

## Perfis por Função em Sistemas Corporativos

Maio de 2008

Autor: Rudnei Guimarães, Consultor Sênior da Order



## Resumo

A implantação e utilização de Perfis por Função é uma prática recomendada pelos órgãos reguladores e normas internacionais. Eles permitem prover os privilégios de acessos aos sistemas corporativos estritamente necessários para os colaboradores desempenharem suas atividades. A criação e manutenção dos Perfis por Função em ambientes corporativos efetuadas por processos manuais podem não acompanhar o dinamismo da corporação. A adoção de sistemas de Gerenciamento de Identidade Corporativa automatizou toda a administração da concessão de acessos e devem estar em sintonia com os Perfis por Função. Diante destes desafios, será apresentado o resultado de um trabalho efetuado utilizando o Eureka Sage como ferramenta de apoio para a criação, administração, revisão e conformidade dos Perfis por Função.

## Introdução

O Perfil por Função (ou *RBAC – Role Based Access Control*) é um projeto do *National Institute of Standard and Technology* (NIST), que tem por objetivo criar um modelo para prover e administrar privilégios de acesso em uma organização.

Sugestão: é um conceito sobre práticas de controle de acesso que originou nos anos 70 e se desenvolveu até ter sua primeira proposta de padrão em 2004 pelo NIST.

O Perfil por Função é o controle de acesso baseado no papel, na atividade ou na função que o colaborador exerce dentro da organização. Vários sistemas corporativos modernos possuem algum modelo de Perfil por Função. Por exemplo:

- SAP são as *profiles*;
- Microsoft AD são os grupos;
- RACF são os domínios e grupos;
- CA Top Secret são as *profiles*;
- Oracle são as *roles*;

- BMC Control-SA são as *profiles*;
- IBM TIM são as *profiles*;
- Novell Identity Manager são as *roles*.

O Perfil por Função agrega os acessos, possibilitando ter uma visão do privilégio de acesso de forma corporativa e não mais por sistema; incorpora a hierarquia organizacional e segregação de funções dentro do seu modelo. A segregação de funções proíbe o usuário de, exercendo certa atividade, executar outra atividade ao mesmo tempo que implique em risco operacional para o negócio. A hierarquia organizacional reflete a estrutura dos papéis desempenhados pelos colaboradores dentro da organização.

Várias normas e regulamentos governamentais, como Sarbanes-Oxley (SOX), COBIT, ISO/IEC 17799, recomendam a implementação de controles, como o Perfil por Função, como forma de seguir as políticas de acesso.

O trabalho desenvolvido foi executado em um sistema proprietário, contendo Perfis por Função, seus privilégios de acesso e os usuários a eles conectados. Englobou:

- O planejamento das atividades;
- A revisão dos privilégios de acesso atual;
- A certificação dos privilégios de acesso pelos responsáveis;
- A verificação se os privilégios de acesso revisados estão em conformidade com as normas da organização;
- A proposição de novos perfis por função;
- A verificação se os perfis por função propostos estão em conformidade com as normas da organização;
- A integração com a ferramenta de Identity Management (IdM) utilizada pela corporação.

Este sistema proprietário é a principal “porta de entrada” da plataforma de negócios, sendo utilizada pelos colaboradores que atendem os clientes da empresa e continha inicialmente 292 Perfis por Função. Ele controla os acessos a 152 plataformas de negócio.

O principal objetivo do trabalho foi reorganizar os privilégios de acesso em novos Perfis por Função.

## Planejamento das Atividades

A seguinte metodologia foi utilizada para desenvolver o trabalho:

- Obtenção de Dados:
  - RH: definição e obtenção de dados essenciais dos usuários (como Status, lotação, cargo, etc);
  - Regras de Negócio: obtenção das regras de negócio dos privilégios de acesso, normas, regulamentos e segregação de função, utilizadas na organização;
  - Levantamento das atividades: entendimentos de como os serviços são desempenhados pelos colaboradores;
  - Importação e tratamento das Bases Autoritativas: manipulação dos dados do formato proprietário da base autoritativa para o formato Sage e saneamento dos dados;
- Campanhas de certificação: foram criadas campanhas para envolver os responsáveis e solicitar a revisão de certificação dos privilégios de acesso atuais;
- Prospecção de novos Perfis por Função: após o saneamento e certificação, propor nova organização dos Perfis por Função;
- Certificação dos Perfis por Função: avaliar junto com o gestor do Negócio e a área de Segurança da Informação, os Perfis por Função e os privilégios de acesso propostos.

Um dos desafios na engenharia de Perfis por Função é encontrar o nível correto de granularidade que permita controle e que, ao mesmo tempo, não resulte em excesso ou falta de privilégios de acesso. Para efetuar o ajuste fino e encontrar o ponto de equilíbrio entre Perfis por Função e excesso/falta de privilégios, foram utilizados os seguintes critérios:

- Sobreposição de usuários em mais de um Perfil por Função: 0%;

- Número mínimo de privilégios de acesso: média dos privilégios de acesso;
- Fusão de perfis por Função:
  - 100% dos usuários devem ser iguais ou;
  - No mínimo 90% dos privilégios de acesso devem ser iguais ou;
  - Usuários devem ser da mesma área de negócio e no mínimo 80% dos privilégios de acesso devem ser iguais.

## Revisão dos Privilégios de Acesso Atuais

Após a fase de obtenção de dados, já se pode obter os primeiros resultados:

- Usuários inativos: ao cruzar os usuários do sistema com os dados obtidos do RH, identificou-se que 23% dos usuários já tinham sido desligados da empresa;
- Responsáveis pelo Perfil por Função que não estão em conformidade com os regulamentos: 0,55%;
- Perfis por Função inativos: 23% dos Perfis por Função não eram utilizados por ninguém, sendo que um Perfil por Função não tinha nem privilégio de acesso;
- Perfis por Função iguais: 6% dos Perfis por Função possuíam exatamente os mesmos privilégios de acesso;
- Privilégios de acesso inativos: 26,7% dos privilégios de acesso cadastrados não eram utilizados. Foi identificado de imediato que a funcionalidade provida por 1 privilégio de acesso, apesar de cadastrado, não existia mais;
- Privilégios de acesso com a mesma descrição: 7% dos privilégios de acesso possuíam a mesma descrição, porém com funcionalidades diferentes. Destes, dois privilégios de acesso não tinham descrição.

Adicionalmente, foi identificada a taxa de utilização de cada privilégio de acesso do usuário, provido pelo Perfil por Função. Esta taxa de utilização auxiliou o responsável na certificação do privilégio de acesso.

## **Certificação de Privilégios de Acesso pelos Responsáveis**

Um dos principais desafios na certificação de privilégios de acesso é envolver o responsável pelo Perfil por Função de tal modo que ele possa entender que esta atividade é importante para o desempenho das atividades dos usuários com mais qualidade e segurança.

Para que o principal objetivo do trabalho fosse atingido (reorganizar os privilégios de acesso em novos Perfis por Função), uma nova abordagem foi utilizada em relação à tradicional.

Na abordagem tradicional, o responsável verificaria se os usuários e privilégios de acesso deveriam estar conectados àquele Perfil por Função. A abordagem utilizada foi mostrar para o responsável a taxa de utilização de cada privilégio de acesso pelos usuários de seu Perfil por Função. Deste modo, ficava evidente o que era e o que não era utilizado, auxiliando o responsável na certificação do Perfil por Função. Estes dados foram disponibilizados no Sage Portal e foram criadas campanhas de esclarecimento e certificação.

As campanhas de esclarecimentos foram efetuadas por meio de *workshops*, de no máximo 2 horas. Foi fornecido um “kit esclarecimento”, que descrevia passo-a-passo o que o responsável deveria efetuar.

As campanhas de certificação foram efetuadas pelo envio de um *link* individual por e-mail para cada responsável pela certificação pelo Perfil por Função. O link abria uma página Web, a qual possibilitava o responsável identificar os privilégios de acesso a serem certificados. Ele podia aprovar ou reprovar e, neste caso, inserir uma justificativa.

A campanha pelo Sage Portal também possibilitou acompanhar a evolução das certificações dos Perfis por Função pelos responsáveis, lembrando, quando necessário, alguns responsáveis sobre necessidade de efetuar a certificação.

Outra vantagem das campanhas foi efetuar a delegação das certificações de alguns responsáveis que estavam saindo de férias ou tiveram suas atividades transferidas para outras pessoas.

## **Verificação se os Privilégios de Acesso revisados estão em conformidade**

Na fase de certificação de privilégios de acesso, foi dada a liberdade para que os responsáveis pudessem solicitar novos privilégios de acesso.

Após a finalização das campanhas, foram verificadas se as solicitações de novos privilégios de acesso estavam em conformidade com as normas da empresa. Esta verificação foi efetuada utilizando a função do Sage ERM de auditoria e regras de negócios.

## **Proposição de Novos Perfis por Função**

Após a revisão dos privilégios de acesso efetuada pelos responsáveis, a variação dos privilégios de acesso dentro de um mesmo Perfil por Função original variou bastante. Por exemplo, um Perfil por Função que abrangia 21% dos usuários, continha 81 privilégios de acesso. Após a revisão, a solicitação de privilégios de acesso para este Perfil por Função variou de 1 a 81.

Dois Perfis por Função agrupavam 35% do total dos usuários e 53% dos Perfis por Função continham apenas uma pessoa. Ao tentar reorganizar em novos Perfis por Função, o resultado foi a proliferação de novos perfis com pouquíssimos privilégios de acesso (menos que 40) e contendo apenas uma ou duas pessoas. A tentativa de reorganizar em novos perfis por função utilizando o critério do organograma também não obteve um bom resultado. Para estas situações, preferiu-se e manter os privilégios de acesso.

Ao avaliar os privilégios de acesso, identificou-se 19 que privilégios de acessos são utilizados por 94% dos usuários antes da proposição dos perfis por função. Estes 19 privilégios de acesso passaram a formar um Perfil por Função básico do sistema. Após a proposição, estes privilégios

passaram a ser utilizados por 99% dos usuários e por 98% dos perfis por função propostos, sem implicar em excesso de privilégios.

O resultado da prospecção por novos perfis por função foi a seguinte proposta:

- 247 novos perfis por função:
  - 1 Perfil por Função contendo 259 usuários (21,5% total de usuários);
  - 65 Perfis por Função contendo uma pessoa (correspondendo a 26% do total).

## **Verificação se os Perfis por Função propostos estão em conformidade**

Após a proposição dos novos Perfis por Função, foram verificados se os usuários e privilégios de acesso do Perfil por Função estavam em conformidade com as normas da empresa, efetuando-se os ajustes necessários para aqueles que violavam as regras.

## **Integração com a ferramenta de Identity Management**

Desde o início do trabalho, ficou evidente que o Sage deveria ser integrado à ferramenta de IdM, atuando como fonte autoritativa dos Perfis por Função. Após estudos, identificaram-se dois modos de integrar o Sage com a ferramenta da IdM:

- Via *Web Service*, no qual a ferramenta de IdM consultaria o Sage para fornecer os Perfis por Função;
- Via arquivo, no qual os Perfis por Função estavam relacionados com seus privilégios de acesso.

Optou-se por utilizar o Web Service, como forma de obter os Perfis por Função sempre atualizados. A integração por arquivo foi utilizada também, como forma de contingência. Neste caso, os Perfis por Função poderiam ficar desatualizados por até 24hs.

Toda vez que um gestor solicita acesso para um novo colaborador, é mostrado os Perfis por Função disponíveis. O gestor selecionar o Perfil por Função e o IdM trata de efetuar os provisionamentos necessários.

A remoção de um colaborador de um Perfil por Função acarreta em remover os privilégios de acesso do colaborador. Neste caso, o Sage não precisa ser informado.

A modificação de um Perfil por Função no Sage é processada pelo IdM diariamente, sendo que as modificações efetuadas nos Perfis por Função são removidas ou concedidas aos colaboradores automaticamente.

A integração do Sage com a ferramenta de IdM proporcionou implantar o Perfil por Função Corporativo. Este Perfil por Função engloba as principais plataformas tecnológicas da empresa.

## **Conclusão**

O trabalho de revisão dos privilégios de acesso atual e proposição de novos Perfis por Função foi concluído em 2 meses e meio. Ficou evidente que a utilização do Sage como ferramenta de auxílio para a revisão, administração e criação de Perfis por Função economizou tempo e adicionou qualidade ao trabalho. Estimou-se que se todo o trabalho fosse efetuado manualmente (planilhas e desenvolvimento de interfaces para tratamento dos dados) demandaria pelo menos 6 meses.

Pôde-se observar que o saneamento inicial da base autoritativa eliminou vários problemas de segurança e violações às normas, sem impacto para as atividades de negócio providas por este sistema.

A integração do Sage com a ferramenta de IdM proporcionou uma maior agilidade para o gestor do negócio, reduzindo o tempo para início do trabalho de um novo colaborador e proporcionando um melhor controle sobre quem faz o quê. A área de Segurança da Informação passou a ter um controle automatizado dos processos e a Área de Auditoria passou a ter uma ferramenta que já verifica os privilégios de acessos contra as normas da empresa.

Ganhos observados:

- Redução da quantidade de Perfis por Função em 15,4%;
- Redução de 74% dos Perfis por Função utilizados por 1 usuário;
- Redução dos privilégios de acesso em 40% dos usuários;
- Manutenção dos privilégios de acesso em 32% dos usuários;
- Redução de 30% no tempo de concessão de acesso em todos os sistemas necessários para o colaborador começar a trabalhar;
- Redução de 60% no retrabalho da concessão de acesso;
- Diminuição substancial dos excessos de privilégios, comprovados pela redução em 80% de pontos de auditoria dos sistemas gerenciados pelo IdM /Sage.