Relatório de Viabilidade *(Feasibility Report)*

Capa

Gestão de Identidades e Acessos

Designação do Relatório:

Análise à viabilidade do projecto “Gestão de Identidades e Acessos”

Versão do Documento:

1.0

Data:
20/03/2012

Proponente: xxxxx

Relatório de Viabilidade

1. Sumário Executivo

É pretendido disponibilizar, até dia 28 de Setembro de 2012 ea todos os utilizadores de uma instituição financeira, uma solução centralizada de gestão de contas e acessos, Assim, os principais sistemas da empresa devem ser ligados a este sistema de controlo, que irá passar a ser utilizado pelas equipas responsáveis pela gestão das contas e acessos dos diversos sistemas internos.

Como enquadramento do âmbito prevê-se a reengenharia dos processos de gestão de identidades da empresa, consequente adopção de suporte informático e respectivos serviços para adequação de uma solução às necessidades de gestão de contas e acessos da empresa. Esta linha de acção prevê uma análise dos processos existentes, a criação de um *workflow* de aprovações, a implementação da solução e respectiva customização.

Para dar resposta aos requisitos pretendidos existem três linhas de acção possíveis:

a) Manter os processos de gestão de identidades e acessos inalterados.
b) Melhorar os processos de gestão de identidades e acessos, sem promover a ligação entre os diversos sistemas.
c) Desenvolver uma solução de raiz, permitindo uma gestão de identidades e acessos integrada.

PRINCIPAIS VANTAGENS

Pretende-se uma maior rapidez no aprovisionamento de contas e acessos, reduções nos custos do processo, nos erros e no número de chamadas ao *Help Desk*, bem como o alinhamento com as políticas de segurança.

PRINCIPAIS INCONVENIENTES

Como principais inconvenientes têm-se as mudanças nos processos e os respectivos impactos, nomeadamente a resistência à mudança e a necessária adaptação dos intervenientes no processo.

Da análise do problema, considerando os custos e benefícios, das três possíveis linhas de acção, é recomendado que seja adquirida e implementada de raiz uma solução de gestão de identidades, ou seja a opção “c”. As outras duas alternativas não se tornam viáveis porque os custos associados a não adoptar este projecto ou apenas melhorar os processos já existentes, sem integração e sincronização total, vão sendo cada vez mais elevados ao longo do tempo.

2. Descrição do Problema

A gestão de identidades compreende as funções de gerir contas de acesso dos colaboradores aos diversos sistemas de informação da empresa. Associado a essa função, há também a gestão de grupos (ou perfis) que permite atribuir a cada colaborador níveis variáveis de acessos aos recursos lógicos (pastas compartilhadas, filas de impressão, etc.). A quantidade elevada de sistemas existentes na empresa é suficiente para tornar as actividades de gestão onerosas e demoradas, além de ser extremamente difícil manter a conformidade com as políticas de seguranças.

Da grande quantidade de sistemas existentes na empresa e as necessidades de negócio que obrigam aos colaboradores a terem acesso a grande parte desses sistemas, resulta outro problema que é a gestão das *passwords*. Cada colaborador é obrigado, segundo as políticas de segurança, a definir *passwords* únicas e complexas para os sistemas, que por sua vez geram um grande volume de chamadas ao H*elp Desk* para solicitação de *resets* e desbloqueio de contas.

Outro factor de grande importância é a gestão temporal dos colaboradores e os respectivos acessos de forma automática. Actualmente, muitas contas continuam activas nos sistemas, mesmo após a desafectação e/ou a saída de colaboradores, devido à incapacidade dos administradores dos diversos sistemas em identificar os colaboradores inactivos.

3. Critérios de Decisão

- Benefícios tangíveis a curto prazo (ROI), porque diminui a necessidade de recursos humanos para a gestão de acessos e identidades dos sistemas de informação.
- Contribuição da solução para o alinhamento dos processos de TI/SI com as políticas corporativas de segurança da empresa.
- Redução de custos indirectos, aumentando a produtividade dos colaboradores da empresa, devido à optimização do processo de gestão de acessos e identidades.
- Recursos que a solução proporciona promovem uma maior eficiência na gestão dos sistemas de informação, trazendo benefícios tangíveis a médio-longo prazo.

4. Fontes e confiabilidade dos dados

- Análise de “estudo de casos” facultado pelos fornecedores.
- Visita a um “caso de sucesso” facultado por um fornecedor.
- Opiniões de especialistas.
- Análises em revistas especializadas da área.

5. Esboço dos requisitos

- ✓ **Requisitos de negócio:** Assegurar a conformidade com as políticas de segurança corporativas. Assegurar que a atribuição de acessos é sujeita a aprovações e passível de auditoria.

- ✓ **Requisitos técnicos:** Gerir o sistema de identidades e acessos através da *intranet* ou seja, disponibilizar um interface *web*. Disponibilizar um interface de gestão de *passwords self-service.* Garantir a segurança da comunicação através da utilização de *SSL* entre todos os componentes da solução. Integrar com a base de dados de recursos humanos (fonte autoritária de dados). Garantir a sincronização das *passwords* do *Active Directory* para todos os sistemas.

- ✓ **Requisitos funcionais e de qualidade:** Garantir uma disponibilidade mensal do sistema de 99.5%. Garantir que os componentes da solução são redundantes. Garantir a sincronização de dados e *passwords* automaticamente e em tempo quase real, nomeadamente, em até 10 segundos.

- ✓ **Requisitos financeiros:** Garantir o cumprimento do orçamento disponível.

- ✓ **Requisitos temporais:** O projecto deverá terminar dia 28/09/2012 porque o início de exploração da solução deve coincidir com a aplicação das normas corporativas de segurança, que entram em vigor a partir de 01/10/2012.

6. Alternativas de solução

6.1. Alternativa “a”: Manter os processos de gestão de identidades e acessos inalterados.

- ✓ **Descrição técnica da solução:** A gestão dos sistemas continua a ser efectuada de maneira descentralizada, com equipas especializadas para os diversos sistemas e com os processos manuais actualmente em prática.
- ✓ **Benefícios:** Sem novos benefícios a assinalar.
- ✓ **Custos:** Mantêm-se os elevados custos actualmente existentes e associados à gestão dos vários sistemas de forma descentralizada, devido à necessidade de manter nos quadros internos da empresa equipas especializadas na gestão dos diversos sistemas.
- ✓ **Riscos:** Reduzidos na medida em que não implica qualquer alteração.
- ✓ **Problemas:** Manter equipas com conhecimentos das diferentes plataformas tecnológicas; Diversas etapas manuais nos processos, como por exemplo, nas aprovações; Baixa capacidade em auditar os processos e sistemas.
- ✓ **Restrições:** Alterações de pessoal em RH não são reflectidas nos sistemas da empresa. Grande quantidade de contas e acessos indevidos, por falta de sincronização dos dados dos sistemas. Não escalável e de difícil auditoria.
- ✓ **Pressupostos:** Não há alterações relacionadas com o processo de gestão de identidades e acessos.
- ✓ **Recursos necessários:** Mantêm-se os recursos existentes actualmente.
- ✓ **Implicações organizacionais:** Falta de alinhamento com estratégia da empresa. Falta de conformidade com políticas de auditoria. Dificuldade em escalar para maior quantidade de utilizadores.

6.2. Alternativa "b": Melhorar os processos de gestão de identidades e acessos sem integrar os diversos sistemas.

- ✓ **Descrição técnica da solução:** O processo requer a optimização do *workflow* de gestão de identidades que, por sua vez, deve ser implementado com o apoio de uma solução informática.
- ✓ **Benefícios:** Formalização (desenho e documentação) do processo de gestão de identidades e acessos.
- ✓ **Custos:** Aproximadamente 120.000 Euros.
- ✓ **Riscos:** Riscos internos associados à reengenharia de processos: resistência à mudança e demora no fecho/aprovação dos processos.
- ✓ **Problemas e restrições:** Para que os benefícios fossem completamente realizáveis seria necessário efectuar a reengenharia dos processos, implementar uma solução informática que se adapte aos processos e, por fim, automatizar o aprovisionamento das contas e acessos com base em perfis, o que, entretanto, levaria à alternativa "c".
- ✓ **Pressupostos:** Reengenharia de processos.
- ✓ **Recursos necessários:** Responsáveis pelos vários sistemas; Contratação de serviços de consultoria externa.
- ✓ **Implicações organizacionais:** Alinhamento parcial com a estratégia, sem dar resposta aos requisitos definidos.

6.3. Alternativa "c": Desenvolver uma solução de raiz, permitindo uma gestão de identidades e acessos centralizada com integração dos sistemas.

- ✓ **Descrição técnica da solução:** Prevê a reengenharia dos processos de gestão de identidades da empresa, consequente adopção de suporte informático e respectivos serviços para adequação às necessidades de gestão de contas e acessos de forma centralizada. Assim, esta linha de acção prevê uma análise dos processos existentes, criação de um *workflow* de aprovações, implementação da solução e customizações consoante os requisitos identificados.
- ✓ **Benefícios:** Gestão centralizada dos acessos aos vários sistemas; redução significativa dos custos relativos à gestão de identidades e acessos; cumprir com as "melhores práticas" de segurança e facilitar a conformidade com as políticas de segurança da entidade.
- ✓ **Custos:** €200.000.

- ✓ **Riscos:** Não existir documentação dos processos actuais e dificuldade em interligar sistemas com diferentes tecnologias.
- ✓ **Pressupostos:** Reengenharia de processos; Base de dados de RH actualizada; Disponibilidade dos responsáveis dos vários sistemas.
- ✓ **Recursos necessários:** Responsáveis dos vários sistemas; Novos servidores e licenças do *software*; Contratação de serviços de consultoria externa.
- ✓ **Implicações organizacionais:** Alterações nos processos de gestão de identidades e acessos. Melhora na qualidade dos serviços de TI/SI, associados com gestão de contas e acessos. Maior capacidade e maior rapidez em dar resposta às alterações nas políticas de segurança dos sistemas de informação.

7. Comparação e avaliação das alternativas

Alternativa	Viabilidade Temporal	Viabilidade Técnica	Viabilidade Financeira	Alinhamento Estratégico	Ordenação
a	Alta	Alta	Baixa	Baixo	3º
b	Alta	Alta	Baixa	Baixo	2º
c	Alta	Alta	Alta	Alto	1º

A viabilidade financeira, no contexto da tabela acima, deve ser entendida como a relação custo-benefício da solução.

Embora a alternativa "a" não implique custos adicionais, os associados aos processos actuais são elevados e tendem a crescer com a adopção de novos sistemas e com o aumento do número de utilizadores.

A opção b), comparativamente com a opção c), tem um custo de projecto mais baixo. No entanto, acarreta grande parte dos custos identificados na opção a), tornando-a a médio-longo prazo numa alternativa muito dispendiosa.

A opção c) é a única alternativa sustentável a longo prazo. Apesar de ser necessário um investimento inicial superior às restantes opções, os benefícios resultantes são em tudo superiores às outras alternativas.

8. Recomendações

Recomenda-se a adopção de uma solução de raiz que deve incorporar todo o ciclo de vida de identidades e acessos na empresa. O processo deve ser redesenhado de modo a incluir um *workflow* com múltiplos níveis de aprovação. Os principais sistemas da empresa devem ser geridos a partir de um único sistema de gestão, com aprovisionamento automático das contas e acessos, sob controlo da aplicação de gestão, de acordo com os perfis dos colaboradores. Por fim, o sistema deve incorporar sincronismo de *passwords* e *self-reset*. Deste modo, a opção “c” é a recomendada.

Para a recomendação, para além dos benefícios que resultam da sua implementação, atendeu-se ao custo das alternativas e à imprescindível adopção das "melhores práticas" de segurança que possibilitem à empresa estar em conformidade com os critérios de segurança necessários a uma empresa do sector financeiro.

9. Glossário

Active *Directory* - Serviço de directório de utilizadores e acessos, que armazena informações sobre objectos lógicos em rede (pastas compartilhadas, impressoras, etc) e disponibiliza essas informações a utilizadores dessa rede.

Aprovisionamento – Processo que inclui as actividades de criação de um identificador único de utilizador (conta, ou ainda *username*), criação dessa conta em um sistema e atribuição de acessos e grupos.

Autorização – Recurso quer permite definir níveis de acesso de utilizadores a recursos lógicos nos sistemas de informação.

Directory Services – Um recurso lógico, normalmente composto de uma grande base de dados, que centraliza dados e informações relativos a uma entidade ou recurso, como por exemplo, colaboradores da empresa ou serviços disponíveis em uma aplicação.

Gestão de Identidades – Gestão das contas dos colaboradores, normalmente de modo transversal na empresa.

Gestão de Acessos – Gestão dos acessos aos sistemas corporativos, através de recursos de gestão de identidades e autorização.

HR *Feed* (*Human Resources Feed*) - Processo de obtenção dados a partir de uma fonte de dados autoritária, que é normalmente acedida somente em modo de leitura, e que vai alimentar os demais sistemas de informação através de um processo de replicação de dados selectivo.

IAM – Identity and Access Management (ver "Gestão de Identidades" e "Gestão de Acessos").