Cobalto UFPel: Gerenciamento de permissões a partir da relação de chefia

**Cássio S. Carvalho, Diego S. Oliveira,
José Hiram S. Noguez, Rafael T. Santos, Amanda Argou**

[1]Pró-Reitoria de Gestão da Informação e Comunicação
Coordenação de Sistemas de Informação
Universidade Federal de Pelotas - UFPel
Pelotas – RS – Brazil

{cassio.carvalho, diego.oliveira} @ufpel.edu.br

{hiram.noguez, rafael.santos, amanda.argou} @ufpel.edu.br

Abstract. *This article presents a proposed solution for the concession management and access deprivation of Cobalto users - Integrated Information System within the Federal University of Pelotas (UFPel). Among the main motivations for development are: the need for IT independence, hierarchical organization by the nature of the institution and the opportunity to organize data from the implementation of the Electronic Information System (SEI). The proposed solution directly relates the system's functionalities to the units 'heads, which grant and/or withdraw users' access permissions to the features that compete with them, even automatically.*

Resumo. *Este artigo apresenta uma solução proposta para o gerenciamento de concessão e privação de acesso dos usuários do Cobalto - Sistema Integrado de Informações no âmbito da Universidade Federal de Pelotas (UFPel). Dentre as principais motivações para o desenvolvimento, estão: necessidade de independência da TI, organização hierárquica pela natureza da instituição e oportunidade de organização de dados advinda da implantação do Sistema Eletrônico de Informações (SEI). A solução proposta relaciona diretamente as funcionalidades do sistema com chefias das unidades, que concedem e/ou retiram permissões de acesso dos usuários às funcionalidades que lhe competem, inclusive de forma automática.*

1. Introdução

A partir de 2012 a Universidade Federal de Pelotas oficializa o Cobalto como o Sistema Integrado de Gestão, em desenvolvimento na própria instituição até o momento. Desde então, a plataforma vem agregando novas funcionalidades, a fim de atender de forma unificada e padronizada a gestão acadêmica e administrativa institucional [Cobalto].

Dentre os desafios inerentes ao desenvolvimento e gerenciamento de sistemas integrados, está o controle de acesso dos seus usuários. Geralmente, os sistemas informatizados contém módulos de gerenciamento de permissões de acesso dos usuários como um todo, mais especificamente, de suas funcionalidades. Dessa forma, tem-se grupos de

usuários com características análogas, que acabam necessitando de acessos à funcionalidades semelhantes, de acordo com a unidade em que trabalham e com o tipo de serviço que lhes compete.

Um dos problemas desse gerenciamento acaba extrapolando as questões relacionadas ao software propriamente dito. As questões que surgem começam por quem deve fazer a liberação dos acessos (onde incluem-se as restrições de dados, unidades, etc.) e como registrar tais solicitações, como forma de apurar os responsáveis. Nesse caminho surge outra situação comum: o usuário que ganhou certa permissão (concessão) pode ter que perdê-la (privação) em algum momento.

Diante desse cenário, com a procura de alternativas automatizadas para amenizar essas ocorrências e buscando facilitar o gerenciamento sobre os usuários, implementou-se no sistema Cobalto UFPel um gerenciamento de permissões a partir da relação de chefia, afastando essa responsabilidade da equipe de TI.

2. Métodos

No Cobalto a gestão de permissões opera basicamente da seguinte forma:

Grupos de acesso - englobam programas e restrições de acesso às funções destes. Para a definição dos grupos procura-se analisar nos setores os diferentes perfis de uso que serão necessários. Relaciona-se os usuários desse setor aos grupos que lhes competem, como por exemplo, o perfil de coordenador de curso.

Restrição de dados - em alguns casos os programas podem ser disponibilizados para diferentes unidades ou cursos. Nessas situações, o que diferencia o acesso de um usuário para o outro é o tipo de restrição que ele possui, por exemplo: um coordenador terá restrição no Curso A e outro coordenador no curso B. Ambos terão acesso aos mesmos programas, porém gerindo informações diferentes.

Existem alguns grupos de acesso pré-definidos, ou pode-se chamar de "perfil" de usuário, que são automaticamente atribuídos às pessoas. Dessa forma, quando uma pessoa é inserida nos cadastros, o sistema detecta qual seu tipo e assim atribui determinados grupos e funcionalidades automaticamente. Como exemplo, uma pessoa que é aluno receberá o perfil "Alunos". No caso da pessoa ser um servidor, receberá o perfil "Servidor". Consequentemente, quando a pessoa enquadra-se em mais de um perfil, acaba por receber todos eles. Esse perfil possui um conjunto de funcionalidades previamente relacionadas e que são minimamente imprescindíveis para cada tipo de pessoa.

Por outro lado, na UFPel, para ganhar alguma funcionalidade específica de acesso é necessário algum tipo de solicitação. Em contrapartida, para que essas funcionalidades sejam retiradas do usuário, via de regra, essa notificação nunca ocorre. Assim, servidores que possuem acesso a determinada funcionalidade no sistema e acabam por trocar de unidade (absorvendo novas funções), geralmente não tem suas permissões retiradas do sistema, pois esta troca não é comunicada aos responsáveis pela administração de permissões.

Dentro desse cenário, é necessária a intervenção de pessoas da TI habilitadas para esse controle, bem como em alguns poucos aspectos, da Coordenação de Registros Acadêmicos, para manter o cadastro de permissões atualizado.

Com a recente implantação do SEI [TRF4], o cadastro de unidades e chefias da UFPel está sendo permanentemente atualizado no Cobalto, o que permitiu evoluir a gestão de permissões já implantada. Dessa maneira, se propôs vincular grupos de acesso a tipos de chefias e unidades da instituição, com uma ação pró-ativa e automática de concessão de permissões. A Figura 1 abaixo apresenta a tela onde o cadastro das chefias é gerenciado no Cobalto.

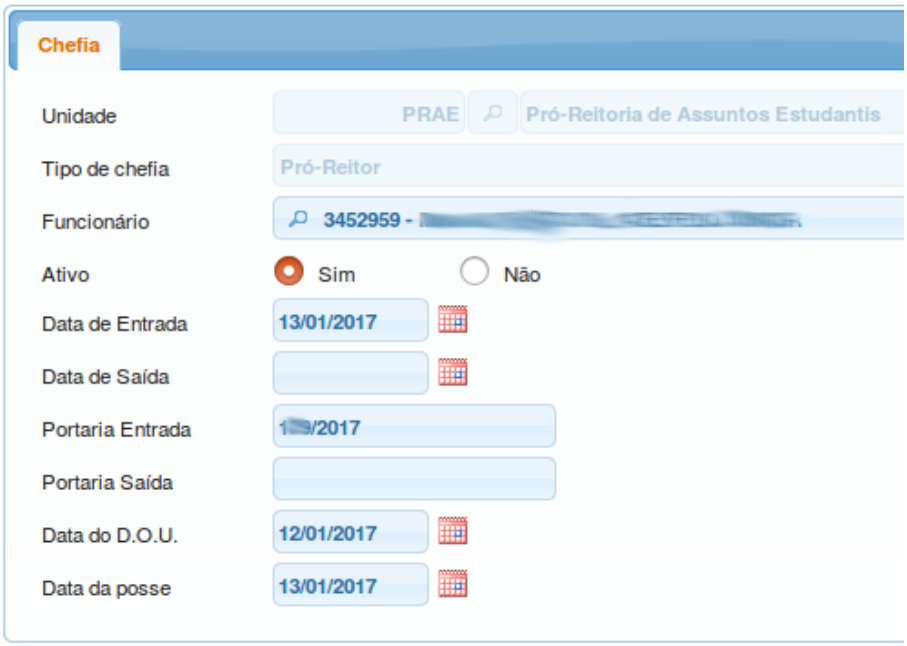

Figura 1. Cadastro de chefias

Na Figura 2 verifica-se que alguns grupos de acesso foram associados ao tipo de chefia "Pró-Reitor". Como parâmetro unidade não foi informado, então isso significa que qualquer Pró-Reitor (independente de unidade), receberá automaticamente os respectivos grupos de acesso. Dentre estes, o grupo 'Conceder acesso', o qual permite que a chefia possa repassar as funcionalidades para outros usuários. Dessa maneira, fica ao cargo da chefia o controle de acesso às funcionalidades do sistema que lhe foram atribuídas, conforme a Figura 3.

De uma maneira geral, quando uma pessoa é cadastrada no módulo de chefias ela recebe automaticamente acessos específicos à funcionalidades do sistema Cobalto pré-definidas. Nesse momento a pessoa já adquire permissão de conceder (ou repassar) o que possui a quem desejar, o grupo chamado "Conceder Acesso". Dessa forma, aquele que era o chefe anterior acaba perdendo suas permissões e funcionalidades.

Também na troca de chefia, todas as pessoas que receberam as permissões da chefia anterior acabarão por perdê-las automaticamente. Isso força uma reorganização da unidade de acordo com as percepções do novo responsável. Outro aspecto importante nesta implementação, foi o atendimento a uma recomendação de auditoria interna, a qual referiu-se às formas como o sistema Cobalto atribuía e retirava as permissões dos usuários.

Figura 2. Cadastro tipos de chefia x grupos de acesso

Figura 3. Tela de concessão de acesso da chefia

3. Resultados

Esta forma de administrar permissões está sendo implementada de forma gradual. Já verificou-se que, se uma chefia passa para alguém a permissão de "Conceder Acesso", essa pessoa, possuindo esse recurso, poderia também ir repassando funcionalidades. Isso poderia acarretar uma falta de controle e uso indiscriminado do sistema. Para contornar, foi estabelecido e alterado para que o grupo "Conceder Acesso" não possa ser repassado por quem o possui.

No momento, avaliações estão sendo feitas com a intenção de melhorar o recurso. Uma discussão atual é se a chefia pode conceder permissões a qualquer servidor ou somente aqueles que respeitam a relação organograma e hierarquia de chefias.

4. Conclusões

Mesmo que um sistema possua bons recursos para administração de usuários, essa tarefa sempre requer um envolvimento de pessoas para gerir de forma eficiente os acessos e permissões. Quando se fala de uma instituição com cerca de 2800 servidores e mais de 100 cursos, esse controle requer ainda mais atenção e responsabilidade.

Com a solução adotada, pretende-se: (i) agregar confiabildade e agilidade no processo de concessão e privação de acesso, (ii) aliviar a equipe da TI da tarefa de administrar as permissões específicas dos usuários, o que requer tempo (disponibilidade) e responsabilidade. Entende-se que a proposta de utilizar diretamente o cadastro de chefias como base para a concessão e exclusão de privilégios foi uma escolha acertada, pois as responsabilidades são divididas com os usuários que possuem hierarquia superior na instituição. Estas pessoas, ao invés de solicitarem acesso, possuem total autonomia para isso. E o ponto mais importante: quando uma chefia é destituída todas as suas permissões são perdidas, bem como aquelas que foram por ela concedidas.

Referências

Cobalto. Cobalto UFPel - Sistema Unificado de Gestão. `https://cobalto.ufpel.edu.br/`. Acesso em: 2018-04-23.

TRF4. SEI Sistema Eletrônico de Informações. `https://softwarepublico.gov.br/social/sei`. Acesso em: 2018-04-23.