

# Os negócios das companhias com a gestão de perfis e privilégios

Maio de 2008

Autor: Sérgio Teixeira, sócio-diretor da Order



## O ciclo de vida do privilégio de acesso

Para ilustrar o tema, vamos recorrer a uma estória, que ocorre de forma parecida na maioria das grandes organizações. As situações e nomes são fictícios.

Emília Lopes, uma nova funcionária, é admitida na companhia. Como todos os demais colaboradores, ela veio para exercer atividades importantes para a companhia, na área de Suprimentos. Seu chefe já a orienta e solicita as suas credenciais nos diversos sistemas: SAP, Siebel, Ponto Eletrônico, Intranet, Internet, Email, Telefonia e Crachá. Por se tratar de uma Analista de Compras nível Pleno, Emília ganha acesso restrito a algumas funções específicas nos sistemas SAP e Siebel. Tudo pronto! Ela já pode começar a trabalhar (afinal, hoje em dia, sem acessos aos sistemas, muitos sequer conseguem trabalhar!). Emília recebeu o seu primeiro conjunto de privilégios de acesso.

A performance de Emília é muito boa, tal qual a companhia, e então ela é promovida: passa a ser Analista de Compras Senior. Ela tem novas responsabilidades e, em consequência, deve ter um nível de acesso superior nos sistemas da companhia. Muito bem: Emília ganha mais um conjunto de privilégios de acesso.

A vida continua, e Emília continua trilhando o sucesso: ela tem uma oportunidade interessante na Área de Marketing. Agora, são necessários acessos aos sistemas de Marketing: Pesquisa de Mercado, Comunicação Interna, Boletim Eletrônico, Pastas de Marketing, entre outros. Emília ganha mais privilégios de acesso.

## Ataques e fraudes: de quem é a culpa?

De uma forma natural, estamos em meio à grande ferida das organizações no tocante à gestão de seu maior bem: a informação. São corriqueiros os relatos de fraudes eletrônicas, furto de identidades de pessoas, evasão de informações confidenciais, modificação indevida de informações...

Estudos de institutos de pesquisa apontam que a grande maioria dos “ataques” eletrônicos ocorrem de dentro da organização. Mas como é possível, se a maioria das pessoas que conhecemos não comete estes “delitos”? Os mesmos institutos indicam que, relacionados ao

fato anterior, a maioria dos incidentes acontece acidentalmente, por erro do usuário. Vamos explicar.

Voltando à nossa estória: um dia, já trabalhando na área de Marketing, Emília, com sua grande virtude de auto-organização, estava “limpando” a sua pasta de arquivos. Ela viu uma planilha com uma data antiga, com um nome que ela não lembrava. “Bem, vou deletar” – pensa Emília, e assim o faz. Que azar! Era a planilha de preços de produtos da Área de Suprimentos!

Vamos deixar de lado os fatos decorrentes desta ação para focarmos no cerne de nossa discussão. Bem, do ponto de vista da auditoria, houve uma ação indevida em uma informação por um usuário não autorizado (que não estava relacionado com a área de Suprimentos). Sim, é um ataque. Já podemos entender muito do por que a maioria dos ataques vem de dentro da organização.

Pergunta fatal: qual a causa? Outros perguntariam: “Emília foi culpada?”. Lembremos, Emília estava agindo de muita boa índole e de forma muito colaborativa à companhia.

Não é necessário nenhum guru para constatar: a pessoa necessita apenas dos privilégios de acesso para suas atividades de negócio, nada mais, nada menos (conceito do mínimo e menor privilégio). Se este princípio estivesse sido aplicado ao caso da Emília, ela sequer teria visão das informações de Suprimentos, uma vez que ela pertencia ao Marketing. Portanto, Emília é inocente. A culpada: a falta de Gestão dos Privilégios.

## **Responsável pela informação: a área de negócios**

Claro que muitos sábios-de-fatos-imprevistos apontarão o dedo pra alguém: a área de TI, o pessoal de Help Desk, a área de segurança da informação, o chefe da Emília, o ex-chefe da Emília... Afinal de contas, quem deve certificar que um determinado privilégio está devidamente assinalado? Aqui, mais um interessante episódio do espetáculo das organizações.

Gosto de utilizar o exemplo dos bancos. A agência central do Banco X possui 100 funcionários: gerente geral, gerente de negócios, gerente administrativo, gerente adjunto, gerente de investimentos, gerente de contas de pessoa física (ou jurídica), coordenador de serviços, caixas, auxiliar de caixas, assistentes, recepcionistas. Este contingente se presta a todos os serviços do

banco: investimentos, pagamentos de contas, aberturas de contas correntes, empréstimos, seguros, cartões de crédito, etc.

O Banco X abriu um posto bancário numa grande empresa. Neste posto, há três funcionários: um gerente e dois caixas. Quais são os serviços oferecidos? Ora, os mesmos da agência central (ou grande parte deles): investimentos, pagamentos de contas, aberturas de contas correntes, empréstimos, seguros, cartões de crédito, etc.

Qual a diferença do conjunto de privilégios de acesso entre a agência central e o posto bancário? Nenhuma! Porém, como era de se esperar, o caixa do posto bancário possui, em tese, um conjunto de privilégios muito maior do que o mesmo caixa da agência central. Abre parênteses: esta é uma arena de boa discussão para as áreas de RH dos bancos. Sempre se procura evitar os desvios de função e as conseqüentes ações trabalhistas dos funcionários. Neste caso, um caixa estaria exercendo atividades de um gerente, inclusive com prova eletrônica (exemplo: cópias de telas de sistemas gerenciais)? Fecha parênteses.

Vida prática: é solicitado privilégio de acesso na função de aprovação de crédito a um caixa do posto bancário. O analista que concederá o acesso exerce a boa prática: consulta as normas da companhia sobre a política de acesso. Está muito claramente expresso: “A função de aprovação de crédito deve ser concedida exclusivamente a gerentes de negócios”. O analista responde: “este privilégio não pode ser concedido”. Minutos depois, o diretor da rede de agências liga: “dê logo este acesso, porque precisamos atender ao cliente que está no balcão!”. Sem muitos comentários: o acesso é concedido.

Meses depois, chega a turma da auditoria. É evidenciado que há um privilégio de acesso indevidamente concedido. Sem muitos comentários: foi necessário para atender a uma exigência de negócios. Grande pergunta: quem é o responsável por este privilégio?

Entra em cena a temida e famigerada sombra das fraudes, riscos operacionais e o batalhão dos controles internos e a exaustiva lista das exigências regulatórias. Cada vez mais as empresas aderem: o responsável pela informação é a área de negócio que responde por ela. As informações não pertencem à “turma do TI”, mas à Finanças, Controladoria e Contabilidade, Recursos Humanos, Vendas e Marketing, Produção, etc. Sim, quem “assina o cheque” são eles. Ou, em outras palavras, as áreas de negócio têm direta co-responsabilidade pelas informações.

## **Roles ou Perfis**

E se olharmos os sistemas das companhias, geralmente empresas antigas, constataremos o “mar de privilégios”: milhares de pessoas com acessos a milhares de recursos de TI. Coça a cabeça: quem acessa o quê? Por onde começar? Seria muito mais agradável, seguro e produtivo fazer esta análise se entendêssemos os grandes agrupamentos de privilégios. Afinal, se uma atividade de negócio existe, há um conjunto de privilégios para ela. Este é o esboço do termo (em inglês) “Role”: um conjunto de privilégios entre pessoas e seus respectivos recursos para uma determinada finalidade.

Ainda não há um padrão para este termo em nossa língua portuguesa. É muito comum nas companhias se empregar “Perfil” como sinônimo. Alguns discordam, e utilizam outros termos, como perfil por função, papel organizacional ou simplesmente papel. Aqui, vou utilizar a terminologia da maioria que conheço: Perfil.

Como mergulhar no mar de privilégios e fazer a modelagem dos agrupamentos em perfis? Falo de experiência própria e de experiências que conheci de algumas empresas: fazer de forma manual, empírica, é oneroso, improdutivo, desgastante, demorado e com grande margem de erro. Começa-se com planilhas Excel, que se tornam insuficientes, que se convertem em bancos de dados Access, que se tornam insuficientes, que se convertem em grandes tabelas de bancos de dados massivos, que se tornam muito difíceis de lidar, por uma série de motivos. Este processo é chamado de Garimpagem de Perfis (Role Mining). Denominação muito adequada quando executada pelo “suor manual”.

## **As tecnologias de Gestão de Perfis e Privilégios**

Há quase três anos, tivemos a satisfação de conhecer a tecnologia da empresa israelense Eurekaify. Ela é muito pragmática e simples de usar. Baseia-se em um algoritmo próprio, patenteadado, que utiliza a inteligência de reconhecimento de padrões. Basta importar para esta ferramenta as informações sobre os privilégios de acesso atuais e cruzar com as informações de RH. É só começar a “brincar”!

A ferramenta permite a completa modelagem de perfis, bem como toda a análise da qualidade dos privilégios: excesso e falta de privilégios, recursos e perfis redundantes, desvios e exceções

dos padrões de privilégios, entre outros. Nisto, são aplicadas algumas metodologias poderosas com simples cliques de mouse. Estas são as atividades de Engenharia de Perfis (Role Engineering), cujos resultados deverão ser validados pelos gestores (donos ou responsáveis) pelas informações de cada um dos perfis.

Tem-se toda a habilidade de se criar regras de auditoria, como, por exemplo, a de segregação de funções (segregation of duties), tão exigidas pelas regulamentações (Sarbanes-Oxley, por exemplo). Os registros *der auditoria* também podem ser encaminhados aos gestores, para que eles sejam favorecidos com as indicações de privilégios suspeitos ou fora do padrão.

## **Certificação de Perfis e Privilégios**

Através de uma interface web, os gestores aprovam ou rejeitam, um a um, as pessoas, os perfis e recursos que estão sob sua gestão. Pode-se adicionar comentários.

Há um grande pulo do gato: as campanhas de certificação. Nelas, os gestores recebem emails sobre a necessidade de revisão dos acessos e dirigem-se à interface web pelo clique no indicador que está no próprio email. Pode-se acompanhar o progresso das certificações, bem como enviar novos emails de lembrete, uma vez que as campanhas podem ter prazo definido.

## **Modelo de Gestão Baseada em Perfis (Role Based Management)**

Desde os anos 70, se emprega o conceito de Controle de Acesso Baseado em Perfis (Role Based Access Control ou RBAC). Até a virada do milênio, este conceito foi utilizado de forma empírica, o que causou grande confusão e má utilização deste conceito. David Ferraiolo e alguns colaboradores desenvolveram o primeiro padrão para este conceito, o qual foi registrado no NIST (National Institute of Standards and Technology). Com ele, hoje há um ponto de convergência para se certificar se o sistema ou modelo segue o conceito de RBAC.

Com a evolução e complexidade dos sistemas de tecnologia e o acelerado dinamismo dos negócios, buscou-se convergir as práticas de RBAC com as exigências das organizações. O mercado começa a adotar o termo Gestão de Acessos Baseada em Papéis (ou Perfis) ou, em inglês, Role Based Management.

Cada vez mais busca-se o aumento de produtividade das empresas. Com isto, sem “chover no molhado”, aumenta-se a performance das organizações, diminui-se a intervenção humana e os consequentes acidentes, diminui-se o risco operacional, melhoram-se os processos, amplia-se a qualidade dos serviços, etc., etc.

Na arena dos sistemas de gestão de acessos, busca-se a automação de processos e as interfaces de auto-serviço para os usuários. Assim, alguns processos e benefícios são cada vez mais cobiçados. Seguem alguns exemplos:

- Por que a pessoa não tem seus novos acessos automaticamente assinalados ao ganhar uma nova função de negócios?
- Da mesma forma, por que seus acessos anteriores não são automaticamente removidos?
- Eu gostaria de solicitar meus acessos pela intranet. Mas não me venha com aquela sopa de letrinhas ou termos de TI que não consigo entender! Quero solicitar algo como “Consulta a Clientes Região Sul” ou “Pedidos de itens de escritório” ou “Consulta a indicadores de mercado” (sim, perfis!)
- Quero lançar um novo produto. Quais colaboradores deveriam ganhar acesso às opções de vendas desde produto?
- Há alta rotatividade de meu pessoal de atendimento. Quero que os acessos sejam “rotacionados” pelo mesmo mecanismo.

Ainda há o desafio dos novos atores do espetáculo das organizações: prestadores de serviço, parceiros de negócios, externos e - nem se imaginava! – os clientes. O cliente tem compra um determinado tipo de produto e pode vir a comprar outro e deixar de comprar outro, e assim por diante. O cliente possui também um perfil de acesso que deve ser modelado, auditado, revisto, validado.

Bem, enfim, agora ganhamos um grande barco (ou navio!) para navegar no mar de privilégios. Vamos navegar!