversas modalidades de adesão, estando, até à data deste documento, divididos entre 2 modelos, o que tem impacto nas suas permissões dentro do sistema (citações seguintes da Dra. Maria Henriqueta Almeida, coordenadora de área na GeRAP, 2011):

- Organismos em regime de Serviços Partilhados → *a GeRAP assume parte dos processos contabilísticos do organismo, ficando as responsabilidades divididas entre a GeRAP e o organismo para a realização destes processos*;
- Organismos em regime de Plataforma Partilhada → *o organismo assume a realização e a responsabilidade de todos os seus processos contabilísticos, usando o portal Web para a sua realização*.

5.1.2 A Gestão de Identidades Anterior ao Projecto

Como já foi mencionado em capítulos anteriores, a gestão de identidades do sistema financeiro é feita a dois níveis: na AD e em SAP. Até ao surgir deste projecto, esta

gestão era quase distinta entre sistemas, existindo uma ferramenta para fazer a gestão na AD, e um programa em linguagem de programação ABAP para fazer a gestão em SAP.

A aplicação de gestão na AD é um cliente Windows Forms desenvolvido em C# na versão 3.5 da Microsoft .NET Framework e que comunica com outros sistemas através de WebServices em WCF (Windows Communication Foundation) na mesma versão 3.5 da .NET Framework (Eng. João Neves Sousa, colaborador da GeRAP, 2011).

Para se perceber o papel desta aplicação, é relevante explicar a arquitectura que compreende a AD e SAP como bases do portal Web da empresa:

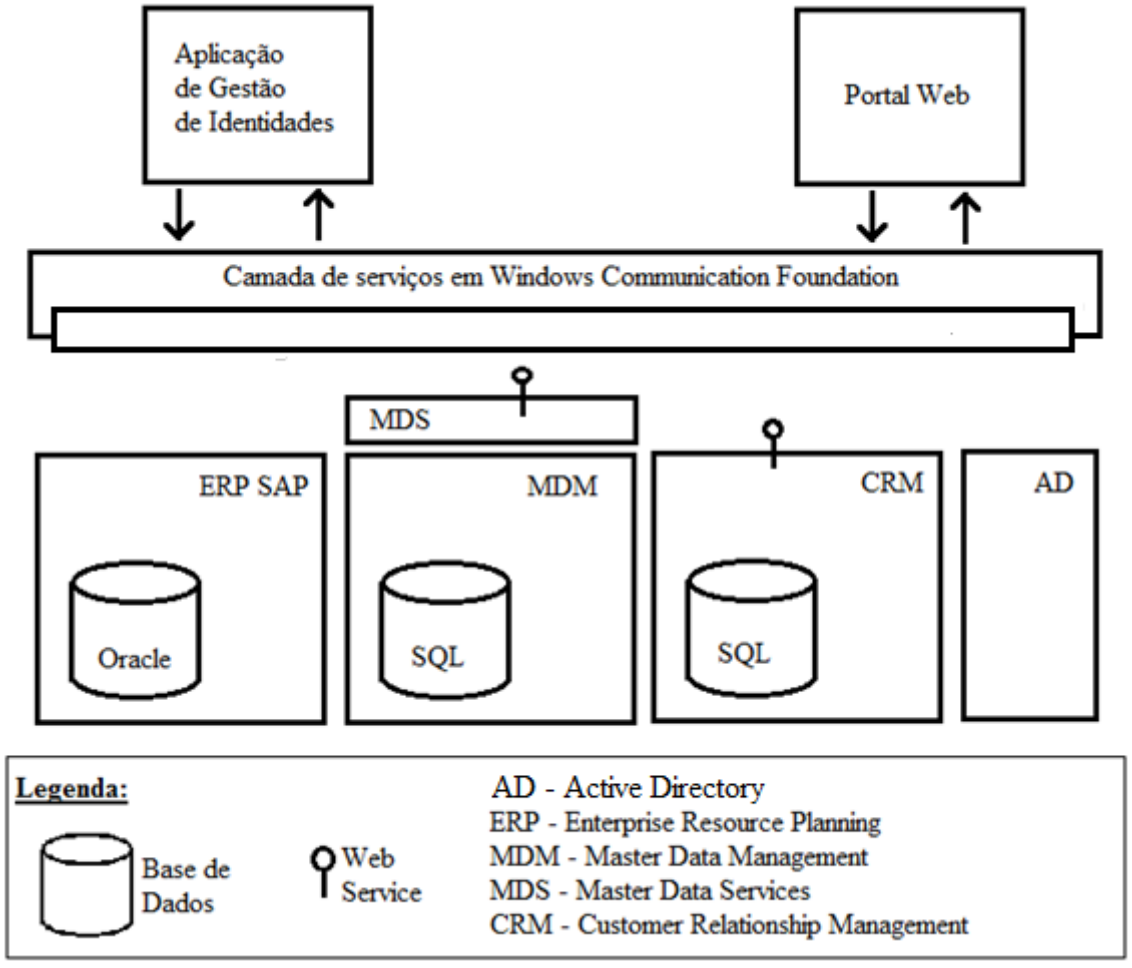


Figura 5-1 Arquitectura do Sistema Financeiro

Além do sistema SAP e da AD, já referidos, e onde é directamente feita a gestão de identidades, o portal Web da empresa tem ainda por trás dois sistemas que estão igualmente envolvidos com a informação de utilizadores que é armazenada: um sistema de dados mestre (MDM) e um sistema de gestão de relação com o cliente (CRM).

Sobre estes sistemas assentam respectivamente quatro camadas de serviços, tendo ainda sido criada pela empresa, uma camada de serviços em WCF que abrange todas as camadas de serviços dos quatro sistemas e as integra numa única. Uma vez que a gestão de identidades é assíncrona, e que os quatro sistemas podem ter os seus serviços invocados por outras aplicações, além das envolvidas na gestão de identidades, esta camada geral é necessária para permitir *rollbacks* correctos em caso de erro e para que as tarefas de gestão de identidades nos vários sistemas não sejam intercaladas com as tarefas de outras aplicações.

Recordando parte da Figura 2-1 (página 23), o fluxo de gestão de identidades na versão anterior da aplicação era o seguinte:

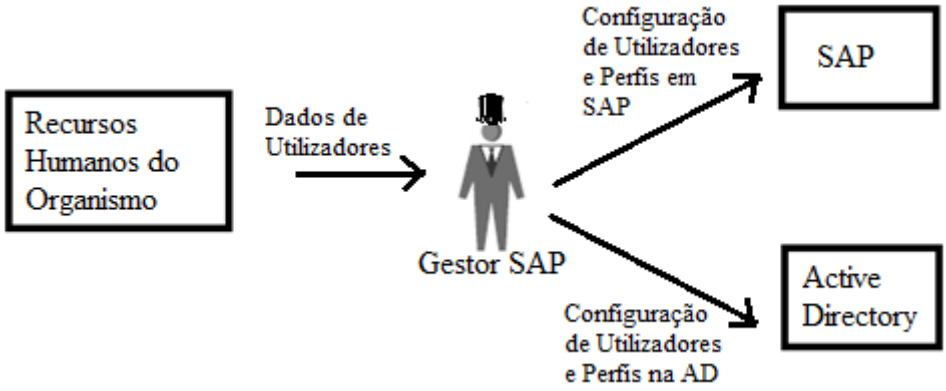


Figura 5-2 Fluxo da Gestão de Identidades Anterior ao Projecto

Esta necessidade de efectuar acções em dois locais distintos com dois programas distintos concluiu-se ser demasiado morosa perante o crescimento de utilizadores que se tem verificado, pelo que se decidiu alterar o fluxo existente (novo fluxo no capítulo 5.3 Automatismos em MS Office Excel, Figura 5-4).

Uma das necessidades identificadas foi a de integrar a gestão de identidades em SAP tanto na ferramenta usada na AD como mais tarde em processos de portal. Estas funcionalidades não seriam possíveis usando o programa ABAP que já era utilizado na gestão em SAP, uma vez que este não permitia invocações externas nem estava orientado para tal. Surgiu, assim, a necessidade de criar uma RFC em SAP que pudesse ser invocada por programas externos ao SAP e que disponibilizasse funcionalidades orientadas a uma utilização via portal Web.

5.1.3 Modelo de Gestão de Identidades Usado no Sistema do Projecto

Tendo em conta os modelos descritos por Audun Jøsang e Simon Pope (Jøsang & Pope, 2005) e referidos no capítulo de Revisão da Literatura deste documento, o sistema da empresa usa um Modelo que mistura as perspectivas Federada e de *Single Sign-On*:

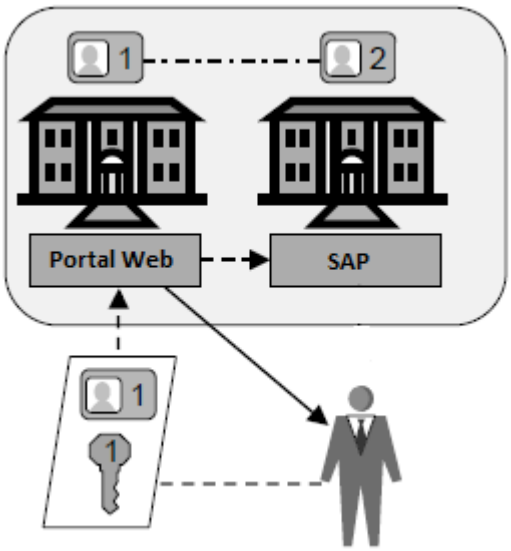


Figura 5-3 Modelo Usado no Sistema da Empresa

Cada utilizador tem conhecimento das credenciais para se autenticar perante o portal Web. Esta autenticação, após ser reconhecida, é mapeada com as respectivas credenciais SAP desse utilizador, que ficam automaticamente validadas de modo transparente para o utilizador.

Feita a autenticação no portal, podem ser invocados serviços do próprio portal ou, através de *iViews*, directamente em SAP.

Este modelo é o ideal para o que se pretende neste sistema financeiro, uma vez que:

1. Os utilizadores só se autenticam perante o portal e, nessa autenticação única, ficam autenticados em todos os sistemas necessários. Esta facilidade de autenticação, comum aos modelos de *Single Sign-On* e Federado, elimina a necessidade de decorar várias credenciais de acesso, existente quando se trabalha com vários sistemas;
2. Os utilizadores ficam com dois identificadores mas efectivamente só conhecem um deles. Isto permite-lhes ter uma identidade no sistema SAP sem conseguirem

aceder através dela, o que garante que só executam as actividades disponibilizadas no portal;

5.2 Ante-Projecto

Importa referir que este projecto teve o apoio directo de um elemento da direcção da GeRAP que, por já ter tratado da gestão de identidades no arranque da empresa, numa fase em que todo o processo era extremamente manual e moroso, tem uma noção do esforço envolvido neste âmbito e tem todo o interesse na automatização e melhoria do processo.

Antes de iniciar o projecto em si, fez-se uma análise do fluxo de gestão de identidades para detectar pontos de melhoria.

A equipa encarregue desta análise (e na qual o autor desta tese estava incluído) determinou que um ponto de partida fundamental seria a reestruturação do modo como os organismos enviam a informação dos utilizadores e respectivas permissões.

Coube ainda a esta equipa a definição das funcionalidades pretendidas para a nova versão da aplicação de gestão de identidades.

5.2.1 Revisão do Ficheiro Recebido dos Organismos

O primeiro passo no fluxo de gestão de identidades na GeRAP é o preenchimento e envio de um ficheiro MS Office Excel por parte de cada organismo. Este ficheiro contém dados gerais de todos os utilizadores e a informação, para cada um deles, das permissões necessárias no sistema de empresa.

Antes da sua revisão, este ficheiro apresentava cerca de 700 linhas com actividades possíveis de seleccionar, tendo cada actividade associada uma função SAP e um conjunto de grupos da AD. Para cada utilizador do organismo seria então necessário assinalar nessas 700 linhas quais as actividades a que deveria ser dado acesso, o que representava semanas de um trabalho moroso por parte do organismo, e muito sujeito a erros.

Por outro lado, embora todas as 700 actividades existam de facto no portal Web, muitas delas encontram-se agrupadas em módulos, não se conseguindo fornecer acesso apenas

a uma delas sem ter de dar, obrigatoriamente, acesso às restantes. Isto conferia ao ficheiro anterior, orientado às actividades, alguma redundância e ineficiência.

A equipa de trabalho tratou então de reformular este ficheiro orientando-o totalmente aos módulos existentes no portal Web. Com esta nova orientação conseguiram-se dois grandes ganhos:

- Relação com o portal que está visível aos utilizadores → é mais simples para os utilizadores identificarem as suas necessidades se as puderem relacionar com o portal com o qual trabalham. Exemplo: Na versão anterior do ficheiro os utilizadores solicitavam acesso às actividades A1, A2, A3… Agora solicitam acesso ao módulo M1 que inclui as actividades A1, A2 e A3. Garante-se assim que não estão a ser pedidos acessos desnecessários.
- Redução do tempo de preenchimento → Passou-se de cerca de 700 linhas (no ficheiro organizado por actividades) para 70 colunas (no ficheiro organizado por módulos). Esta redução para 1/10 do tamanho exigiu alguma reflexão de modo a não criar agrupamentos incorrectos e vai carecer de algumas validações em ambiente produtivo para ser afinada.

5.2.2 Levantamento de Funcionalidades para o Projecto

Tendo em conta a futura disponibilização no portal Web das funcionalidades de gestão de identidades e a ampliação das funcionalidades do programa usado para gestão de identidades na AD pela empresa, a RFC SAP terá de ter um conjunto de funcionalidades que satisfaça ambas as utilizações.

A equipa do projecto determinou então as seguintes necessidades, referentes apenas à RFC SAP:

- Possibilidade de criar novos utilizadores em SAP com um nome e palavra-chave;
    - Esta criação deve poder também ser feita por cópia de um utilizador já existente.
- Possibilidade de bloquear e desbloquear utilizadores em SAP;
- Possibilidade de modificar dados gerais de um utilizador em SAP;

- Possibilidade de atribuir ou retirar funções aos utilizadores em SAP. Esta funcionalidade deve ter em conta as diferenças entre os organismos em regime de Plataforma Partilhada e em Serviços Partilhados.

5.3 Automatismos em MS Office Excel

Apesar de conter toda a informação necessária para a criação de utilizadores e definição de permissões, o ficheiro MS Office Excel que é enviado pelos organismos não tem os dados no formato necessário para carregar na aplicação de gestão de identidades.

Isto ocorre porque o processo de recolha dos dados juntos dos organismos deve ser o mais simples possível. Não se pretende que os responsáveis de cada organismo tenham de receber horas de formação e apoio para conseguirem perceber e preencher este ficheiro, mas sim que consigam percebê-lo de forma quase intuitiva, sabendo o que fazer para enviarem à GeRAP a informação que permita dar aos seus utilizadores todas as permissões, para poderem executar o seu trabalho. A complexidade tem de estar no tratamento da informação introduzida e não na introdução dos dados.

Por essa razão, foi criado um conjunto de automatismos através de macros em MS Visual Basic for Applications com duas grandes funções:

- Permitir transformar de forma simples e rápida a informação enviada pelos organismos num formato em que esta possa ser processada pela aplicação de gestão de identidades;
- Permitir transformar a informação dos novos utilizadores para um formato padrão que é mantido pela GeRAP, de modo a que, a qualquer momento, possa ser consultada a informação completa de qualquer utilizador.

Estas duas funções precisam que sejam produzidos, a partir do ficheiro MS Office Excel enviado pelo organismo, os seguintes outputs por cada utilizador:

- Uma linha de informação a carregar na AD via aplicação, em formato .CSV (*Comma-Separated Values*);
- Uma linha de informação a carregar em SAP via aplicação (que invoca a RFC SAP), em formato .CSV;
- Uma linha de informação com o nome de utilizador no portal Web, nome de utilizador em SAP e palavras-chave de acesso. Esta linha é guardada num

ficheiro protegido e mantido na Intranet da GeRAP, para permitir restituir os acessos e corrigir problemas de SSO (*Single Sign-On*).

O ficheiro MS Office Excel recebido dos organismos contém duas folhas. Na primeira estão identificados os utilizadores desse organismo que trabalharão no portal Web da empresa. Por cada um são recebidos dados como nome, e-mail, telefone, centro de custo com o qual trabalham e superior hierárquico no organismo. Na segunda folha aparecem, também em linha, os utilizadores inseridos na primeira folha, e cerca de 70 colunas correspondentes às actividades de "Exibir" e "Modificar" de cada módulo do portal Web. A cada uma destas colunas está associado um conjunto de grupos da AD (conjunto que pode ter de 1 a N elementos) e um ID de funções SAP.

Esta estratégia de usar IDs para fazer o mapeamento com as funções SAP existe uma vez que, para cada coluna, as permissões necessárias podem mudar com alguma frequência. Assim consegue-se sempre que a coluna A esteja fixamente associada ao ID X, alterando-se (caso necessário) as funções que estão mapeadas com o ID X.

A informação destas duas folhas é depois introduzida no ficheiro MS Office Excel que contém as macros VBA. Estas macros estão divididas pelos outputs que têm de produzir, ocorrendo o seguinte fluxo:

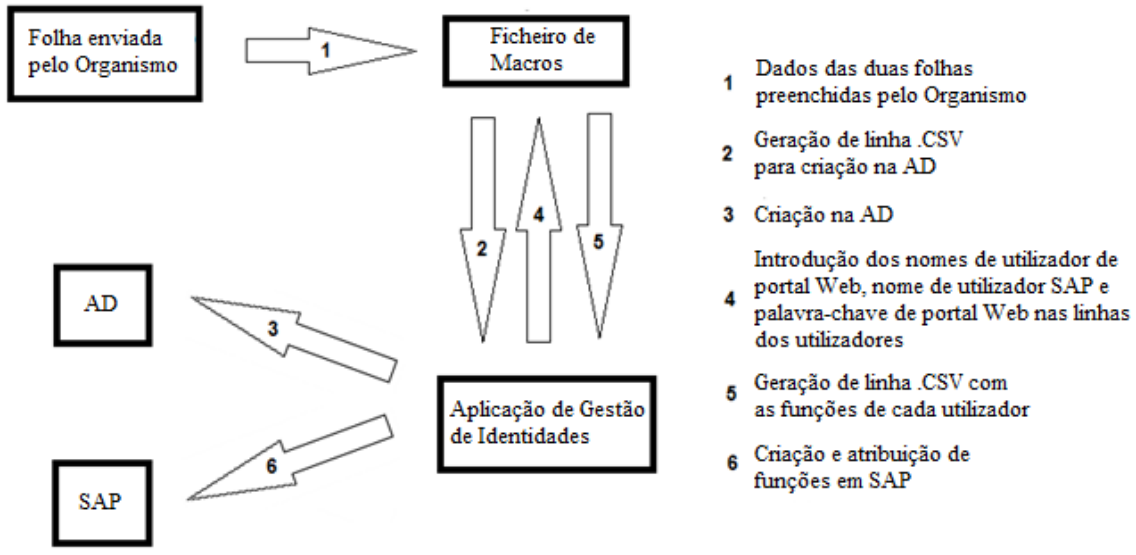


Figura 5-4 Fluxo sequencial do tratamento do ficheiro dos Organismos

Este fluxo contém as 6 acções sequenciais que se desenrolam para que os utilizadores fiquem completamente criados na AD e em SAP. Pode ver-se que as acções 2 e 5 têm

origem no ficheiro de macros, correspondendo a cada uma um conjunto distinto de rotinas.

O que é feito no passo 6 é a invocação da RFC SAP, criada como parte deste projecto, a partir do output produzido pelo ficheiro de macros.

5.4 RFC SAP

A RFC SAP para este projecto foi feita à semelhança de outras RFC SAP existentes na empresa para serem invocadas pelo portal Web, seguindo um padrão de duplicação de tabelas.

Significa isto que, por cada tabela recebida, é recebida uma tabela exactamente com os mesmos campos mas cada um deles de comprimento 1 (à excepção dos campos chave que vêm exactamente iguais), funcionando como uma tabela de *flags* (exemplo na Figura 5-5) que indica, dos campos recebidos pela RFC SAP, quais os que devem ser considerados para criação/alteração.

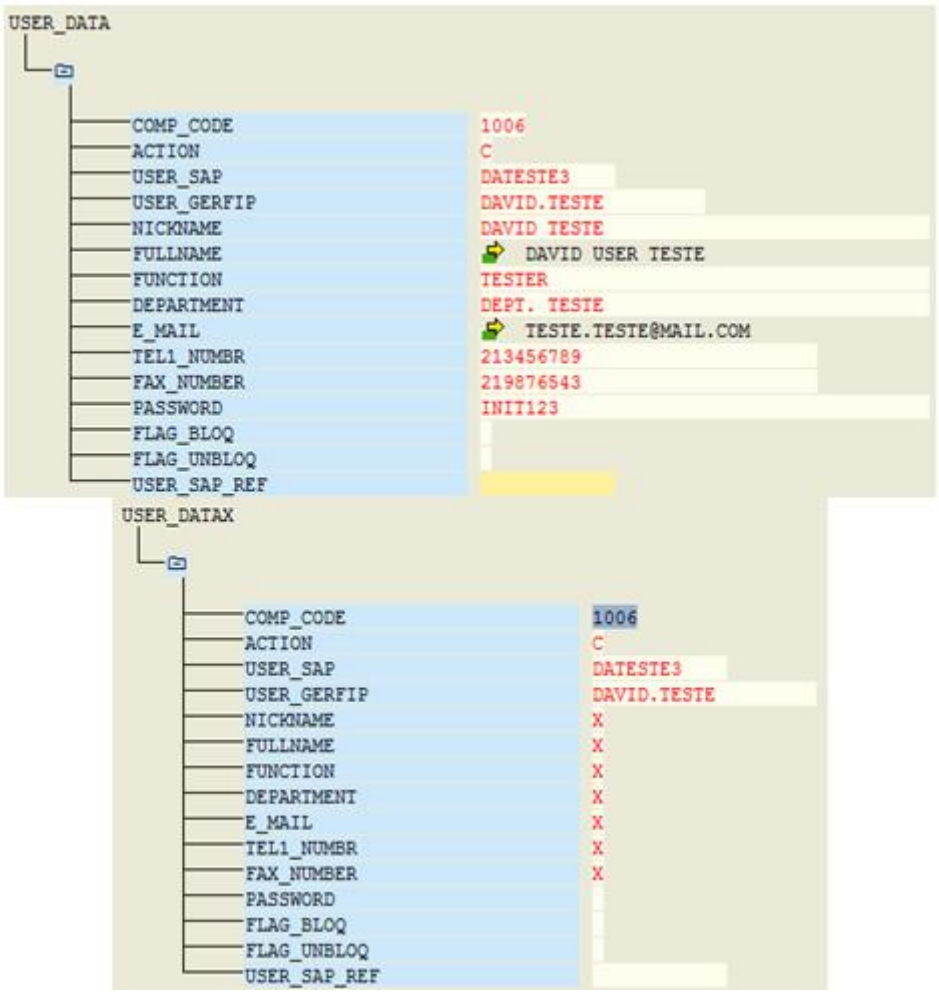


Figura 5-5 Exemplo de linha da tabela USER_DATA e linha respectiva de USER_DATAX

Esta é, aliás, a lógica seguida pelas BAPIs (Business Application Programming Inteface) que foram usadas neste projecto.

Cada objecto SAP tem vários atributos que podem ser alterados. Esta estratégia de *flags* permite indicar claramente quais os que deverão ser alterados, evitando processamento desnecessário de atributos que não serão modificados na alteração de um objecto.

No caso concreto do conjunto de funções de um utilizador, o próprio "atributo" é uma tabela. No trabalho com outras RFC SAP da empresa, concluiu-se como boa prática usar um campo distinto de *flag* para assinalar que deverão fazer-se alterações a atributos que são na verdade tabelas. Tendo isto em conta, os parâmetros da RFC SAP são:

- USER_DATA → tabela com os dados dos utilizadores;
- USER_DATAX → tabela com as *flags* referentes aos dados de utilizadores;
- ROLE_DATA → tabela com as funções de cada utilizador;

- FLAG_ROLE → campo *flag* para determinar a análise (ou não) da tabela ROLE_DATA;
- FLAG_PP → campo *flag* que indica se o organismo a que os utilizadores pertencem está em regime de Plataforma Partilhada;
- RETURN e RETURN_MESSAGES → tabelas de output com as mensagens de erro e sucesso produzidas pela RFC SAP.

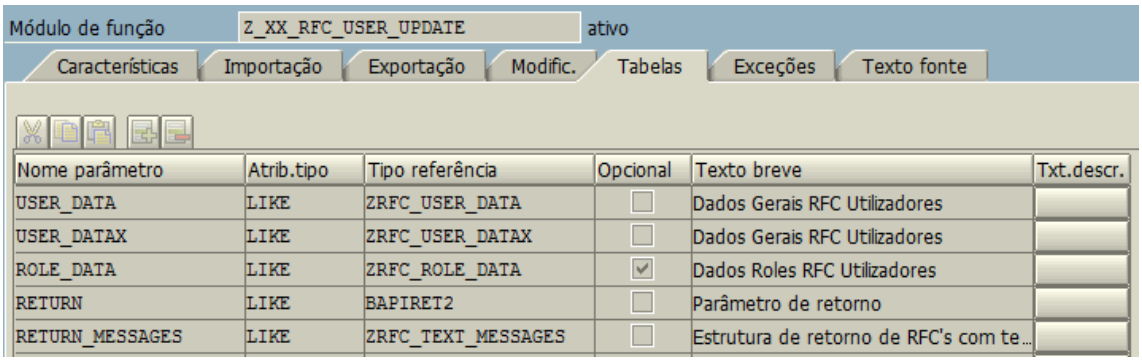


Figura 5-6 Tabelas usadas na RFC SAP

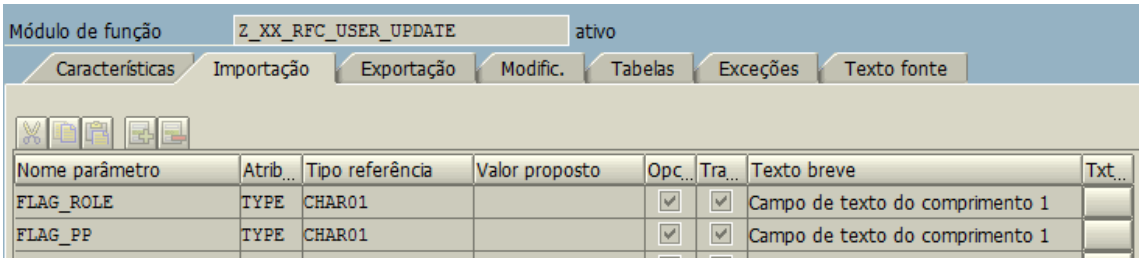
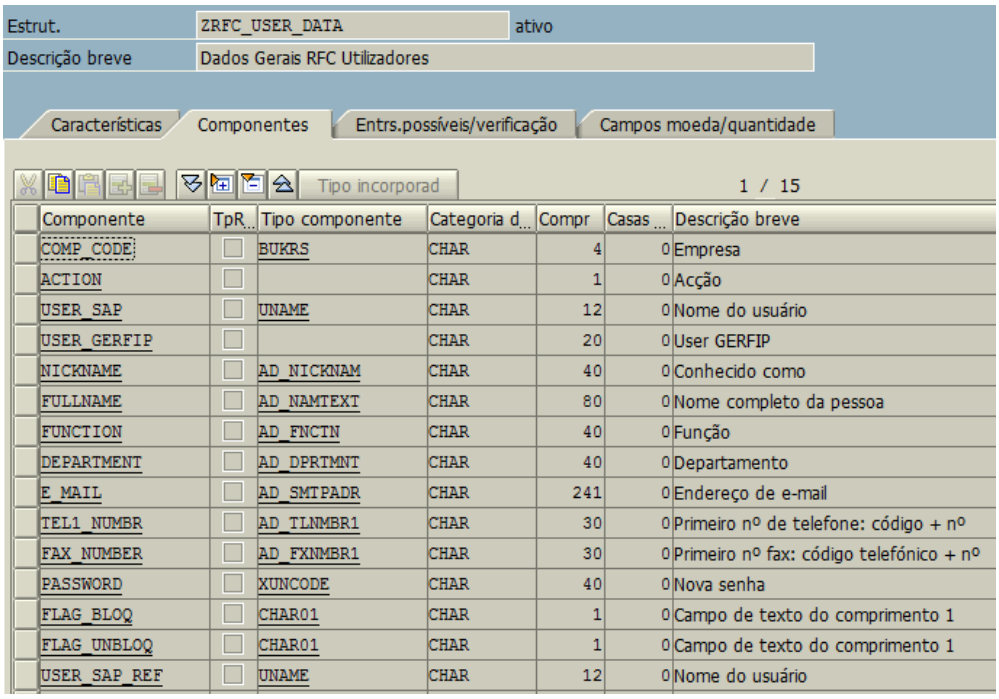


Figura 5-7 Campos de Entrada na RFC SAP

Cada uma destas tabelas tem os seguintes campos:

- USER_DATA → criada com o tipo de estrutura ZRFC_USER_DATA:



Estrut. ZRFC_USER_DATA ativo

Descrição breve Dados Gerais RFC Utilizadores

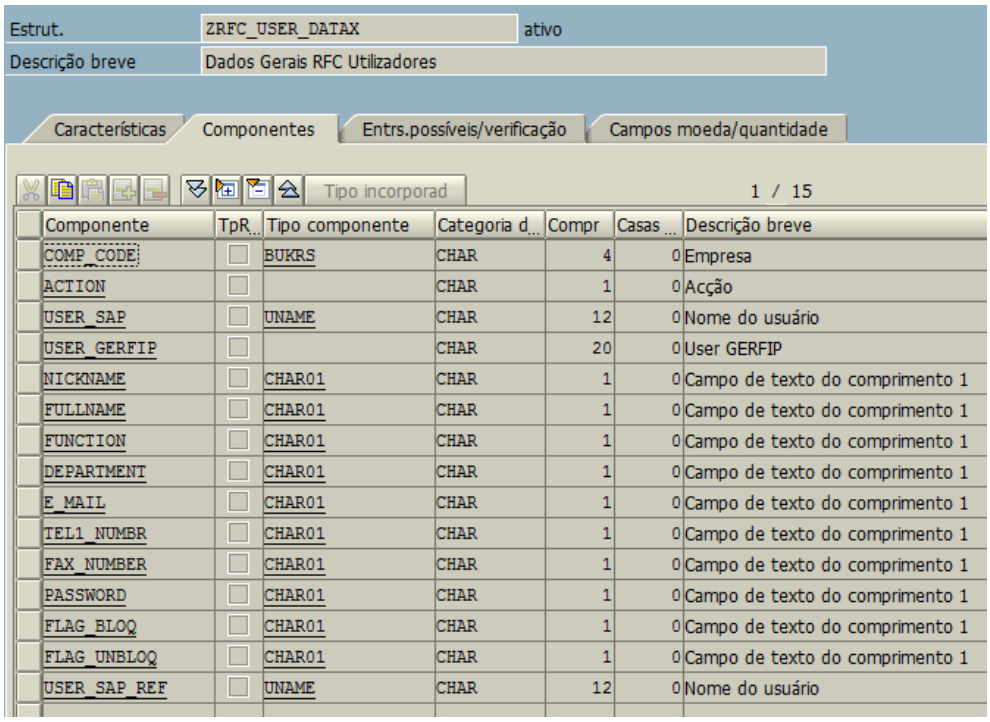
Características | Componentes | Entrs.possíveis/verificação | Campos moeda/quantidade

Tipo incorporad 1 / 15

Componente	TpR...	Tipo componente	Categoria d...	Compr	Casas ...	Descrição breve
COMP_CODE		BUKRS	CHAR	4	0	Empresa
ACTION			CHAR	1	0	Acção
USER_SAP		UNAME	CHAR	12	0	Nome do usuário
USER_GERFIP			CHAR	20	0	User GERFIP
NICKNAME		AD_NICKNAM	CHAR	40	0	Conhecido como
FULLNAME		AD_NAMTEXT	CHAR	80	0	Nome completo da pessoa
FUNCTION		AD_FNCTN	CHAR	40	0	Função
DEPARTMENT		AD_DPRTMNT	CHAR	40	0	Departamento
E_MAIL		AD_SMTPADR	CHAR	241	0	Endereço de e-mail
TEL1_NUMBR		AD_TLNMBR1	CHAR	30	0	Primeiro nº de telefone: código + nº
FAX_NUMBER		AD_FXNMBR1	CHAR	30	0	Primeiro nº fax: código telefónico + nº
PASSWORD		XUNCODE	CHAR	40	0	Nova senha
FLAG_BLOQ		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
FLAG_UNBLOQ		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
USER_SAP_REF		UNAME	CHAR	12	0	Nome do usuário

Figura 5-8 Campos da Tabela USER_DATA

- USER_DATAX → criada com o tipo de estrutura ZRF_USER_DATAX:



Estrut. ZRFC_USER_DATAX ativo

Descrição breve Dados Gerais RFC Utilizadores

Características | Componentes | Entrs.possíveis/verificação | Campos moeda/quantidade

Tipo incorporad 1 / 15

Componente	TpR...	Tipo componente	Categoria d...	Compr	Casas ...	Descrição breve
COMP_CODE		BUKRS	CHAR	4	0	Empresa
ACTION			CHAR	1	0	Acção
USER_SAP		UNAME	CHAR	12	0	Nome do usuário
USER_GERFIP			CHAR	20	0	User GERFIP
NICKNAME		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
FULLNAME		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
FUNCTION		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
DEPARTMENT		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
E_MAIL		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
TEL1_NUMBR		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
FAX_NUMBER		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
PASSWORD		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
FLAG_BLOQ		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
FLAG_UNBLOQ		CHAR01	CHAR	1	0	Campo de texto do comprimento 1
USER_SAP_REF		UNAME	CHAR	12	0	Nome do usuário

Figura 5-9 Campos da Tabela USER_DATAX

- ROLE_DATA → criada com o tipo de estrutura ZRFC_ROLE_DATA:

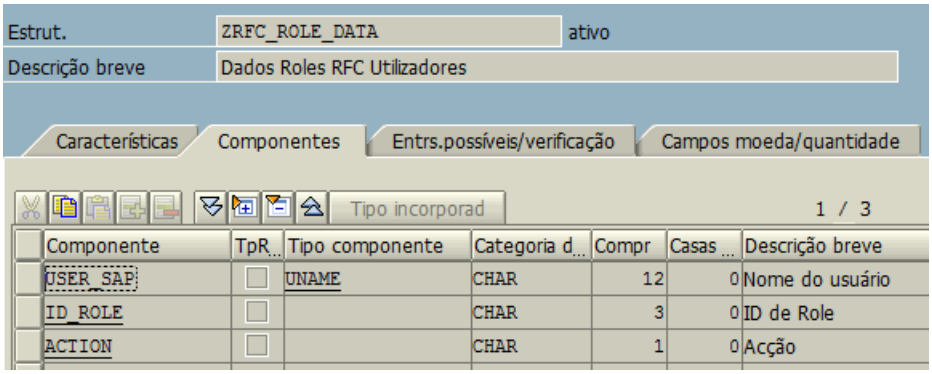


Figura 5-10 Campos da Tabela ROLE_DATA

O procedimento da RFC SAP consiste num ciclo que percorre a tabela de utilizadores USER_DATA. Em cada iteração deste ciclo é, por sua vez, percorrida a tabela USER_DATAX até encontrar a linha em que os campos COMP_CODE, ACTION, USER_SAP e USER_GERFIP das duas tabelas coincidam (Figura 5-11).

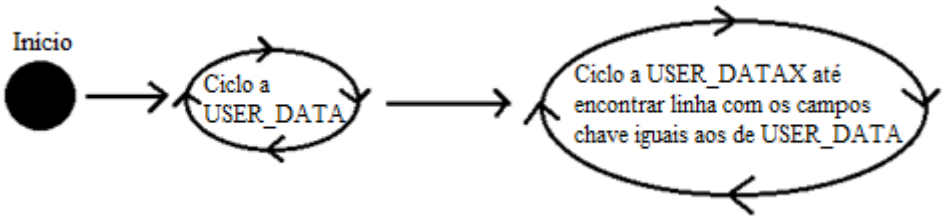


Figura 5-11 Início da RFC SAP

Isto garante-nos que estamos a validar a linha do utilizador com a correspondente linha de *flags*.

A alteração/criação do utilizador ocorre em dois passos:

1. Alteração dos dados gerais e bloqueio/desbloqueio;
2. Alteração da atribuição de funções.

Dentro de cada iteração do ciclo à tabela USER_DATA é chamada a BAPI de alteração de dados gerais (BAPI_USER_CHANGE) ou a BAPI de criação (BAPI_USER_CREATE). Se estivermos na criação de um utilizador e a operação tiver corrido com sucesso, chama-se a função SUSR_USER_CHANGE_PASSWORD_RFC para que a palavra-chave deixe de ter o status "inicial" e passe a ter o status "produtiva". Isto é necessário pois um novo utilizador SAP ao fazer o seu primeiro acesso ao sistema activa uma janela para alterar a sua palavra-chave de acesso, o que regra geral é uma

boa política de segurança. No caso do portal Web da empresa, no entanto, os utilizadores acedem a SAP através do mecanismo de SSO (*Single Sign-On*) e nunca directamente em SAP, pelo que não se pretende que eles alterem a sua palavra-chave de acesso mas sim que nunca tenham conhecimento dela.

Se a acção for de "M" (Modificação), após a alteração dos dados gerais valida-se se os campos da linha do utilizador FLAG_BLOQ ou FLAG_UNBLOQ vêm preenchidos com X. Após esta validação pode ser chamada uma das funções:

- BAPI_USER_LOCK → bloqueio de utilizador (se FLAG_BLOQ = "X");
- BAPI_USER_UNLOCK → desbloqueio de utilizador (se FLAG_UNBLOQ = "X").

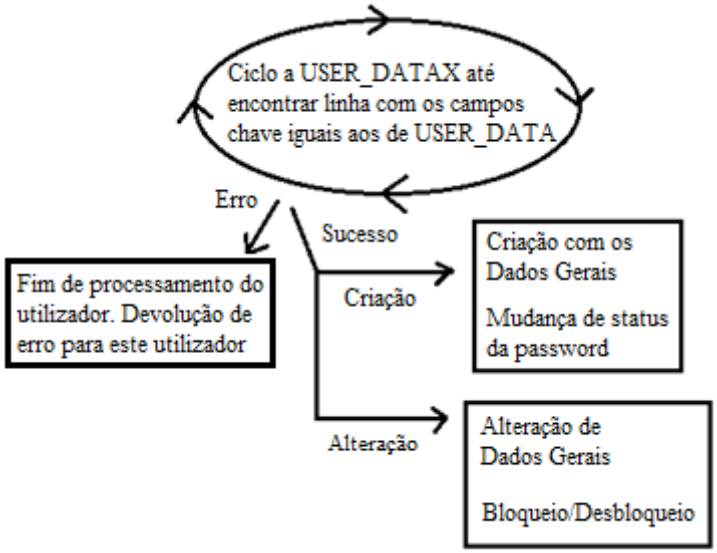


Figura 5-12 Acções em cada ciclo à tabela de utilizadores

Após a alteração de dados e o possível bloqueio/desbloqueio (Figura 5-12), é feito um ciclo à tabela ROLE_DATA (caso o campo FLAG_ROLE venha preenchido com X) e são guardadas numa tabela auxiliar todas as linhas cujo nome de utilizador SAP seja igual ao do utilizador da iteração actual da tabela USER_DATA (Figura 5-13). Esta tabela auxiliar é então passada para o método de atribuição de funções.

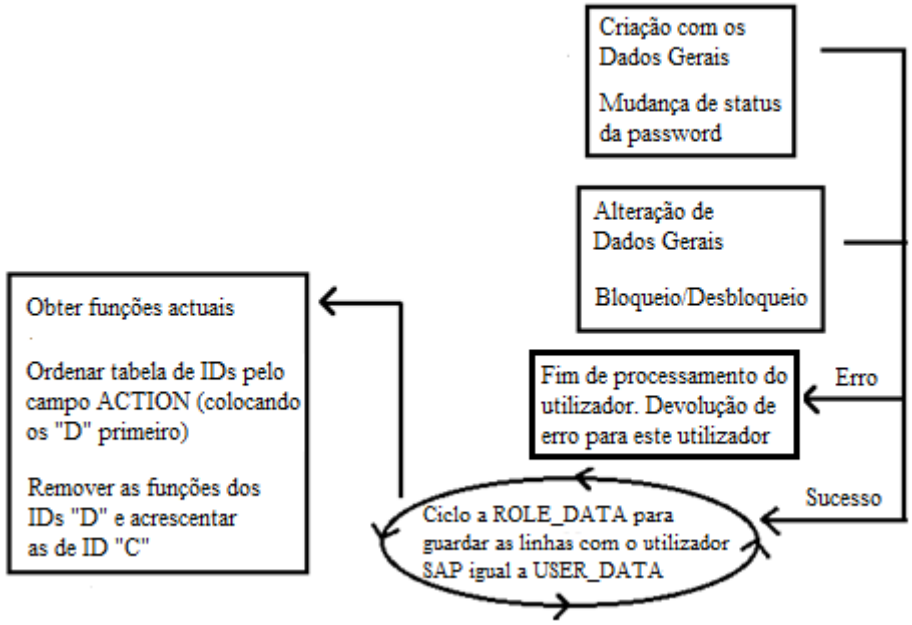


Figura 5-13 Configuração de Funções em SAP

Foi necessário criar um método para alterar as funções de cada utilizador pois a BAPI BAPI_USER_ACTGROUPS_ASSIGN usada para o efeito substitui as funções actuais do utilizador pelas novas a atribuir, o que não era o pretendido.

O método criado começa por usar a BAPI BAPI_USER_GET_DETAIL para obter as funções actuais do utilizador, guardando-as numa tabela auxiliar. Depois é feito um ciclo à tabela ROLE_DATA e são feitas duas operações:

1. Para todos os IDs com a acção "D", são identificadas as funções correspondentes a esse ID (com uma consulta à tabela ZXX_ID_ROLE criada para guardar a correspondência entre IDs e funções) e, caso existam para a COMP_CODE do utilizador nas suas funções actuais, são retiradas da tabela auxiliar;
2. Para todos os IDs com a acção "C", são identificadas as funções correspondentes a esse ID (com uma consulta à tabela ZXX_ID_ROLE) e são adicionadas à tabela auxiliar de funções, caso não existissem lá para a COMP_CODE do utilizador.

Em ambas estas operações é tido em consideração o tipo de Organismo a que o utilizador pertence (Plataforma Partilhada ou Serviço Partilhado). Tal como explicado no início deste capítulo, os organismos em Plataforma Partilhada têm um leque de permissões mais alargado, pelo que as funções existentes do tipo "_G_" não podem ser

atribuídas a organismos em Serviços Partilhados. Esta validação deve ser feita tanto na atribuição de funções como na sua remoção, através do valor do campo FLAG_PP (se tiver "X" trata-se de um organismo em plataforma partilhada).

É importante tratar primeiro os IDs com a acção "D" uma vez que há funções que existem em vários IDs em simultâneo. A título de exemplo:

- ID 1: Funções A, B, C;
- ID 2: Funções C, D, E;
- Utilizador com as funções C, D, E, F ao qual se vai acrescentar o ID 1 e retirar o ID 2.

Se acrescentarmos o ID 1 antes de retirar o ID 2 o que acontece é o seguinte:

Funções Iniciais	**Acrescentar ID 1**	**Retirar ID 2**
C, D, E, F	A, B, C, D, E, F	A, B, F

Quando o pretendido seria o utilizador ficar com as funções A, B, C, F, o que se consegue com:

Funções Iniciais	**Retirar ID 2**	**Acrescentar ID 1**
C, D, E, F	F	A, B, C, F

Para conseguir esta sequência o que é feito é ordenar a tabela de IDs a tratar, pelo campo ACTION em ordem decrescente, garantido que todos os IDs com acção "D" são analisados primeiro pelo ciclo.

Feitos os ajustes à tabela auxiliar de funções, esta é então dada como entrada juntamente com o nome de utilizador à BAPI BAPI_USER_ACTGROUPS_ASSIGN que elimina as funções anteriores do utilizador e as substitui pelas dadas.

Dispondo graficamente os passos referidos, o fluxo da RFC SAP é o seguinte:

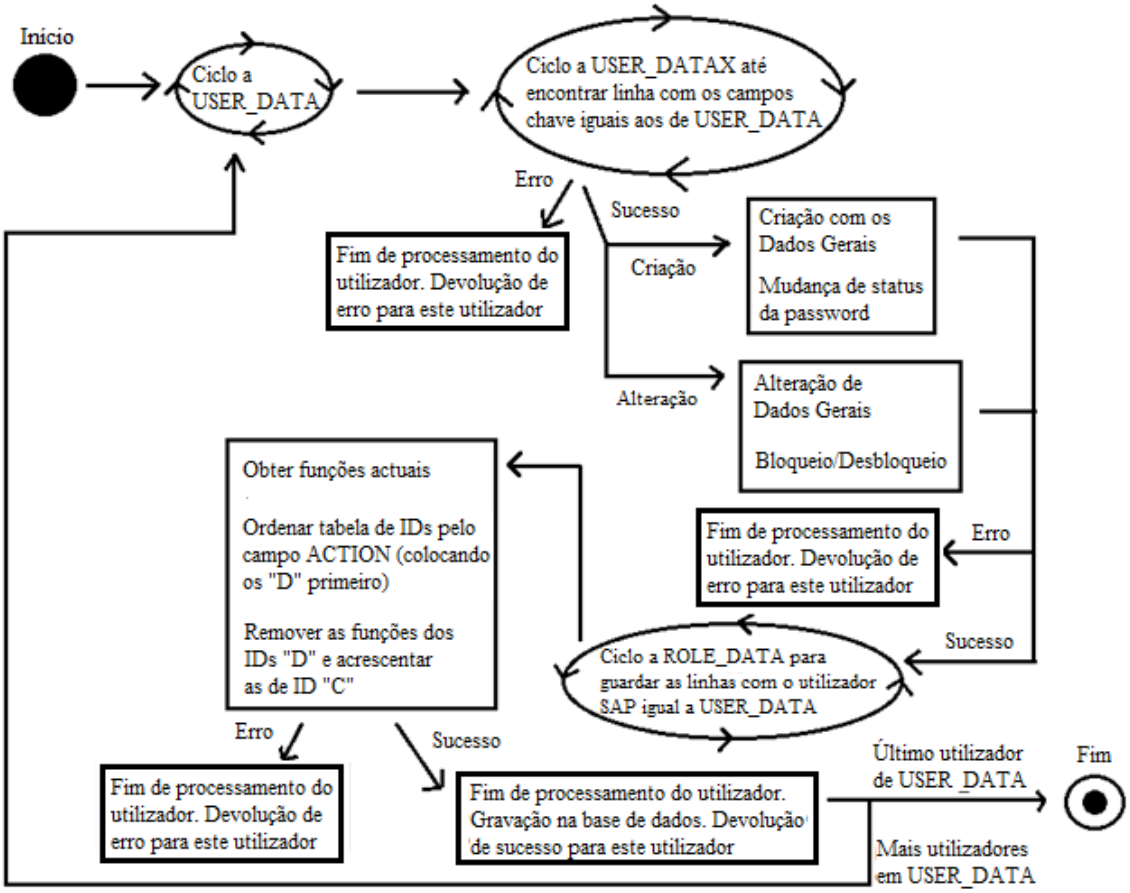


Figura 5-14 Fluxo da RFC SAP

5.4.1 Validação da RFC SAP e Testes

Foram feitos testes à RFC SAP após o seu desenvolvimento para identificar possíveis falhas e pontos de melhoria, bem como para validar a adequação da ferramenta à sua utilização.

Estes testes incluem-se, no processo de testes de software, como Testes de Componentes, uma vez que foram testes apenas à RFC SAP sem integração com outros sistemas e foram da responsabilidade do programador derivando da sua experiência (Alexandre, 2009, p. 4). Tiveram um objectivo essencialmente de Validação, ou seja, *demonstrar ao programador e cliente que o software está de acordo com os requisitos* (Alexandre, 2009, p.7), mas também, quando possível, procuraram a identificação de Defeitos, ou seja, *descobrir erros no software* (Alexandre, 2009, p.6).

O procedimento de teste começou por definir um conjunto de casos compostos por:

- Dados de Entrada;
- Resultado Esperado;
- Resultado Obtido.

Depois de definidos todos os casos de teste, foi usado o método de "Testes e *Debugging*", ou seja, executou-se a RFC SAP para cada caso, analisando os resultados do código linha a linha para permitir identificar erros ou pontos de melhoria (Alexandre, 2008, p.17):

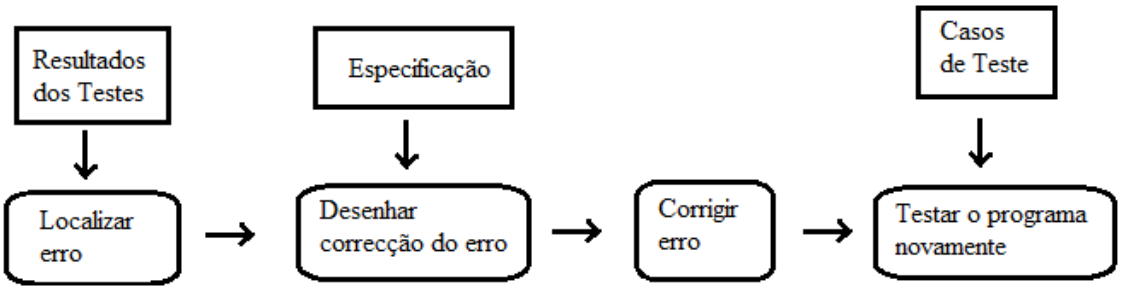


Figura 5-15 Testes e *Debugging*

(fonte: EngSoftI-Validacao&Verificacao0809 (Alexandre, 2008))

Os testes tiveram em consideração situações de 1 e 3 utilizadores, pertencentes ao mesmo organismo ou com utilizadores de organismos diferentes:

1. Criar utilizador sem funções
2. Criar um utilizador com funções de Serv. Part.
3. Criar um utilizador com funções Plat. Part.
4. Criar três utilizadores com funções de Serv. Part. diferentes
5. Criar três utilizadores com funções de Plat.Part. diferentes
6. Criar um utilizador que já exista
7. Criar três utilizadores em que dois já existam
8. Bloquear um utilizador desbloqueado
9. Bloquear um utilizador bloqueado
10. Bloquear três utilizadores desbloqueados
11. Desbloquear um utilizador bloqueado
12. Desbloquear um utilizador desbloqueado
13. Desbloquear três utilizadores

14. Bloquear um utilizador e desbloquear um utilizador
15. Modificar um utilizador
    1. Dados Gerais
    2. Acrescentar funções
    3. Retirar funções
    4. Acrescentar e retirar funções
16. Modificar três utilizadores
    1. Dados Gerais
    2. Acrescentar funções
    3. Retirar funções
    4. Acrescentar e retirar funções
17. Modificar um utilizador que não exista
    1. Dados Gerais
    2. Acrescentar e retirar funções
18. Modificar três utilizadores em que dois não existam
19. Modificar um utilizador bloqueado
20. Criar um utilizador por cópia de um outro
21. Criar dois utilizadores por cópia de dois utilizadores diferentes

Os resultados dos testes foram de sucesso em 26 de 28 casos (considerando um caso de sucesso aquele em que o resultado obtido foi igual ao esperado) como se pode ver na tabela abaixo:

Nº	**Designação**	**Sucesso**	**Erro**	**Melhoria**
1	Criar utilizador sem funções	X		
2	Criar um utilizador com funções de Serv. Part.	X		
3	Criar um utilizador com funções de Plat. Part.			A
4	Criar três utilizadores com funções de Serv. Part. diferentes	X		
5	Criar três utilizadores com funções de Plat. Part. diferentes	X		A
6	Criar um utilizador que já exista	X		
7	Criar três utilizadores em que dois já existam	X		A
8	Bloquear um utilizador desbloqueado	X		
9	Bloquear um utilizador bloqueado	X		
10	Bloquear três utilizadores desbloqueados	X		
11	Desbloquear um utilizador bloqueado	X		
12	Desbloquear um utilizador desbloqueado	X		

13	Desbloquear três utilizadores	X		B
14	Bloquear um utilizador e desbloquear um utilizador	X		B
15	Modificar um utilizador			
15.1	Dados Gerais	X		
15.2	Acrescentar funções	X		A
15.3	Retirar funções	X		A
15.4	Acrescentar e retirar funções	X		A
16	Modificar três utilizadores			
16.1	Dados Gerais	X		
16.2	Acrescentar funções	X		A
16.3	Retirar funções	X		A
16.4	Acrescentar e retirar funções	X		A
17	Modificar um utilizador que não exista			
17.1	Dados Gerais			C
17.2	Acrescentar e retirar funções	X		C
18	Modificar três utilizadores em que dois não existam	X		A,C
19	Modificar um utilizador bloqueado	X		A
20	Criar um utilizador por cópia de um outro	X		
21	Criar dois utilizadores por cópia de dois utilizadores diferentes	X		
TOTAL	28	26	0	3

Tabela 5-1 Resultados dos Casos de Teste

As melhorias indicadas decorrem não nos resultados em si, mas das mensagens produzidas pelas BAPIs Standard.

Apesar de as operações a efectuar serem concluídas com sucesso, verificou-se um excesso de mensagens, desnecessário para a boa utilização da RFC SAP pelo portal Web e pela aplicação de gestão de identidades (Melhoria B). No teste 13, para um utilizador que foi desbloqueado e cujos dados e funções foram alterados, foram recebidas três mensagens, uma para cada acção. Determinou-se que é suficiente uma mensagem por utilizador com a indicação de "alterado com sucesso" caso todas as três alterações tenham sucesso.

Por outro lado, na atribuição/remoção de funções, percebeu-se que algumas das funções criados não existem para todos os organismos, sendo devolvida uma mensagem de aviso "A Função X não existe". Para os utilizadores finais da RFC SAP este tipo de mensagens é desnecessário, pelo que, após a conclusão dos testes, a política de

mensagens da RFC SAP foi revista. Deixaram de ser usadas as mensagens Standard devolvidas pelas BAPIs e passaram a usar-se mensagens de erro ou sucesso criadas para o efeito, mais simples e em menor número de modo a devolver apenas a informação realmente necessária (Melhoria A).

Ainda nos casos em que se tentou alterar utilizadores inexistentes (Casos de Teste 17.1, 17.2 e 18), foram produzidas mensagens de "erro interno" que não teriam sentido para um utilizador final (Melhoria C). Foi adoptado o mesmo procedimento de revisão da política de mensagens que se aplicou à Melhoria A.

A RFC SAP, em conjunto com os respectivos casos de teste e após implementação das melhorias identificadas, foi considerada adequada à função que se lhe pretende pela equipa afecta a este projecto.

Para comprovar a eficiência e correcção da RFC SAP num contexto real, foi utilizado um organismo da APP como piloto de testes, o qual reformulou as permissões de todos os seus utilizadores (cerca de 190). Estas alterações afectaram utilizadores já existentes antes do projecto, e incluíram ainda a criação de utilizadores com recurso às novas macros. A criação em SAP, apesar de ter tido como dados de entrada as linhas produzidas pelas macros VBA, foi efectuada no ambiente de produção através do programa anterior ao projecto, pois a RFC SAP ainda não se encontrava (à data do processamento) neste ambiente.

Foram, no entanto, replicados estes utilizadores e correspondentes permissões no ambiente de qualidade através da nova versão da aplicação de gestão de identidades, tendo-se já seguido todo o fluxo desde a recepção do ficheiro MS Office Excel do organismo até à criação em SAP.

5.4.2 Próximos passos

Ao longo do restante ano de 2011 está em fase de finalização o processo de entrada de mais um conjunto de organismos da APP no sistema da empresa. Estes organismos servirão de meio de optimização da RFC SAP através do seu uso via aplicação de gestão de identidades e, no médio/longo prazo, via portal Web.

Em Janeiro de 2012 está previsto o arranque do projecto de delegação efectiva do processo de gestão de identidades via portal Web nos utilizadores dos Organismos.

Sendo este um passo tão importante como crítico, será essencial ter as conclusões deste documento como base, em conjugação com as necessidades de melhoria identificadas ao longo do restante ano de 2011, para garantir que as funcionalidades delegadas aos utilizadores permitem apenas o que é necessário para a sua gestão interna.

Ao longo do ano de 2012 poderá ser feita uma análise dos problemas decorrentes desta delegação, bem como dos ganhos de eficiência que esta trará tanto para a GeRAP como para os organismos utilizadores do sistema.

Como contribuição para o tema da gestão de identidades ficará a evolução e documentação de problemas e respectivas soluções decorrentes do uso da RFC SAP integrada nesta gestão de identidades via aplicação (gestão central) e via portal Web (gestão delegada).

Um dos objectivos do projecto que se irá iniciar é o de possibilitar a criação de permissões à medida, afastando-se da modalidade actual segundo a qual há um conjunto de funções SAP e grupos no portal criados *a priori* para atribuição. Perante este novo paradigma, a RFC SAP terá de ser adaptada, pelo que, para facilitar este processo, todo o código foi detalhadamente comentado.

6. Conclusões

Tendo por base os casos de testes utilizados e a análise dos resultados obtidos em comparação com os esperados, pode considerar-se o uso de uma RFC SAP no âmbito da gestão de identidades como uma abordagem de sucesso. O resultado deste projecto afecta, no curto prazo, tanto os 65 organismos da APP que já se encontram no sistema como os cerca de 100 que irão aderir em Janeiro de 2012. No médio/longo prazo e acompanhando e evoluindo com o próprio sistema, prevê-se que o projecto de gestão de identidades venha a servir toda a APP, que se pretende completamente integrada no sistema em 2012 segundo directivas do Memorando de Entendimento internacional com o qual Portugal se comprometeu (Memorando de Entendimento, 2011, p. 15).

Partindo dos Objectivos e do Problema levantados no capítulo introdutório deste documento e após trocas de impressões com os restantes elementos da equipa afecta ao projecto, podem retirar-se as seguintes conclusões:

Objectivo Principal

- Factores que levam um gestor de identidades a colocar do lado dos utilizadores a sua própria gestão de identidades:
    - Ganhos de eficiência perante um volume crescente de utilizadores do sistema;
    - Maior sensibilidade de um gestor de identidades local para os problemas diários do organismo do que a de um gestor de identidades central.

Objectivos Específicos

- Identificar riscos em dar este tipo de poder aos utilizadores:
    - Informação errada introduzida no sistema;
    - Remoção errada de permissões necessárias;
    - Acrescento errado de permissões desnecessárias;
    - Possibilidade de falha na validação de permissões.
- Sugerir soluções minimizadoras dos riscos encontrados:
    - Restrição da informação que pode ser introduzida através de menus, limitando ao máximo os campos de inserção livre;

- A remoção/acrescento errado de permissões - estando nomeado um gestor de identidades local no organismo, não só é mais rapidamente identificado e comunicado mas é também mais agilmente corrigido com uma gestão delegada;
- O facto de o processo ser feito via portal Web obriga ao uso de um utilizador autenticado. Como tal, as suas permissões são validadas antes de ser possível fazer qualquer consulta ou alteração, restringindo-se a possibilidade de alterações não autorizadas.

Problema

- Como pode um gestor de identidades de um sistema financeiro na Administração Pública Portuguesa delegar essa gestão nos utilizadores do sistema, controlando o risco associado a essa delegação?

A estratégia adoptada pela equipa de começar com uma fase de afinação das ferramentas em que estas são usadas pelo gestor central antes de serem disponibilizadas aos utilizadores finais apresenta-se como muito benéfica.

Por outro lado o facto de se usar um portal Web com autenticação de utilizadores e no qual a permissão para gerir identidades só pode ser dada pelo gestor central consegue limitar eventuais falhas de segurança.

Recuperando os processos relevantes de acordo com a Hitachi para a Gestão de Permissões mencionados no glossário (Hitachi, 2011):

1) *Criar e actualizar regularmente uma base consolidada de permissões;*
2) *Definir funções de modo a que as permissões possam ser atribuídas aos utilizadores em moldes compreensíveis pelos próprios;*
3) *Permitir pedidos e aprovações em regime self-service, de modo a que as decisões sobre permissões possam ser feitas pelos utilizadores funcionais com conhecimento do contexto e não por utilizadores mais técnicos;*
4) *Sincronizar permissões entre sistemas, quando apropriado;*
5) *Convidar periodicamente pessoas de uma área mais funcional (menos técnicas) para reverem as permissões e funções associadas aos utilizadores de modo a identificar situações que já não sejam apropriadas e tenham de ser revistas ou removidas.*

Por constrangimentos temporais e técnicos, apenas a actividade 3 foi disponibilizada aos utilizadores nesta versão do projecto de delegação de gestão de identidades. Numa versão posterior deste projecto, prevê-se que as actividades 1 e 2 ficarão ao alcance dos organismos da APP, estando para já a cargo da empresa que mantém o sistema. As actividades 4 e 5 serão sempre da responsabilidade da empresa central.

Verificou-se também que foi importante para o projecto o facto de ter o apoio directo da direcção da empresa, que muitas vezes se mostrou um factor facilitador perante a necessidade de fazer testes ou de coordenar trabalhos e reuniões, em equipas com elementos de diferentes áreas da empresa.

Teria sido de grande interesse avaliar a aceitação e os problemas reais dos utilizadores da gestão de identidades em ambiente de portal Web, bem como a mudança de paradigma para o gestor de identidades central.

A título pessoal o autor ficou satisfeito com o resultado dos testes, em particular com o uso da RFC SAP via aplicação no contexto da actualização de permissões no organismo piloto (ainda que em ambiente de qualidade). Apesar de não se ter alcançado ainda uma delegação efectiva de gestão de identidades nos utilizadores finais do sistema, foram criadas as bases para que isto possa ocorrer num futuro próximo. O projecto foi importante, não só na empresa para o início da integração de actividades de gestão de identidades no portal Web, mas também porque enriqueceu o tema da gestão de identidades através de um caso de aplicação prática.

7. Bibliografia

ALEXANDRE, Isabel 2009. *EngSoftI-TestesSoftware0910:* ISCTE-IUL, 2009, páginas 4, 6, 7.

ALEXANDRE, Isabel 2008. *EngSoftI-Validacao&Verificacao0809:* ISCTE-IUL, 2008, página 17.

BERNDT, Rüdiger e COWLING, James, *et al* 2005. *SAP User and Access Management with Microsoft Identity Integration Server*: Oxford Computer Group Ltd e Collaboration Technology Support Center Microsoft [*Online*] 2005 [Citação: 9 de Março de 2011]. http://download.microsoft.com/download/5/7/f/57f1490e-8a8d-497b-bbae-ec2a44b3799f/miis_sap.pdf

CARMO, Hermano e FERREIRA, Manuela 1998. *Metodologia de Investigação: Guia para auto-aprendizagem.* Universidade Aberta, 1998, página 213.

CHADWICK, David 2006. *Delegation of Authority (DyVOSE project)*: University of Kent [*Online*] 2006 [Citação: 6 de Setembro de 2011]. http://www.jisc.ac.uk/uploaded_documents/Delegation%20of%20AuthorityJISCdemo.ppt

GRANT, Ian 2007. *Identity Management: The Expert View*: ComputerWeekly.com [*Online*] 2007 [Citação 9 de Março de 2011] http://www.computerweekly.com/Articles/2007/11/23/225715/Identity-management-the-expert-view.htm

Hitachi ID Systems, Inc. *Identity Management Terminology* [*Online*] [Citação: 9 de Março de 2011]. http://hitachi-id.com/identity-manager/docs/identity-management-terminology.html

JØSANG, Audun e POPE, Simon 2005. *User Centric Identity Management*: CRC for Enterprise Distributed Systems Technology (DSTC Pty Ltd), The University of Queensland, Australia [*Online*] 2005 [Citação: 10 de Abril de 2011] http://folk.uio.no/josang/papers/JP2005-AusCERT.pdf

SILVA, Edna Lúcia da e MENEZES, Estera Muszkat 2001. *Metodologia da Pesquisa e Elaboração de Dissertação* 3ª ed. Universidade Federal de Santa Catarina, Florianópolis, 2001**.**

Memorando de Entendimento 2011. *Portugal: Memorandum of Understanding on Specific Economic Policy Conditionality* [*Online*] 2011 [Citação: 10 de Setembro de 2011] http://www.jornaldenegocios.pt/archivos/2011_05/memorando.pdf

NABETH, Thierry e **HILDEBRANDT, Mireille 2005.** *D 2.1: Inventory of topics and clusters*: FIDIS (Future of Identity in the Information Society) [*Online*] 2005 [Citação: 28 de Maio de 2011] http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.1_Inventory_of_topics_and_clusters.pdf

- **CLAUß, Sebastian e MARIT, Köhntopp 2001**; *Identity Managements and Its Support of Multilateral Security*; in: Computer Networks 37 (2001), Special Issue on Electronic Business Systems; Elsevier, North-Holland 2001; 205-219
- **HILDEBRANDT, Mireille 2005**; Privacy and Identity; in: Erik Claes and Antony Duff (ed.), *Privacy and the Criminal Law,* proceedings of the Conference on Privacy and the Criminal Law 14th-15th May 2004, to be published 2005
- **RICOEUR, Paul 1992**, *Oneself as another*, Chicago and London: University of Chicago Press 1992

NYQUIST, Jeanne 2007. *Delegation & Empowerment*. [*Online*] 2007 [Citação: 6 de Setembro de 2011] http://www2.apwa.net/documents/education/institutes/ppt/Delegation.ppt

SAP 2011. *RFC and BAPI Interfaces to SAP Systems*. [*Online*] 2011 [Citação: 10 de Setembro de 2011]

http://help.sap.com/saphelp_45b/helpdata/de/cf/8ccab761ea11d2804a00c04fada2a1/content.htm

SAUNDERS, Mark, LEWIS, Philip, e THORNILL, Adrian 2009. *Research methods for business students*. 5th ed. Pearson Education Limited, 2009.

8. Anexos

Anexo A – Parte da Tabela com as Funções e IDs

Data Browser: Tabela ZXX_ID_ROLE

MANDT	ID_ROLE	ROLE
120	1	ZCTOR_G_PS_DUODECIMO
120	1	ZCTOR_O_PS_ALTERORCM
120	1	ZCTOR_O_PS_CABIMENTO
120	1	ZCTOR_O_PS_CATIVDESC
120	1	ZCTOR_O_PS_COMPROMIS
120	14	ZCAPG_A_PS_IMPRDOCMS
120	14	ZCAPG_G_PS_PREAPRPGM
120	14	ZTESO_O_PS_EXECTESO
120	17	ZCAPG_G_PS_REGCAUCOE
120	17	ZCAPG_G_PS_REGDOCMTS
120	17	ZCAPG_G_PS_REGRECEIT
120	17	ZCTGE_G_PS_DOCUMFINC
120	17	ZCTGE_G_PS_ESTORDOCM
120	17	ZTESO_G_PS_EXECTESO
120	17	ZVEND_G_PS_DOCUMFINC
120	17	ZVEND_O_PS_OFERTAS
120	17	ZVEND_O_PS_ORDEMVEND
120	22	ZTESO_G_PS_EXECTESO
120	22	ZTESO_O_PS_EXECTESO
120	23	ZCTOR_A_PS_CONSULTAR
120	23	ZTESO_O_PS_CONSULTA
120	24	ZARM_O_PS_FORNECIME
120	24	ZARM_O_PS_MOVMERC
120	24	ZCTAN_G_PS_ANLTMESTR
120	24	ZCTGE_G_PS_DOCUMFINC
120	24	ZCTRE_G_PS_DADOMESTR
120	24	ZVEND_G_PS_DOCUMFINC
120	24	ZVEND_O_PS_CONTRATOS
120	24	ZVEND_O_PS_OFERTAS
120	24	ZVEND_O_PS_ORDEMVEND
120	24	ZVEND_O_PS_PROJECTOS
120	24	ZVEND_O_PS_PROPVENDA
120	25	ZCTRE_O_PS_CONSULTA
120	26	ZARM_O_PS_GESTARM
120	26	ZARM_O_PS_INVENT
120	26	ZARM_O_PS_PLANARM
120	26	ZCAPG_O_PS_ALTECABIM
120	26	ZCTOR_O_PS_NPDAPROVA
120	27	ZARM_O_PS_INVENT

Figura de Anexo 1 - Funções dos IDs 1, 14, 17, 22, 23, 24, 25, 26 e 27

Anexo B – Casos de Teste da RFC

Criar um Utilizador com Funções de Serviços Partilhados

Dados de Entrada

FLAG_ROLE: X

FLAG_PP:

USER_DATA:

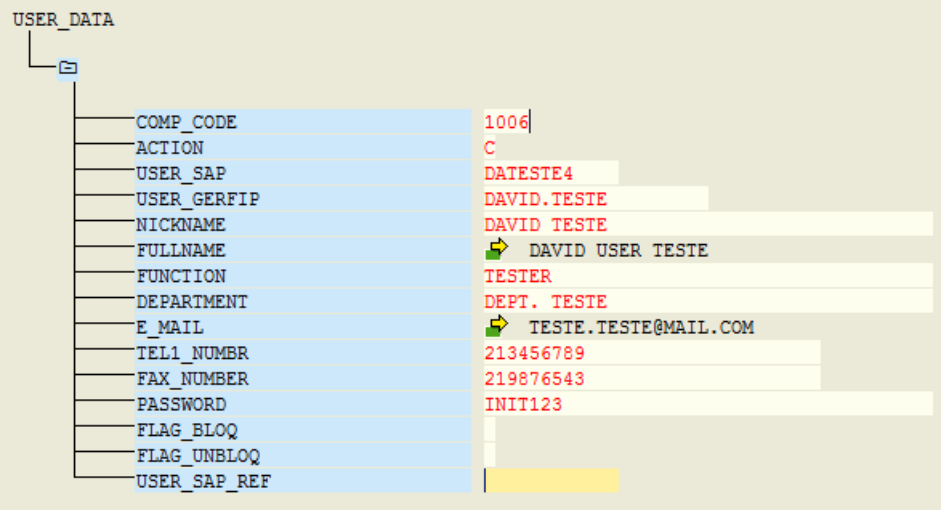


Figura de Anexo 2 - Dados de entrada de USER_DATA no teste 2

USER_DATAX:

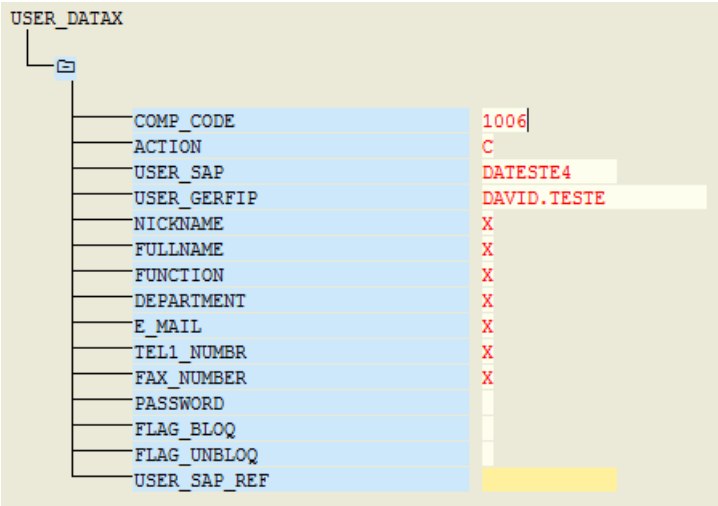


Figura de Anexo 3 - Dados de entrada de USER_DATAX no teste 2

ROLE_DATA:

USER_SAP	ID_	A
DATESTE4	1	C
DATESTE4	14	C
DATESTE4	17	C

Figura de Anexo 4 - Dados de entrada de ROLE_DATA no teste 2

Resultado Esperado

Era esperado que fosse criado o utilizador DATESTE4 e que, dos IDs 1, 14 e 17, tivesse apenas as funções sem _G_ da tabela do Anexo A.

Resultado Obtido

Editor de estrutura: Exibir RETURN a partir de entrada 1

Coluna | Entrada | Metadados

2 Entradas

T	ID	NUM	MESSAGE
S	01	102	Usuário DATESTE4 criado
S	01	048	A atribuição de funções ao usuário DATESTE4 foi modificada.

Figura de Anexo 5 - Conteúdo da tabela RETURN após o teste 2

Editor de estrutura: Exibir RETURN_MESSAGES a partir de entrada

Coluna | Entrada | Metadados

2 Entradas

MSG_INDX	M	MSG_TEXT
2	S	Usuário DATESTE4 criado
3	S	A atribuição de funções ao usuário DATESTE4 foi modificada.

Figura de Anexo 6 - Conteúdo da tabela RETURN_MESSAGES após o teste 2

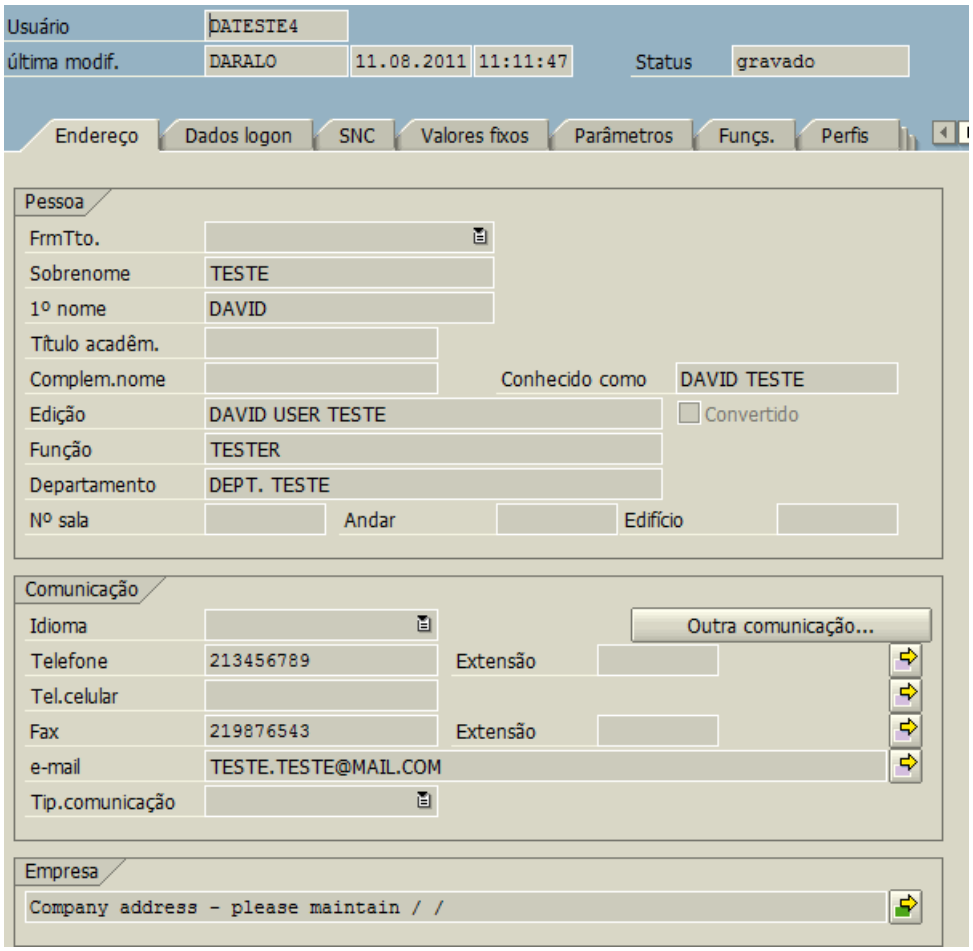


Figura de Anexo 7 - Dados do utilizador DATESTE4 após o teste 2

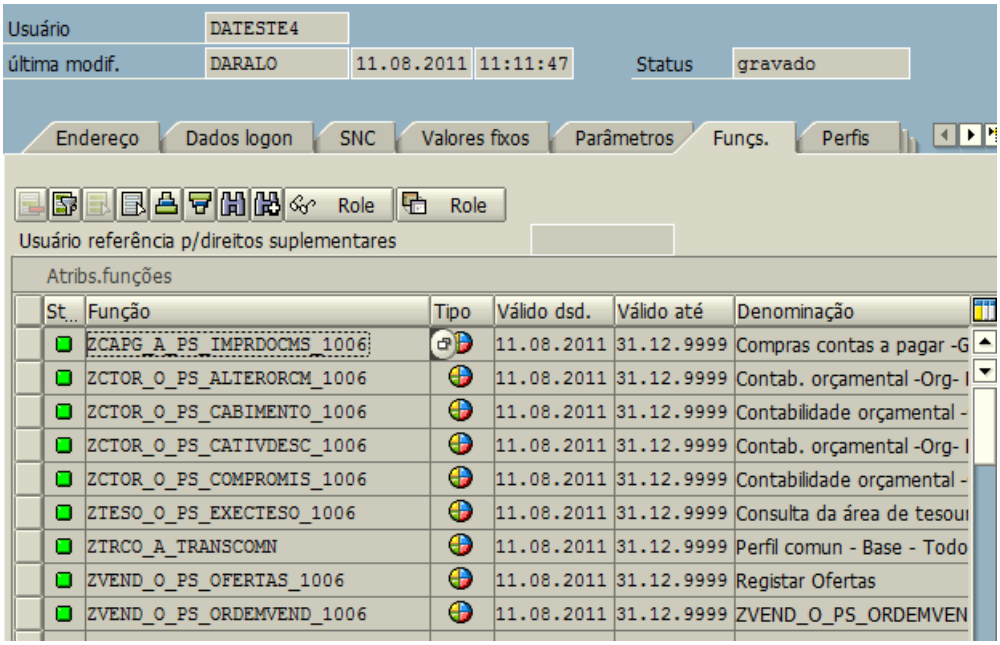


Figura de Anexo 8 - Funções do utilizador DATESTE4 após o teste 2

Criar um Utilizador com Funções de Plataforma Partilhada

Dados de Entrada

FLAG_ROLE: X

FLAG_PP: X

USER_DATA:

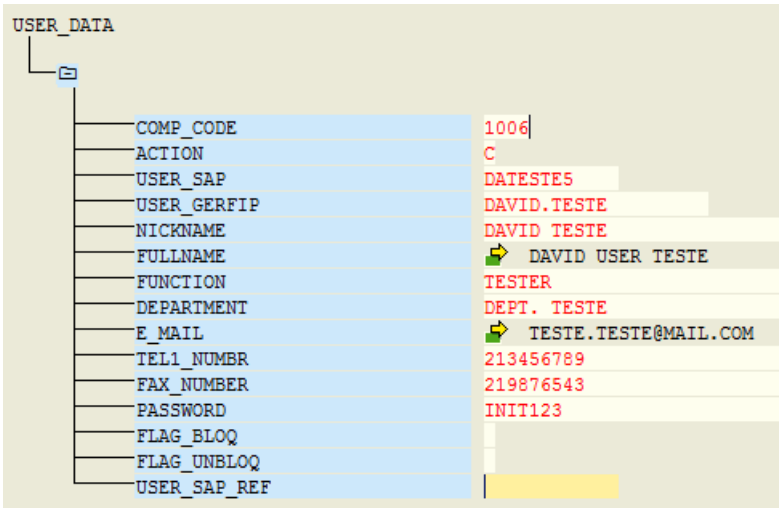


Figura de Anexo 9 - Dados de entrada de USER_DATA no teste 3

USER_DATAX:

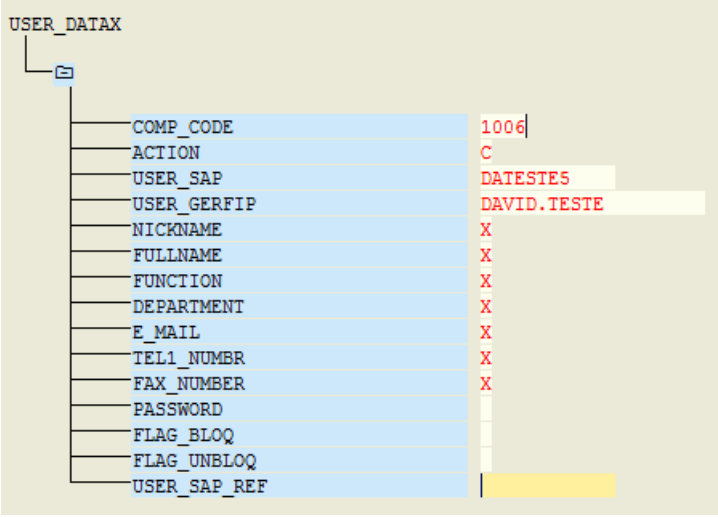


Figura de Anexo 10 - Dados de entrada de USER_DATAX no teste 3

ROLE_DATA:

USER_SAP	ID_	A
DATESTE5	1	C
DATESTE5	14	C
DATESTE5	17	C

Figura de Anexo 11 - Dados de entrada de ROLE_DATA no teste 3

Resultado Esperado

Era Esperado que fosse criado o utilizador DATESTE5 e que, dos IDs 1, 14 e 17, tivesse todas as funções da tabela do Anexo A.

Resultado Obtido

T	ID	NUM	MESSAGE
S	01	102	Usuário DATESTE5 criado
W	S#	234	Função ZCAPG_G_PS_PREAPRPGM_1006 não existe
W	S#	234	Função ZCAPG_G_PS_REGCAUCOE_1006 não existe
W	S#	234	Função ZCAPG_G_PS_REGDOCMTS_1006 não existe
W	S#	234	Função ZCAPG_G_PS_REGRECEIT_1006 não existe
S	01	048	A atribuição de funções ao usuário DATESTE5 foi modificada.

Figura de Anexo 12 - Conteúdo da tabela RETURN após o teste 3

6 Entradas

MSG_INDX	M	MSG_TEXT
1	S	Usuário DATESTE5 criado
2	W	Função ZCAPG_G_PS_PREAPRPGM_1006 não existe
3	W	Função ZCAPG_G_PS_REGCAUCOE_1006 não existe
4	W	Função ZCAPG_G_PS_REGDOCMTS_1006 não existe
5	W	Função ZCAPG_G_PS_REGRECEIT_1006 não existe
6	S	A atribuição de funções ao usuário DATESTE5 foi modificada.

Figura de Anexo 13 - Conteúdo da tabela RETURN_MESSAGES após o teste 3

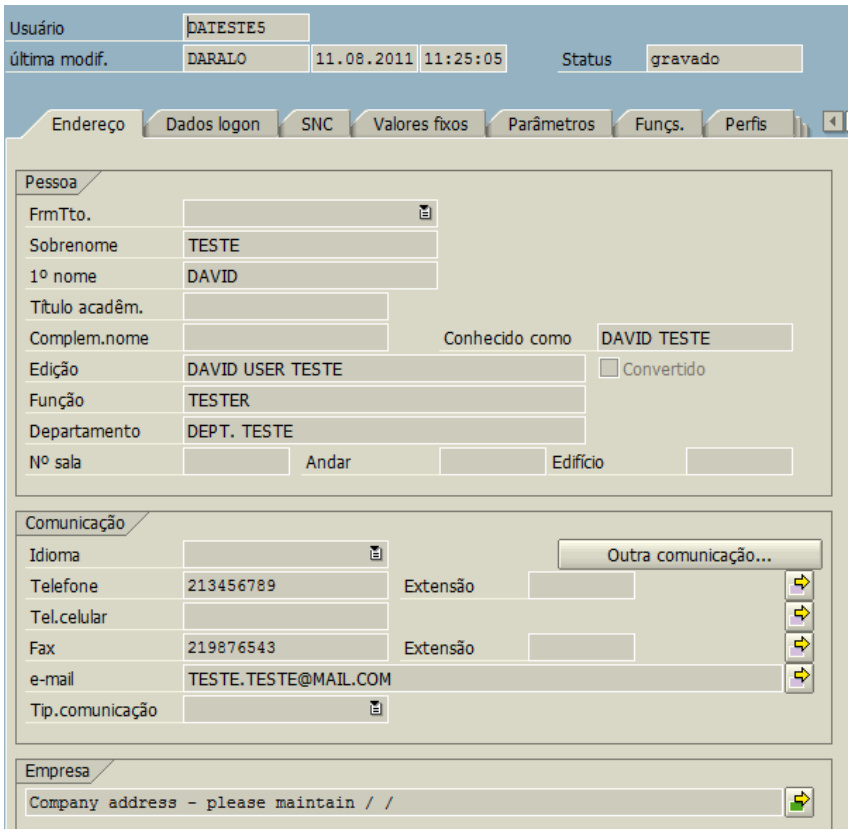


Figura de Anexo 14 - Dados do utilizador DATESTE5 após o teste 3

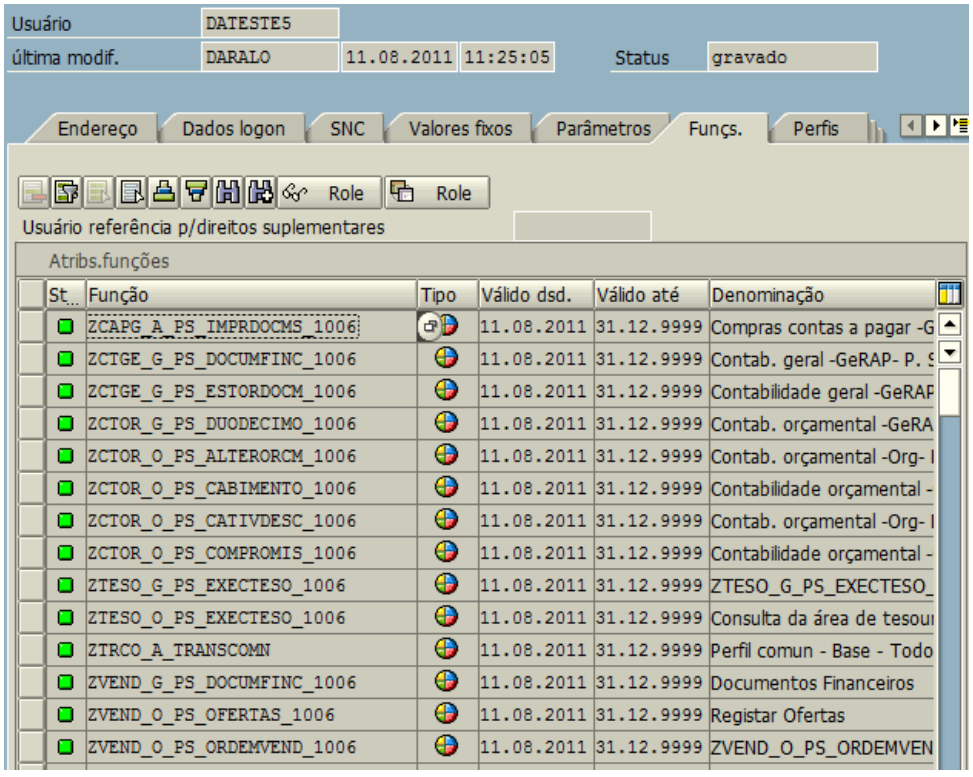


Figura de Anexo 15 - Funções do utilizador DATESTE5 após o teste 3

Bloquear um Utilizador Desbloqueado

Dados de Entrada

FLAG_ROLE:

FLAG_PP:

USER_DATA:

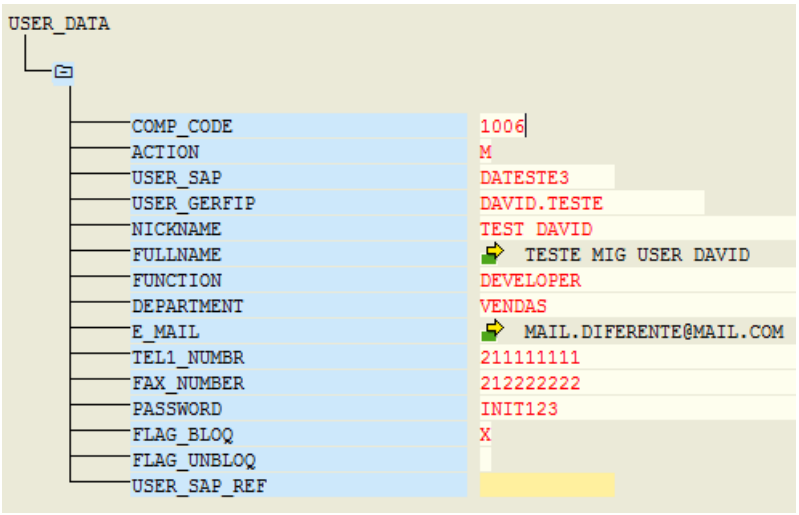


Figura de Anexo 16 - Dados de entrada de USER_DATA no teste 8

USER_DATAX:

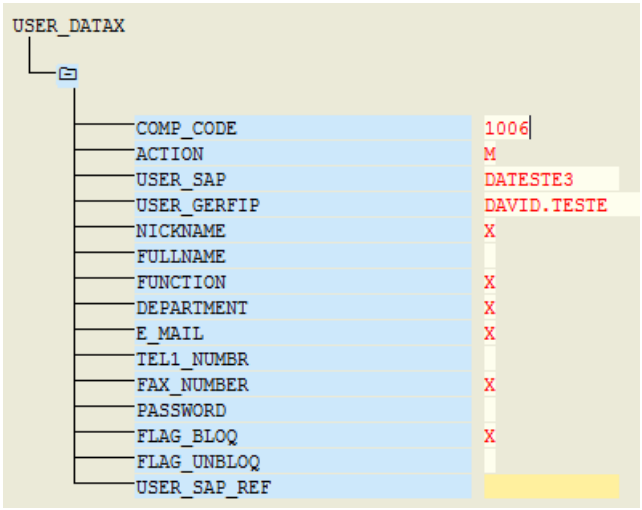


Figura de Anexo 17 - Dados de entrada de USER_DATAX no teste 8

ROLE_DATA:

Resultado Esperado

Era esperado que o utilizador DATESTE3 ficasse bloqueado.

Resultado Obtido

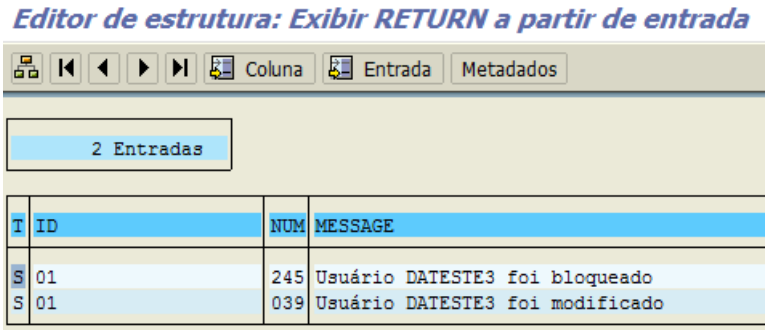


Figura de Anexo 18 - Conteúdo da tabela RETURN após o teste 8

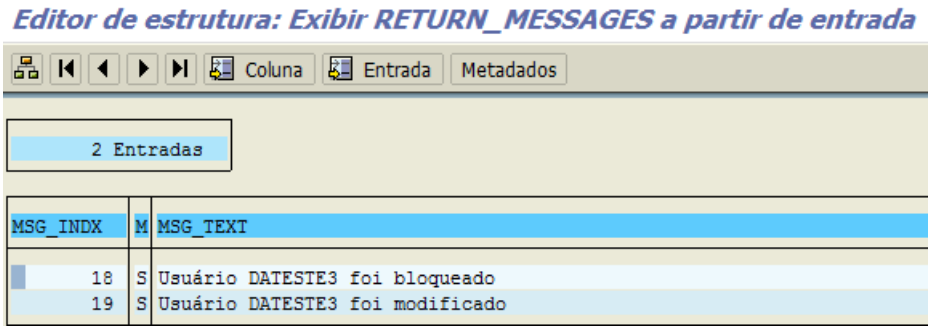


Figura de Anexo 19 - Conteúdo da tabela RETURN_MESSAGES após o teste 8

Figura de Anexo 20 - Estado de bloqueio do utilizador DATESTE3 após teste 8

Desbloquear três Utilizadores

Dados de Entrada

FLAG_ROLE: X

FLAG_PP:

USER_DATA:

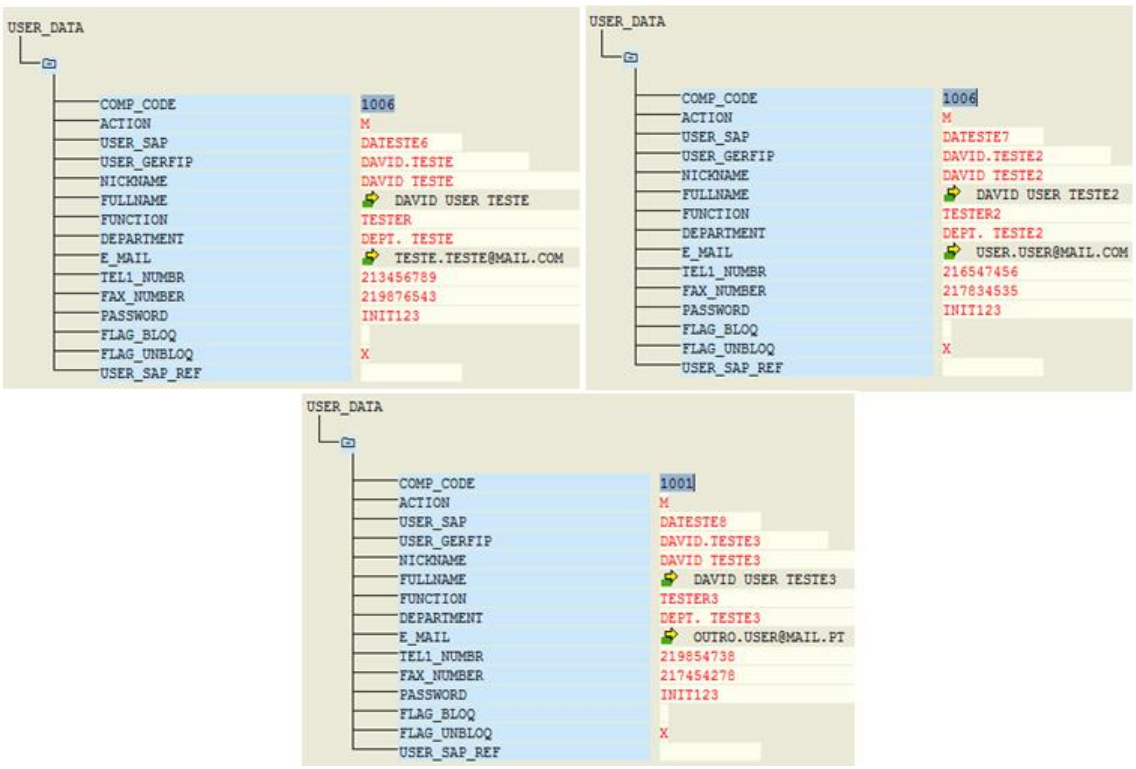


Figura de Anexo 21 - Dados de entrada de USER_DATA no teste 13

USER_DATAX:

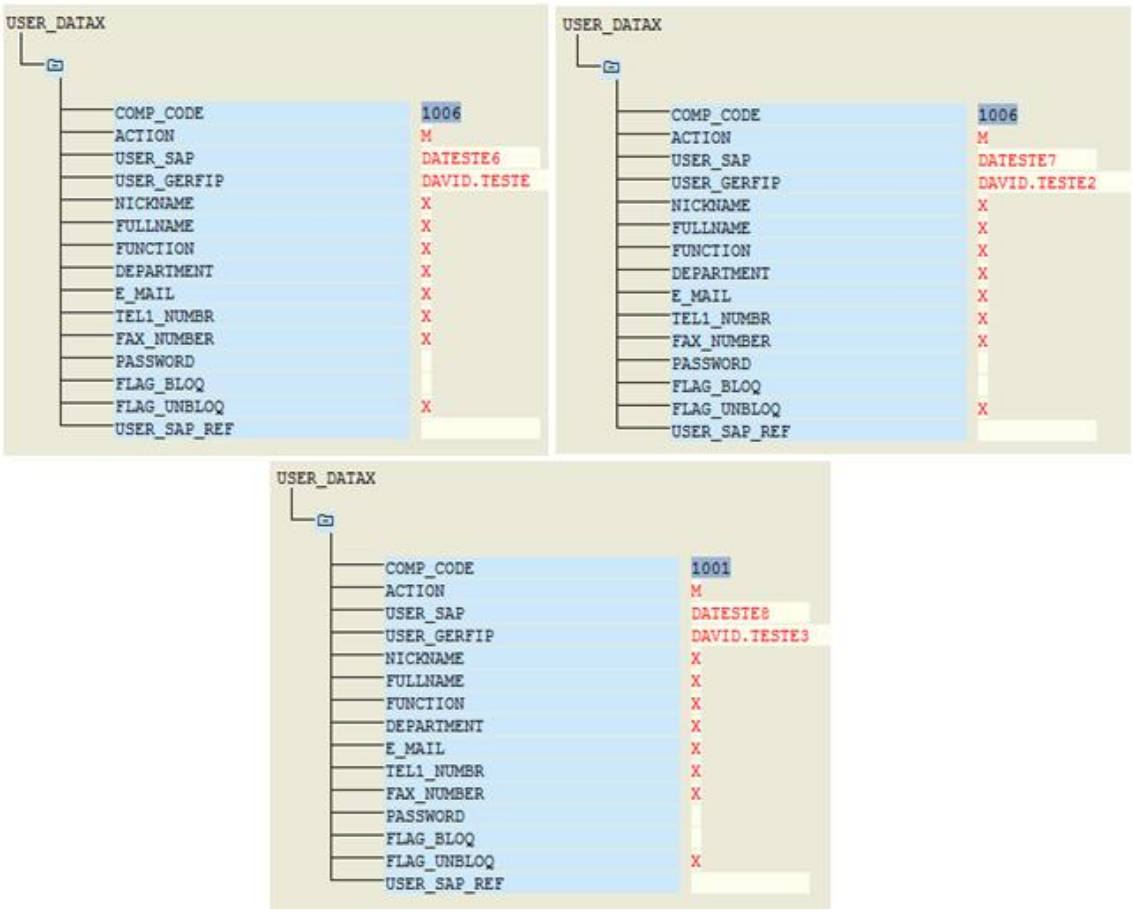


Figura de Anexo 22 - Dados de entrada de USER_DATAX no teste 13

ROLE_DATA:

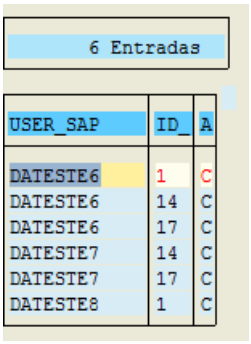
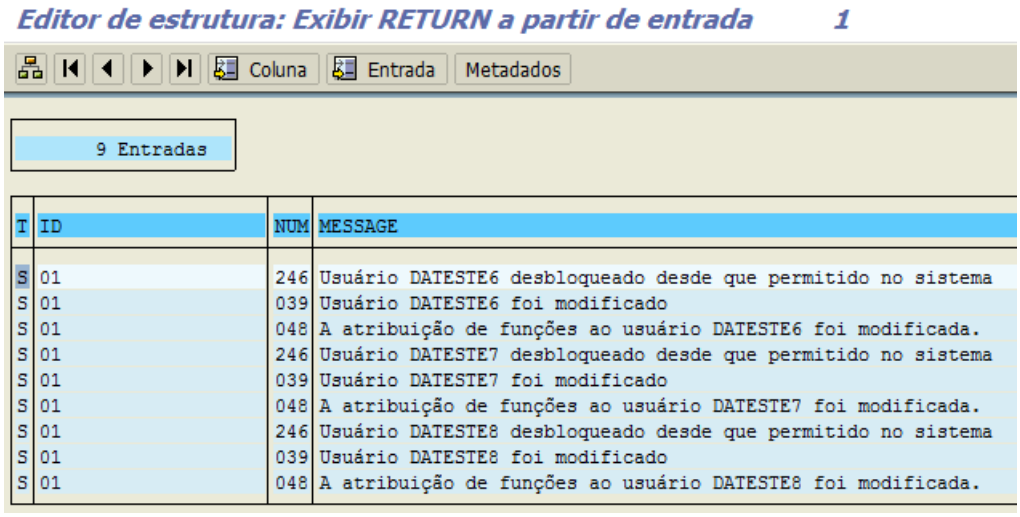


Figura de Anexo 23 - Dados de entrada de ROLE_DATA no teste 13

Resultado Esperado

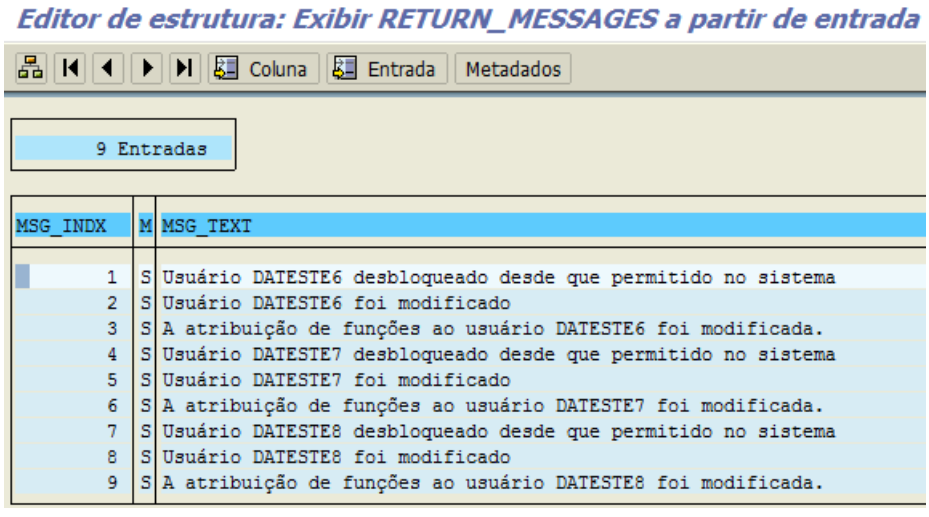
Era esperado que os utilizadores DATESTE6, DATESTE7 e DATESTE8, bloqueados em testes anteriores, fossem desbloqueados. Como foram enviadas *flags* de modificação de dados e de funções, era igualmente esperado que estes fossem modificados.

Resultado Obtido



T	ID	NUM	MESSAGE
S	01	246	Usuário DATESTE6 desbloqueado desde que permitido no sistema
S	01	039	Usuário DATESTE6 foi modificado
S	01	048	A atribuição de funções ao usuário DATESTE6 foi modificada.
S	01	246	Usuário DATESTE7 desbloqueado desde que permitido no sistema
S	01	039	Usuário DATESTE7 foi modificado
S	01	048	A atribuição de funções ao usuário DATESTE7 foi modificada.
S	01	246	Usuário DATESTE8 desbloqueado desde que permitido no sistema
S	01	039	Usuário DATESTE8 foi modificado
S	01	048	A atribuição de funções ao usuário DATESTE8 foi modificada.

Figura de Anexo 24 - Conteúdo da tabela RETURN após o teste 13



MSG_INDX	M	MSG_TEXT
1	S	Usuário DATESTE6 desbloqueado desde que permitido no sistema
2	S	Usuário DATESTE6 foi modificado
3	S	A atribuição de funções ao usuário DATESTE6 foi modificada.
4	S	Usuário DATESTE7 desbloqueado desde que permitido no sistema
5	S	Usuário DATESTE7 foi modificado
6	S	A atribuição de funções ao usuário DATESTE7 foi modificada.
7	S	Usuário DATESTE8 desbloqueado desde que permitido no sistema
8	S	Usuário DATESTE8 foi modificado
9	S	A atribuição de funções ao usuário DATESTE8 foi modificada.

Figura de Anexo 25 - Conteúdo da tabela RETURN_MESSAGES após o teste 13

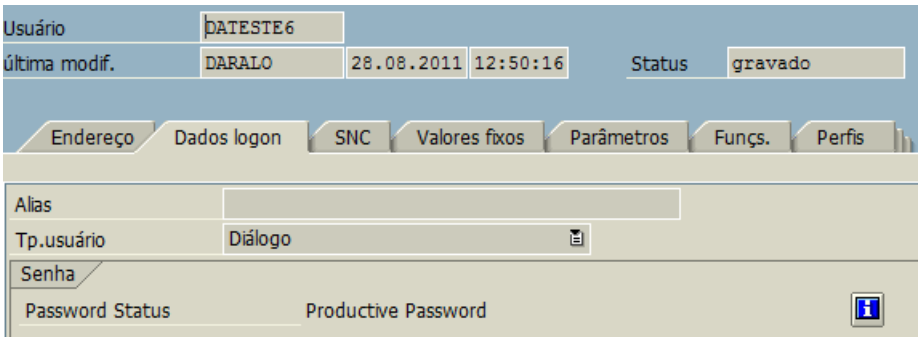


Figura de Anexo 26 - Estado de bloqueio do utilizador DATESTE6 após teste 13

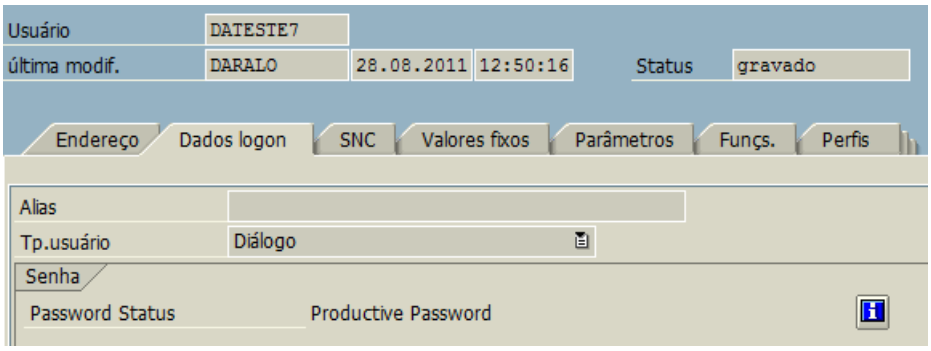


Figura de Anexo 27 - Estado de bloqueio do utilizador DATESTE7 após teste 13

Figura de Anexo 28 - Estado de bloqueio do utilizador DATESTE8 após teste 13

Modificar três Utilizadores em que dois não Existam

Dados de Entrada

DADOS DE UTILIZADOR:

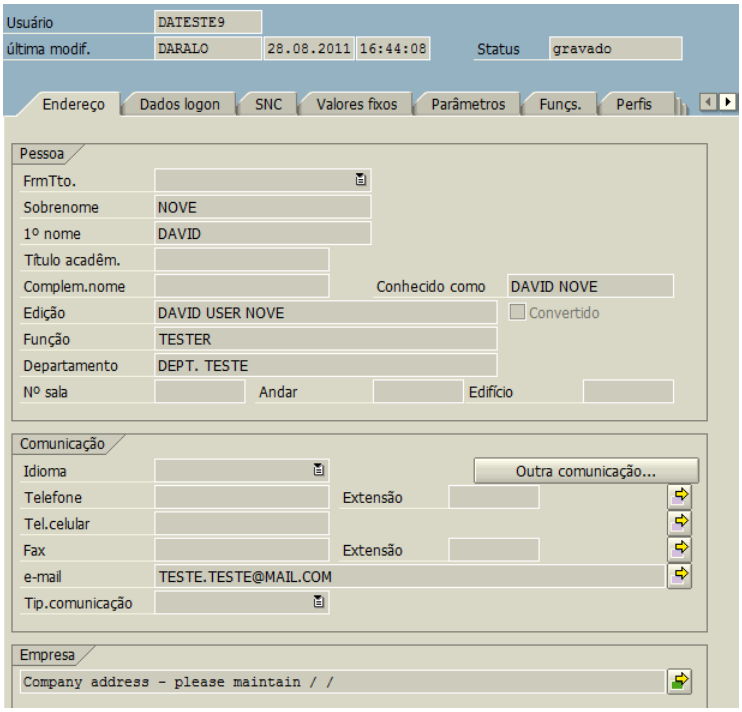


Figura de Anexo 29 - Dados do utilizador DATESTE9 antes do teste 18

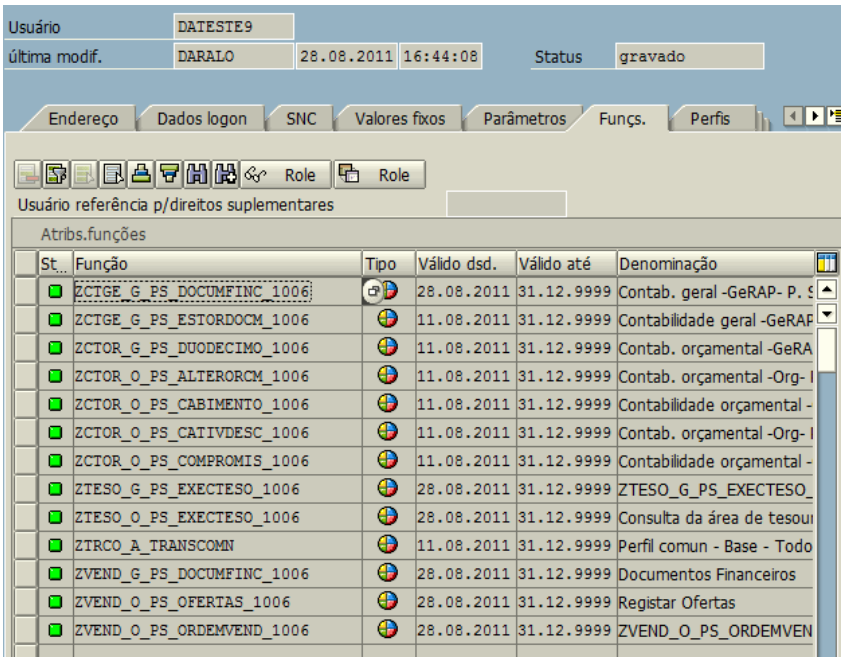


Figura de Anexo 30 - Funções do utilizador DATESTE9 antes do teste 18

FLAG_ROLE: X

FLAG_PP: X

USER_DATA:

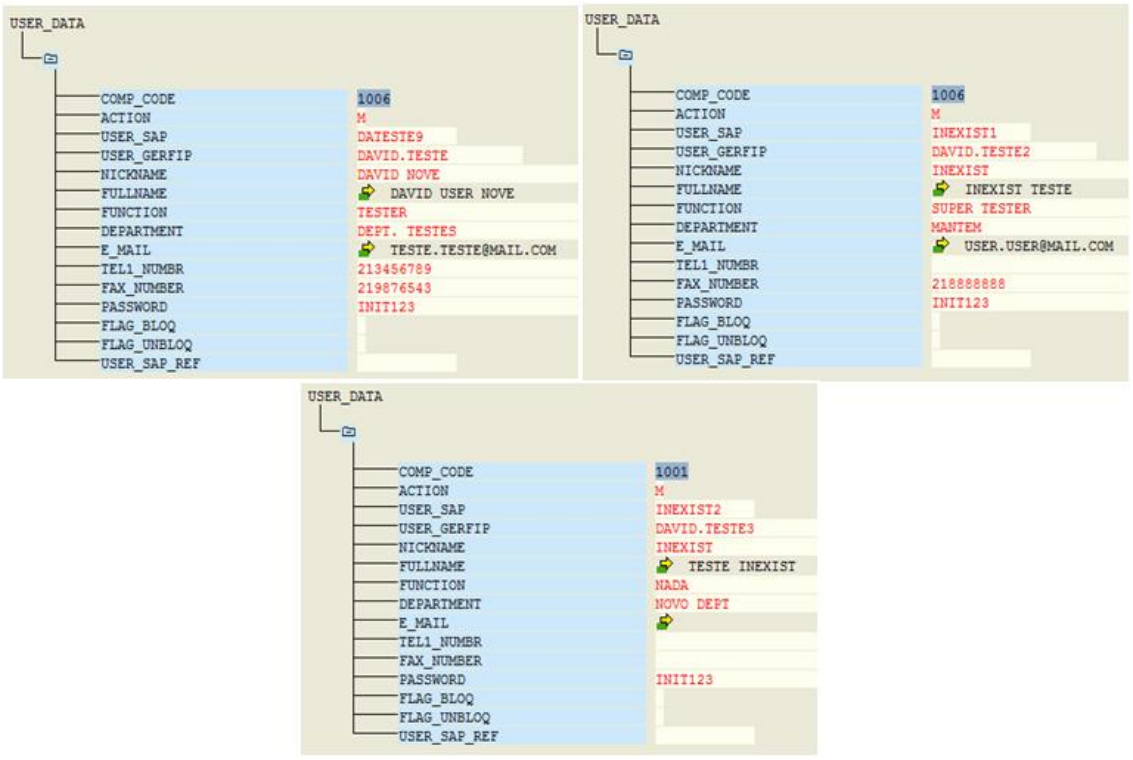


Figura de Anexo 31 - Dados de entrada de USER_DATA no teste 18

USER_DATAX:

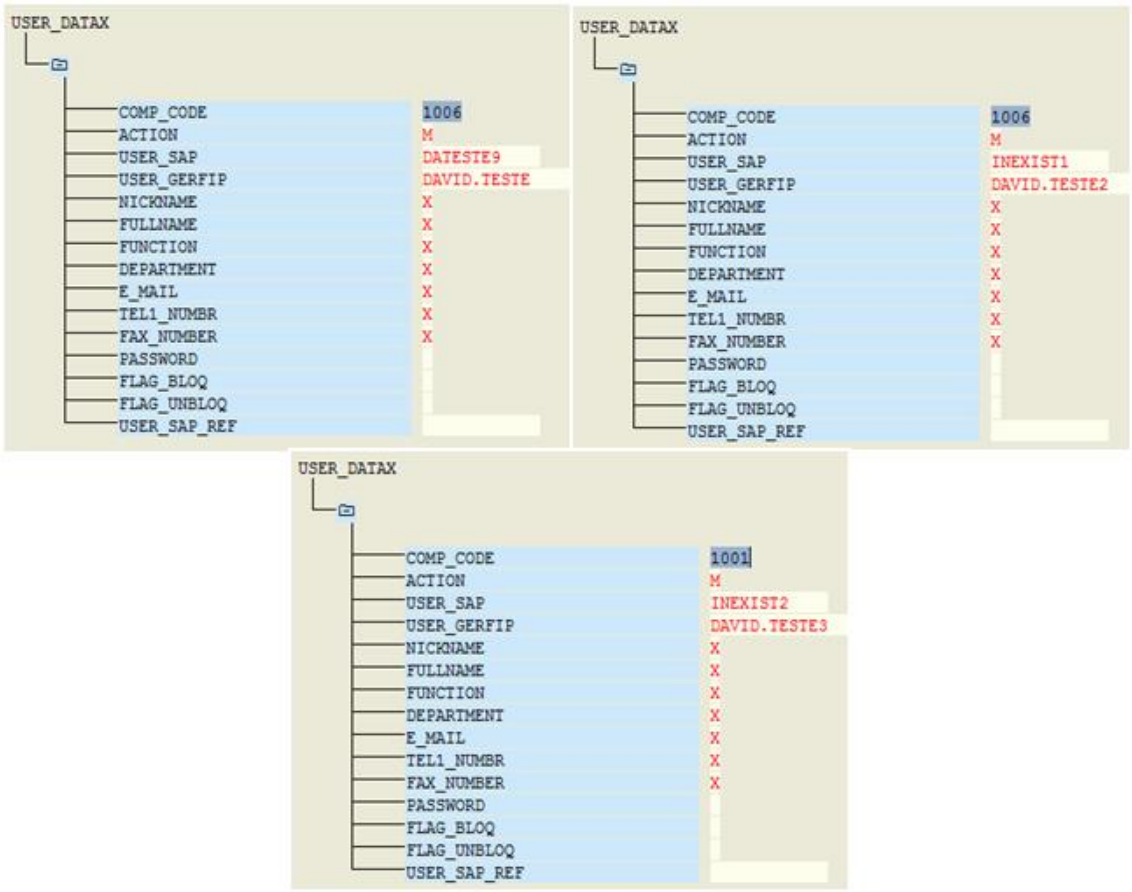


Figura de Anexo 32 - Dados de entrada de USER_DATAX no teste 18

ROLE_DATA:

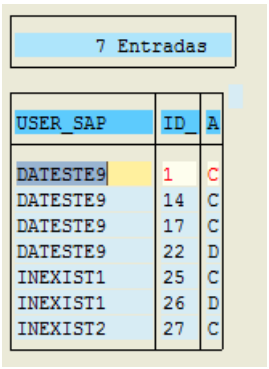
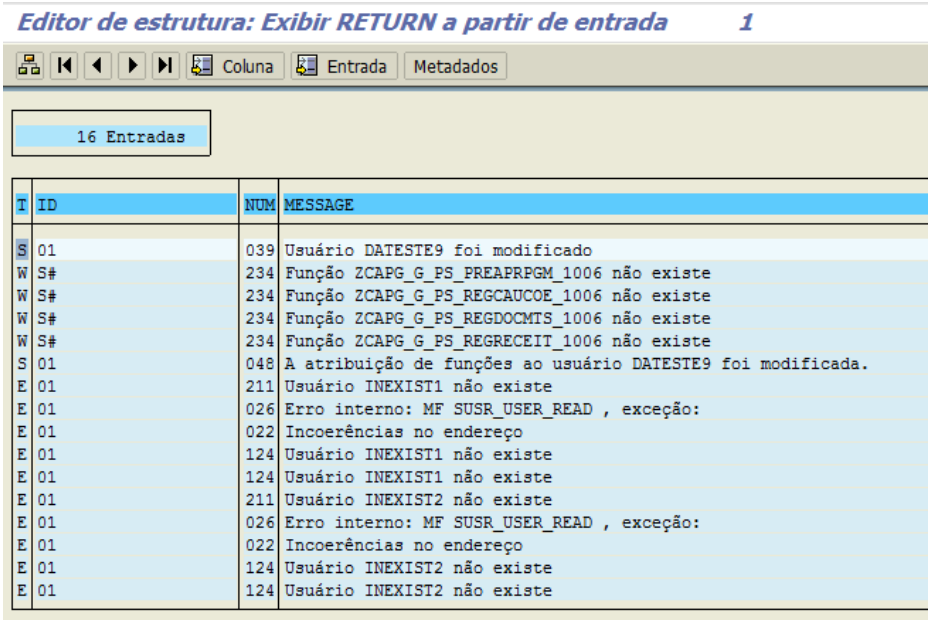


Figura de Anexo 33 - Dados de entrada de ROLE_DATA no teste 18

Resultado Esperado

Era esperado que os dados e funções do utilizador DATESTE9 fossem modificados, e que fossem devolvidos erros de utilizador inexistente para os utilizadores INEXIST1 e INEXIST2.

Resultado Obtido



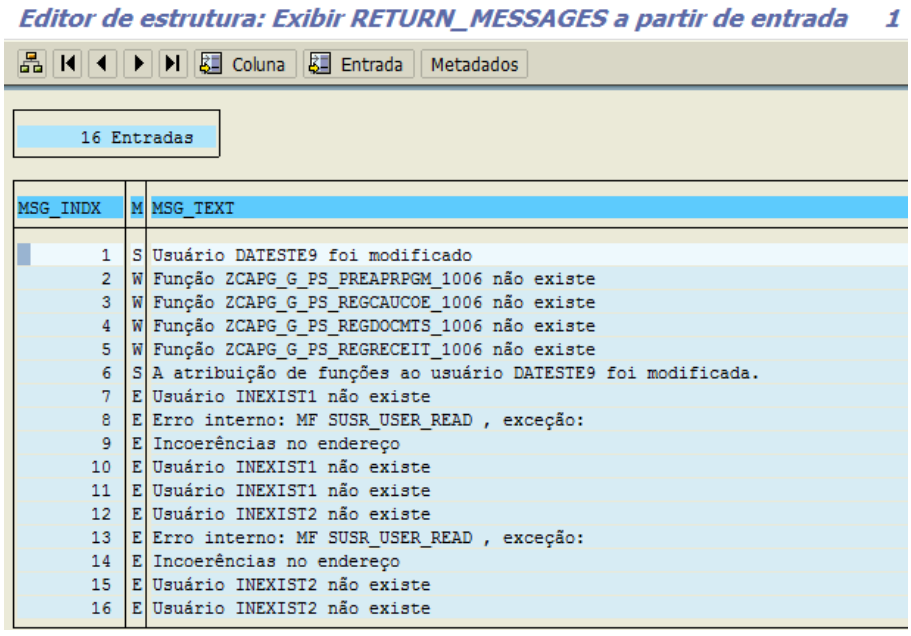
Editor de estrutura: Exibir RETURN a partir de entrada 1

Coluna | Entrada | Metadados

16 Entradas

T	ID	NUM	MESSAGE
S	01	039	Usuário DATESTE9 foi modificado
W	S#	234	Função ZCAPG_G_PS_PREAPRPGM_1006 não existe
W	S#	234	Função ZCAPG_G_PS_REGCAUCOE_1006 não existe
W	S#	234	Função ZCAPG_G_PS_REGDOCMTS_1006 não existe
W	S#	234	Função ZCAPG_G_PS_REGRECEIT_1006 não existe
S	01	048	A atribuição de funções ao usuário DATESTE9 foi modificada.
E	01	211	Usuário INEXIST1 não existe
E	01	026	Erro interno: MF SUSR_USER_READ , exceção:
E	01	022	Incoerências no endereço
E	01	124	Usuário INEXIST1 não existe
E	01	124	Usuário INEXIST1 não existe
E	01	211	Usuário INEXIST2 não existe
E	01	026	Erro interno: MF SUSR_USER_READ , exceção:
E	01	022	Incoerências no endereço
E	01	124	Usuário INEXIST2 não existe
E	01	124	Usuário INEXIST2 não existe

Figura de Anexo 34 - Conteúdo da tabela RETURN após o teste 18



Editor de estrutura: Exibir RETURN_MESSAGES a partir de entrada 1

Coluna | Entrada | Metadados

16 Entradas

MSG_INDX	M	MSG_TEXT
1	S	Usuário DATESTE9 foi modificado
2	W	Função ZCAPG_G_PS_PREAPRPGM_1006 não existe
3	W	Função ZCAPG_G_PS_REGCAUCOE_1006 não existe
4	W	Função ZCAPG_G_PS_REGDOCMTS_1006 não existe
5	W	Função ZCAPG_G_PS_REGRECEIT_1006 não existe
6	S	A atribuição de funções ao usuário DATESTE9 foi modificada.
7	E	Usuário INEXIST1 não existe
8	E	Erro interno: MF SUSR_USER_READ , exceção:
9	E	Incoerências no endereço
10	E	Usuário INEXIST1 não existe
11	E	Usuário INEXIST1 não existe
12	E	Usuário INEXIST2 não existe
13	E	Erro interno: MF SUSR_USER_READ , exceção:
14	E	Incoerências no endereço
15	E	Usuário INEXIST2 não existe
16	E	Usuário INEXIST2 não existe

Figura de Anexo 35 - Conteúdo da tabela RETURN_MESSAGES após o teste 18

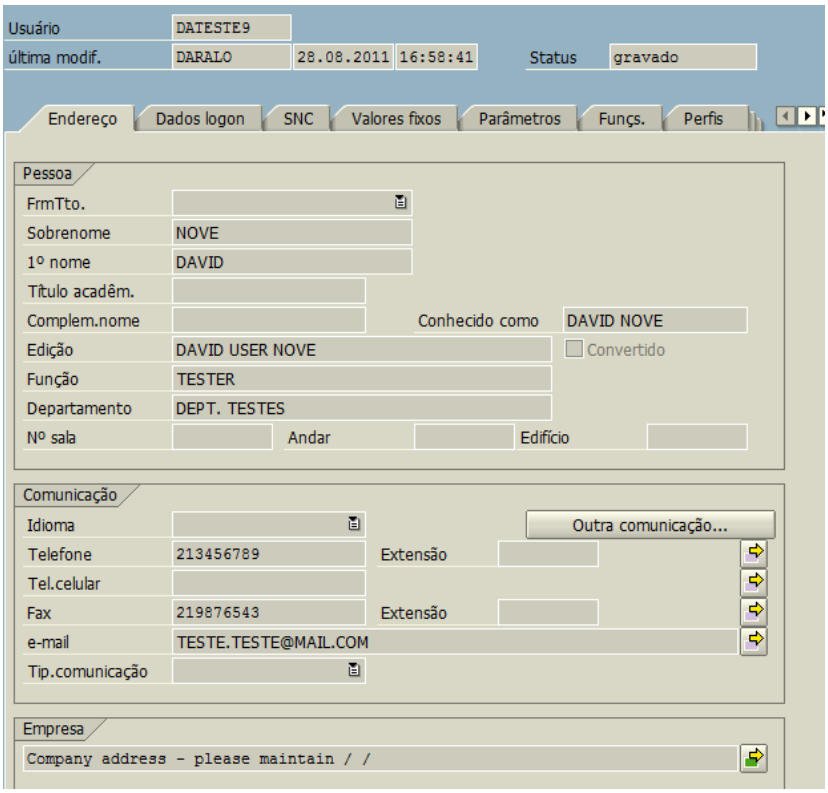


Figura de Anexo 36 - Dados do utilizador DATESTE9 após o teste 18

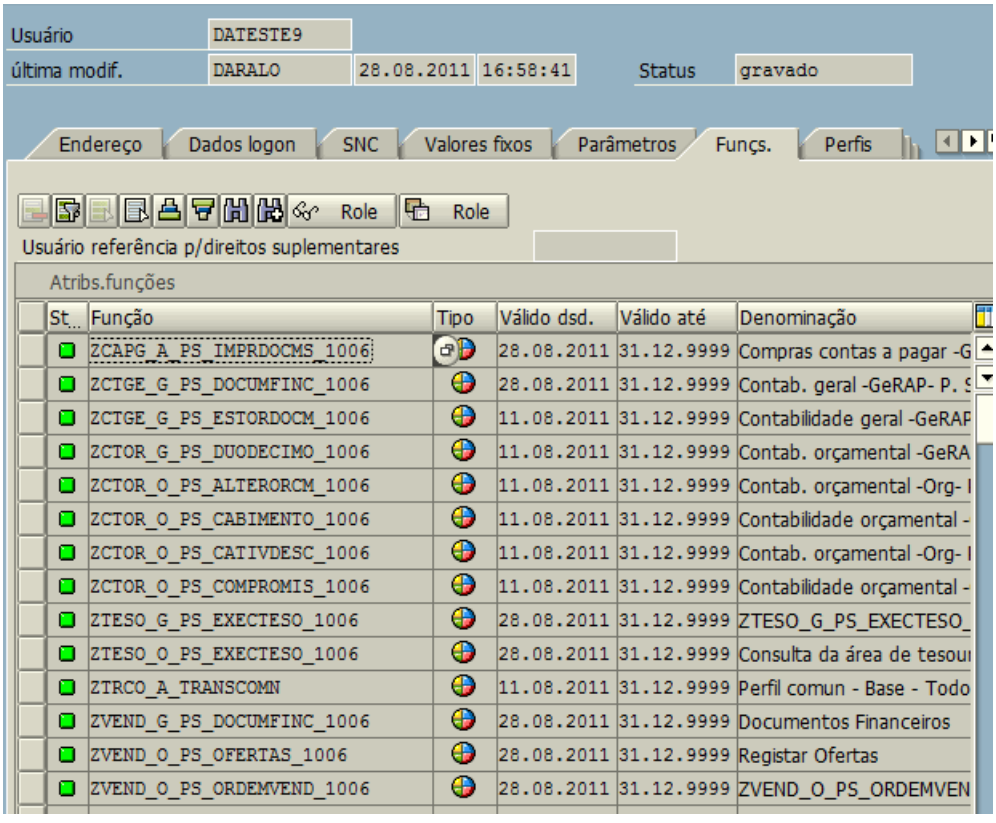


Figura de Anexo 37 - Funções do utilizador DATESTE9 após o teste 18

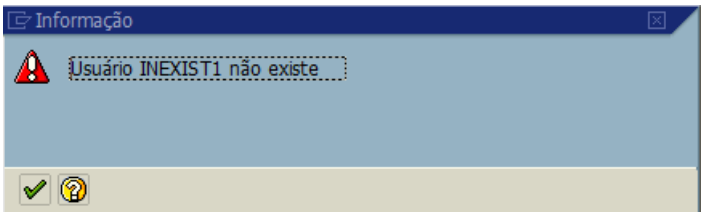


Figura de Anexo 38 - Erro ao tentar consultar o utilizador INEXIST1 após teste 18

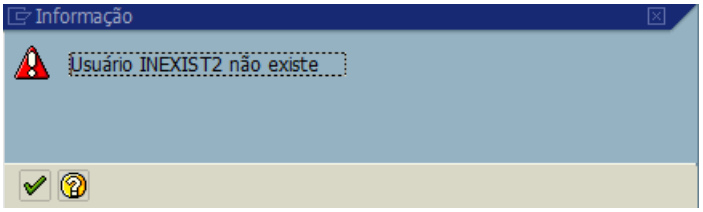


Figura de Anexo 39 - Erro ao tentar consultar o utilizador INEXIST2 após teste 18

Criar um Utilizador por Cópia de Outro

Dados de Entrada

FUNÇÕES DO UTILIZADOR A COPIAR:

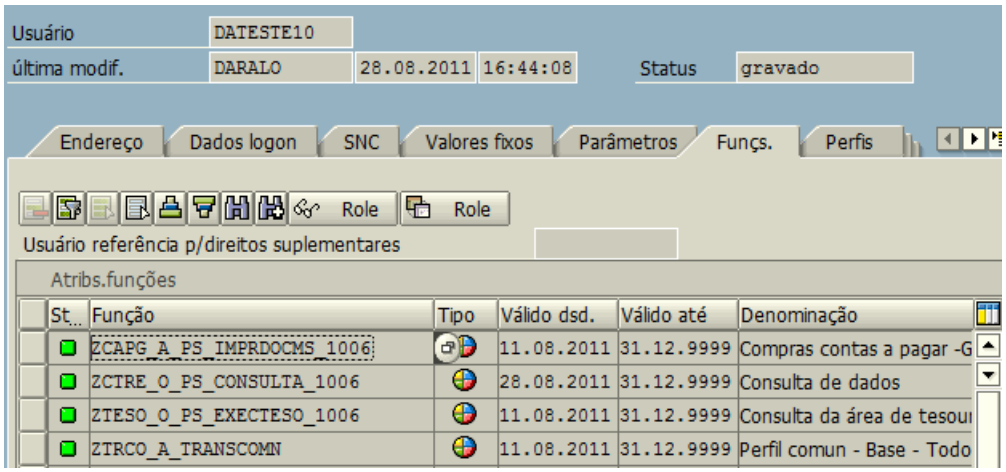


Figura de Anexo 40 - Funções do utilizador DATESTE10 antes do teste 20

FLAG_ROLE: X

FLAG_PP: X

USER_DATA:

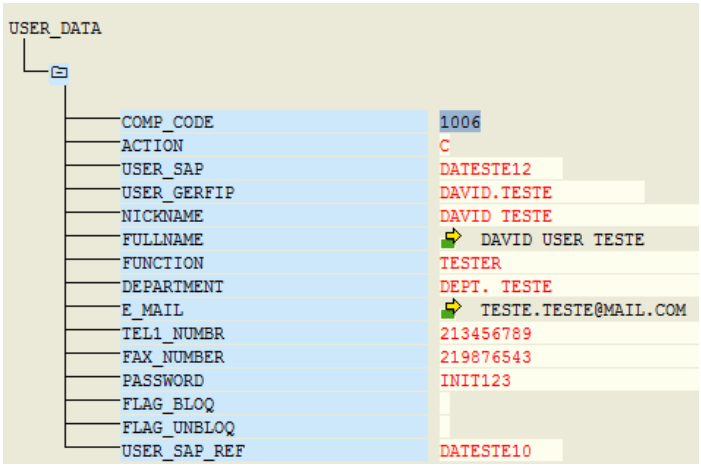


Figura de Anexo 41 - Dados de entrada de USER_DATA no teste 20

USER_DATAX:

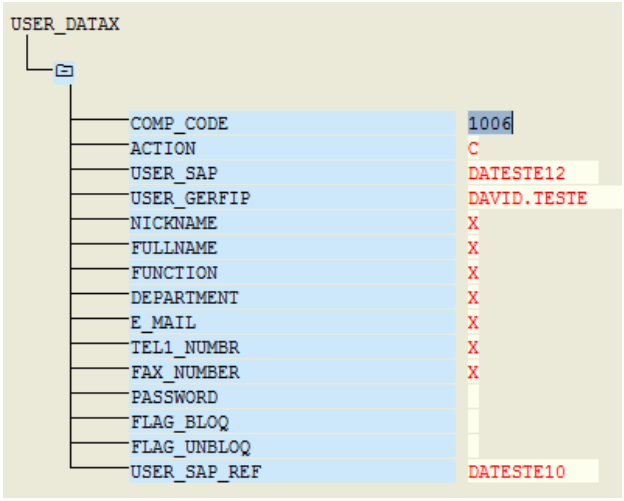


Figura de Anexo 42 - Dados de entrada de USER_DATAX no teste 20

ROLE_DATA:

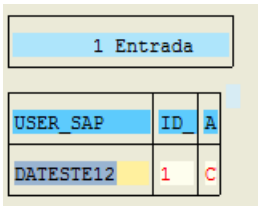


Figura de Anexo 43 - Dados de entrada de ROLE_DATA no teste 20

Resultado Esperado

Era esperado que o utilizador DATESTE12 fosse criado com as funções do utilizador DATESTE10 e as correspondentes ao ID 1, dado como entrada na tabela ROLE_DATA.

Resultado Obtido

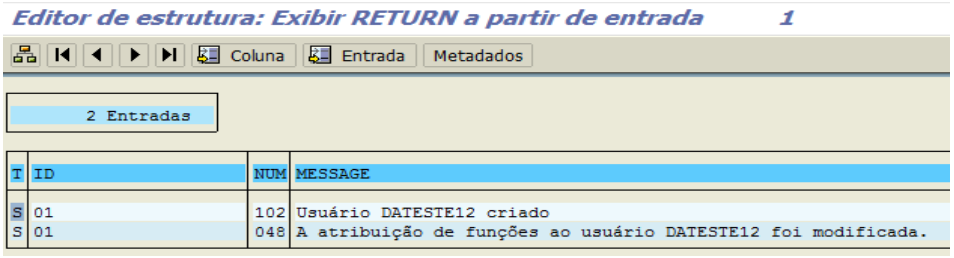


Figura de Anexo 44 - Conteúdo da tabela RETURN após o teste 20

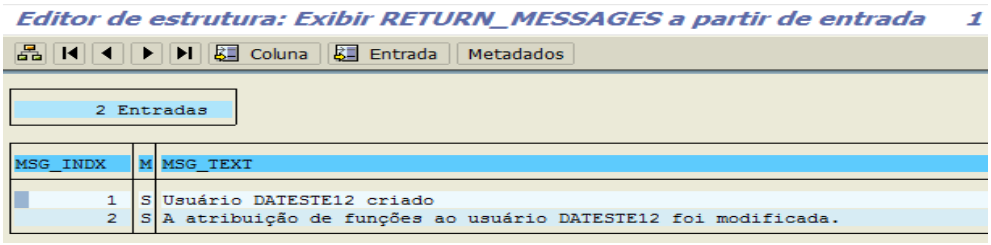


Figura de Anexo 45 - Conteúdo da tabela RETURN_MESSAGES após o teste 20

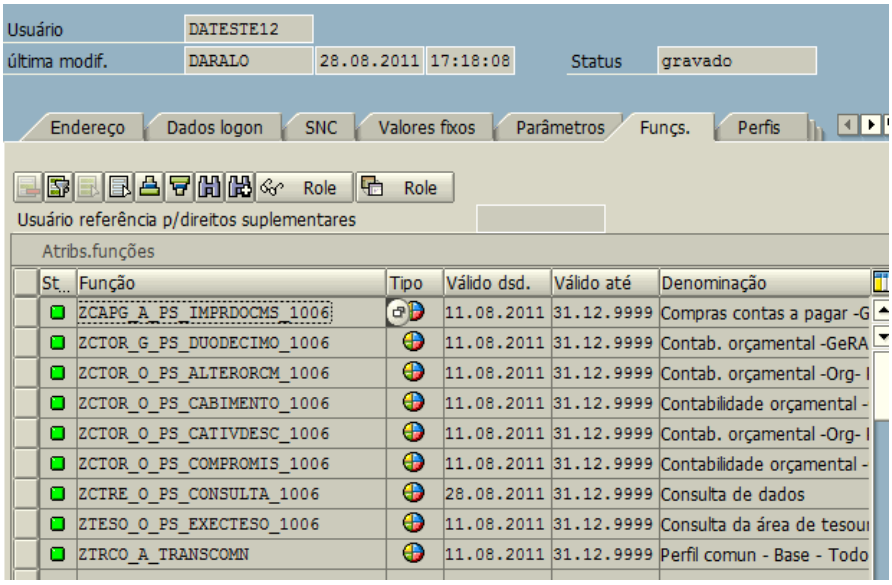


Figura de Anexo 46 - Funções do utilizador DATESTE12 após o teste 20