



SEGURANÇA DA INFORMAÇÃO – SEGREGAÇÃO DE FUNÇÃO

Ana Caroline Zavatta¹
Juliano Shimiguel²

RESUMO

Este trabalho tem como objetivo descrever a utilização de Segregação de Função dentro de uma organização, identificando as principais características de segurança (tendo como base o ERP SAP) e propondo uma nova estrutura técnica de acesso dentro de uma área específica de uma empresa; contendo exemplificações e modelos de implantação.

Palavras-chave: Segurança da Informação, Segregação, Risco.

ABSTRACT

This task describes the utilization of functions segregation in the company, identifying the main security feature (based on ERP SAP) and proposing a new technical structure for accessing inside the specific department of the organization; containing exemplification and implantation exemples.

Keywords: Information security, Segregation, Risk.

¹ Sistemas de Informação

² Doutorado e Mestrado em Ciência da Computação pelo Instituto de Computação da Unicamp.

Professor dos cursos de Sistemas de Informação Analise de Sistemas e Engenharia de Produção do Centro Universitário Padre Anchieta.

1.INTRODUÇÃO

Podemos dizer que hoje a Informação é um dos bens mais valiosos, se não o mais valioso. Ela está inserida em todos os aspectos da vida moderna, seja para fins lucrativos ou de uso pessoal. Quanto mais utilizamos a informação, mais ela cresce, tornando-se cada vez mais essencial. Com tantos meios, ferramentas e possibilidades de acesso à informação surgiu também a preocupação em como manter a segurança desta. Assim, como houve a evolução das informações, houve também a necessidade de ampliar as técnicas de segurança, que se tornam continuamente ultrapassadas. Neste processo, uma dessas técnicas que foram aprimoradas conforme as novas necessidades dos cenários atuais das organizações foi a Segregação de Função.

A Segregação de Função consiste na separação de atribuições potencialmente conflitantes, tais como autorização, aprovação, execução, controle e contabilização das operações. Em face prática, seria a execução de boas práticas que poderão ser avaliadas posteriormente por algum órgão auditor. Tendo em vista o aspecto funcional de uma organização empresarial é altamente perigoso que um colaborador tenha acesso a uma solicitação de reembolso e ao mesmo tempo, tenha acesso para fazer essa aprovação dentro do sistema. As possibilidades de fraudes são enormes.

Aderindo às especificações da Segregação de Função, teremos uma diminuição significativa de riscos como este. Segundo citação do autor Gil (no ano 2000), para que haja a segurança mútua dentro de uma organização, é necessária uma sinergia constituída pelos gestores, usuários e os analistas de Tecnologia da Informação. Na visão do executivo, segundo publicado no site IT FORUM (ano 2015), as principais razões para a evolução da governança da segurança da informação é que as discussões sobre o tema estão extrapolando a TI, quebrando a antiga mentalidade de que a proteção corporativa é responsabilidade única e exclusivamente da tecnologia da informação. Segundo publicação da revista DomTotal (ano 2011), vivemos na Era da Informação ou seja, conceitos antes conhecidos anteriormente por nós podem não ser mais a melhor escolha para os dias atuais.

Hoje os usuários do sistema SAP da empresa o qual desenvolvemos o estudo prático deste trabalho, possuem um único perfil constituído de transações que são as responsáveis pelas autorizações que os usuários possuem no sistema. Nossa idéia é atuar justamente em cima dos perfis. Assim, definiremos padrões de segurança preestabelecidos pela área de controles internos e por uma empresa de auditoria contratada pelo grupo.

O princípio da segregação de funções decorre do princípio da moralidade (art. 37, da CF/88), e consiste na necessidade de a Administração repartir funções entre os agentes públicos cuidando para que esses indivíduos não exerçam atividades incompatíveis umas com as outras, especialmente aquelas que envolvam a prática de atos e, posteriormente, a fiscalização desses mesmos atos. Tendo o cenário de uma organização como um todo, a utilização da Segregação de Função torna-se essencial para administração de segurança dos sistemas. Exemplo: não seria interessante para uma empresa, descobrir através de auditorias que um determinado colaborador pode solicitar valores de reembolso para sua conta bancária e que ele mesmo tem acesso a realizar essa aprovação dentro do sistema. Visando assegurar a própria segurança da empresa é de mera importância a realização de rotinas que assegurem a efetivação dos processos que foram estabelecidos anteriormente. Conforme trabalho de conclusão de curso publicado pelo então aluno Fabricio de Jesus de Lima, titulado como “Estudo de melhorias em segurança da informação”, a segregação das funções é citada como um dos principais tópicos para que a Segurança das Operações empresarias sejam garantidas.

Este trabalho tem como objetivo descrever a utilização de Segregação de Função dentro de uma organização, identificando as principais características de segurança (tendo como base o ERP SAP) e propondo uma nova estrutura técnica de acesso dentro de uma área específica de uma empresa. Podendo também: exemplificar como é feita e aplicação da segurança, farão com que o leitor possa entender não só da parte processual como também da parte técnica e operacional; Realizar a implantação da Segregação de Função agregando valores à organização; Investigar possíveis conflitos de segregação de função; Pesquisar sobre técnicas anteriormente já implantadas visando a segurança e aperfeiçoamento da organização.

Este projeto está dividido em cinco partes: referencial Teórico: onde teremos o conceito de segregação de função, histórico, pilares da segurança da informação,

seus pontos positivos e negativos; Metodologia: onde há uma especificação do que precisaremos utilizar para implementar a técnica; Estudo de caso: teremos um cenário como modelo para aplicar a técnica, mostrando resultados anteriores e posteriores; Considerações finais: onde será abordada uma análise geral do projeto implantado; Referência: neste capítulo será descrita toda e quais fonte utilizada para elaboração deste trabalho.

2.REFERENCIAL TEÓRICO

2.1 Conceito de Segregação de Funções

Segundo fonte do dicionário Michaelis, Segregar significa: afastar, apartar, isolar, separar. E o conceito de função pode ser descrito do tópico números dois das definições citadas pelo dicionário, como: atividade especial, serviço, encargo, cargo, emprego, missão.

Conforme livro da ABNT NBR ISSO/IEC 17799:2005, o Controle convém que funções e áreas de responsabilidades sejam segregadas para reduzir as oportunidades de modificações ou uso indevido não autorizado ou não intencional dos ativos da organização.

Diretrizes para implementação: A segregação de funções é um método para redução do risco de uso indevido accidental ou deliberado dos sistemas. Convém que sejam tomados certos cuidados para impedir que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção. Convém que o início de um evento seja separado de sua autorização. Convém que a possibilidade de existência de conluios seja considerada no projeto dos controles. As pequenas organizações podem considerar a segregação de funções difícil de ser implantada, mas convém que o seu princípio seja aplicado sempre que possível e praticável. Onde for difícil a segregação, convém que outros controles, como a monitoração das atividades, trilhas de auditoria e o acompanhamento gerencial, sejam considerados. É importante que a auditoria da segurança permaneça como uma atividade independente.

(livro da ABNT NBR ISSO/IEC 17799:2005, 2005, página 41)

Com base no trecho citado acima, podemos concluir que a prática de segregar as funções dentro das organizações hoje, é muito válido. Assim garantimos que os processos atuais estão sendo executados da forma mais segura e transparente possível.

A prática de segregar consiste nada mais do que “separar” as funções dentro de uma organização. Dependendo do cenário, sua implantação pode ser demorada. Porém, se concluída corretamente, o sucesso – visando a segurança – será certo.

Um dos pontos citados no trecho acima, refere-se à dificuldade das pequenas empresas em implementar a segregação de função. Isso ocorre porque para que seja separa um processo por inteiro, necessita-se (na maior parte das vezes) de mais pessoal. Ou seja, o que antes precisava de apenas dois colaboradores para

ser executado, hoje, com a visão da segregação de função, necessita de quatro pessoas. Muitas vezes isso se torna inviável para organização, tendo em vista que não será possível contratar mais pessoas para que se atenda às normas de segurança. Então, a melhor solução que se vê é aceitar o risco. Nada mais é que um “de acordo” do responsável do departamento. Esse documento pode ser impresso ou eletrônico. É importante apenas que fique claro o reconhecimento e aceitação do risco pela gestão funcional.

O conceito de segregação é usado em uma tese publicada na faculdade USP, dentro do tópico chamado de “Princípios fundamentais de segurança”, feita pelo então aluno Richard Silva, ano 2010.

Após a implantação ser realizada, é importante que sejam realizadas rotinas constantes para verificar se o cenário proposto/implantado inicialmente está sendo cumprido. Esse é um ponto que deve ser analisado com maior cautela pela área de segurança. Exemplo: o surgimento de uma nova área pode necessitar da criação de um novo perfil específico para atendê-los, sendo assim a análise de segregação de função também deve ser aplicada em cima do novo pacote de acessos; verificando-se assim se não haverá aumento de riscos na área anteriormente já analisada. Toda e qualquer mudança nos perfis já revisados, deve ser realizada com cautela, pois qualquer inclusão de permissão nos processos podem resultar em um novo conflito de função.

2.2 Novas necessidades em Segurança da Informação

Atualmente não há registros específicos de quando começaram a ser utilizadas as práticas de segregação de função. Até mesmo porque, entendemos que essa prática veio sendo adotada e aprimorada conforme o crescimento de utilização da informação e suas técnicas de segurança.

Conforme dito no livro CISSP (ano 2013) pela autora Shon reconhecida como uma das 25 mulheres com maior domínio no assunto Segurança da Informação do mundo, computadores e os dados tratados por eles, normalmente tem uma relação direta com as missões e objetivos críticos de uma empresa.

Devido a esta importância, a alta gestão deve olhar de forma atenciosa para itens de alta prioridade. Prestando apoio, recursos e tempo para garantir que os sistemas e suas informações sejam protegidos de forma mais lógica e eficaz em termos de custos.

Essa análise deve ser feita de forma geral dentro de uma organização, desde a gestão sênior até o nível mais baixo, conforme a hierarquia da constituição em questão. Isso ocorre porque todos dentro de uma organização podem ter uma diferente visão de valores e experiências pessoais, que trazem de forma direta ou indireta para o ambiente de trabalho no se diz respeito para a segurança. Podemos citar como exemplo, uma colaboradora que entrou recentemente no grupo corporativo de uma determinada empresa. Na empresa que ela trabalhou anteriormente, possuía acesso à todos os demonstrativos financeiros, pois nesse antigo ambiente, realmente não havia a preocupação com a disponibilidade de informações. Mas agora na nova empresa essa preocupação e restrição existem. Caso não tivesse sido empregada anteriormente, ela tivesse consultado todos os dados, simplesmente por não saber que não podia. Por isso é importante analisar toda função como particular, em matéria de segurança a um nível que atenda as necessidades da organização, conforme determinado por leis, regulamentos, requisitos e objetivos de negócio que foram determinados por avaliações de risco no ambiente da organização, para que assim possamos estabelecer um padrão entre as atividades exercidas para cada área, independente da pessoa que ocupe a vaga de colaborador dentro da instituição.

Para obtermos sucesso em um plano de segurança de uma empresa, ele deve começar no nível mais alto e ser útil e funcional em todos os níveis abaixo dela. A gerência sênior precisa definir o âmbito da segurança, identificar e decidir o que deve ser protegido e em que medida. Compreendendo também os regulamentos, leis e questões de responsabilidade. É responsável por cumprir em matéria de segurança e garantir que a empresa como um todo cumpre com suas obrigações, definindo também o que se espera dos seus empregados e quais as conseqüências de não cumpri-las.

“Um programa de segurança contém todas as peças necessárias para proporcionar uma proteção global para uma corporação e estabelece uma estratégia de segurança a longo prazo.”

(Harris, ano 2013, pág 127)

É indispensável que questões tais como: idioma, nível de detalhe, formalidade nos documentos e mecanismos de apoio devam ser previamente analisados e escolhidos com cuidado. Tendo em vista o público alvo, o documento deve ter em

vista ser o mais realista e eficaz possível para bons resultados dentro de uma organização. Quanto mais detalhadas são as especificações, mais fácil saber quando uma for violada. Contudo, documentação excessiva e regras detalhadas podem revelar-se mais onerosa do que útil. A análise do tipo de negócio, sua cultura e seus objetivos também devem ser avaliados.

2.3 Pilares da Segurança da Informação

Conforme citado pelo especialista em Segurança da Informação Feleol (ano 2012), hoje a segurança da informação é constituída por três pilares fundamentais: confidencialidade, integridade e disponibilidade. O interessante, é que para que as três bases funcionem de forma correta, é indispensável a aplicação da segregação de função.

Vemos uma ligação direta dos três pontos citados com a técnica de segurança em questão. Vejamos:

Confidencialidade é a garantia de que apenas pessoas autorizadas poderão ter acesso a determinadas informações. Como a segregação de função estuda, molda e aplica exatamente o que cada colaborador exercerá dentro da organização, ficará mais fácil saber qual a melhor maneira de disponibilizar (ou não) determinadas informações.

Integridade é a salvaguarda da exatidão da informação e dos métodos de processamento. Ou seja, se as informações forem disponibilizadas de forma correta para as pessoas que realmente sabem utilizá-las o risco dos dados serem apagados ou até mesmo corrompidos será reduzido.

Disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário. Ou seja, quando moldado de forma correta o que cada colaborador poderá acessar, sabemos que não haverá o risco de identificar uma “falta de autorização” inesperada pelo sistema. Os testes refletem de forma significativa nesse ponto, pois de nada adianta não identificar essas possíveis faltas de autorizações em fases de testes e correr o risco de simplesmente atrasar para um fechamento financeiro.

O conceito utilizado como “pilares”, não foi por acaso. É importante que seja realmente assimilado a imagem de pilares para sustentar a Segurança da

Informação. Para melhor entendimento, disponibilizamos a imagem abaixo. Onde podemos observar os três itens citados acima:



Figura 1 - Pilares da Segurança da Informação – Fonte: <http://segtenca.blogspot.com.br/2009/08/definicao-da-seguranca-da-informacao.html>

A aplicação de segregação de função pode fazer a grande diferença quando estamos falando dos Pilares de Segurança da Informação. Tendo em vista que a integridade das informações estará segura, pois apenas pessoas preparadas poderão ter acesso a elas. A confidencialidade também estará protegida, pois se houver um bom desenho dos acessos que todos deverão ter acesso, apenas pessoas autorizadas estarão com acesso a essas informações. Em relação à disponibilidade também não será diferente, pois se for disponibilizada de forma correta para quem deverá ter acesso, elas estarão disponíveis a qualquer momento que forem solicitadas.

Um ponto que precisa um pouco mais de atenção refere-se ao fato de que poderão ocorrer situações onde apenas um grupo de pessoas poderá resolver um determinado incidente. Exemplo: sem a prática de segregar, muitas pessoas podem ter acesso a muitas atividades dentro do sistema. Assim, qualquer uma delas terá acesso a fazer alguma correção no sistema se necessário. Já aplicando a técnica, isso provavelmente não será possível, tendo que recorrer primeiramente à área responsável para correção dos dados no sistema.

3.METODOLOGIA

3.1Tecnologia Utilizada

Tendo com método para o desenvolvimento de estudo uma revisão de literatura com levantamentos utilizando como foco os princípios básicos sobre o que é segurança da informação, como aplicá-la e administrá-la.

Para que seja possível o início da reestruturação de uma determinada área dentro de uma organização aplicando-se a técnica de segurança de segregação de função, é que tenhamos traçadas todas atividades que em conjunto com outras sejam conflitantes. Essa relação é fornecida por empresas especializadas em auditorias e controles internos de segurança. Nada mais são, que atividades possivelmente realizadas dentro da empresa traduzidas como transações. Transações essas, que os funcionários utilizam durante seu trabalho para inserção, modificação, exclusão ou apenas consulta de dados dentro do ERP utilizado pela organização.

Abaixo segue exemplo de uma das análises de riscos identificadas. Podemos observar que se trata de um processo de negócio de compras e que seu risco global é alto. Na linha de conflito avaliado, temos sua descrição: Liberar pedido de compra x Executar pagamento. Na tabela “Impacto”, podemos ver quais riscos serão possíveis caso haja esse conflito disponibilizado para algum colaborador.

ANÁLISE DE RISCO - MATRIZ DE CONFLITO DE ACESSO	
Processo de Negócio:	<u>Compras</u>
Conflito Avaliado:	<u>Liberar pedido de compra x Executar pagamento</u>
Risco Global:	Alto
Riscos Mapeados	
Atividades executadas em desacordo com as políticas, normas e/ou expectativas do Grupo.	
Liberação de pedido de compra fraudulenta.	
Realizar pagamentos não autorizados.	
Impacto (abrangência das falhas, erros ou fraudes no processo)	
Alto	Comprometer a empresa com compras fraudulentas e iniciar pagamentos para mercadorias e serviços não autorizados.

Figura 2 - Análise de Risco retirada de uma Matriz de Conflito – Fonte: EMPRESA FOCO

Uma matriz de conflito pode variar de acordo com o negócio da empresa. Uns podem ter um maior número de riscos identificados que outros. Neste projeto, essa matriz será convertida para um documento com extensão em Excel; podendo assim ser transportada para o ERP utilizado (SAP).

Tendo em mãos essa matriz de conflito, será feita uma análise das atividades de cada colaborador dentro da área que deverá reestruturada. “Pacotes” de transações serão formados, construindo assim as funções. Após as funções estarem formadas, serão geradas no próprio ERP as análises de conflitos (com base na matriz fornecida anteriormente).

Para que a possibilidade de sucesso na reestruturação seja maior, é indispensável a presença de um analista técnico da área, também conhecido como usuário chave. Essa pessoa necessita ter um conhecimento maior de todo o processo operacional da área que será analisada. Tomando cuidados, para que não seja esquecida nenhuma parte de acesso que seja fundamental para o cotidiano dos

colaboradores da empresa. Essa presença se faz crucial, pois os analistas de T.I. podem não ter o conhecimento necessário, para fazer as distribuições de acesso dentro da área.

Este trabalho precisará de testes, baseado nos cenários atuais dos usuários da área reestruturada. Para que não haja impacto no trabalho de cada um, deverão ser disponibilizados usuários de testes com as novas funções montadas para cada usuária. Nessa fase contaremos principalmente com os analistas técnicos envolvidos no projeto. Temos como base a área financeira. Sendo assim testes como: movimentações de caixa, encerramento do período financeiro, lançamentos e pagamentos de contas, etc. deverão ser simulados. Os ajustes e reparos deverão ser feitos pela equipe de T.I. É importante após os ajustes, que não se esqueça de analisar a matriz de riscos. Para assim, ter certeza de que a manutenção não influenciou uma decisão anteriormente tomada. Caso seja identificado um novo risco, onde não tenha a possibilidade de mitigá-lo, é indispensável reportar para todos os envolvidos no projeto.

3.2Arquitetura SAP

Neste tópico explicaremos um pouco sobre a arquitetura do sistema SAP para verificação de permissões para cada usuário.

Inicialmente, quando um colaborador tenta acessar qualquer transação válida para o sistema SAP, é feita uma verificação interna no sistema para analisar se tão transação poderá ser executada. Essa decisão tem como princípio, as permissões disponibilizadas para o usuário. Pode-se dizer que essa hierarquia de permissões está subdivida em quatro principais classes, que foram separadas por cores na imagem a seguir. São elas:

- PERFIL - consiste no pacote de transações disponibilizadas para determinada função;
- CLASSE DE OBJETOS – baseia-se basicamente na separação dos módulos do sistema, estão exemplificados na cor rosa;
- OBJETO DE AUTORIZAÇÃO – refere-se ao objeto específico onde será feita a verificação da permissão dos acessos, estão representados na cor verde;

- VALORES DOS OBJETOS DE AUTORIZAÇÃO – consiste no valor no objeto de autorização que está disponibiliza. Exemplo: caso seja necessário o valor 01 para criação de um determinado documento e ele não constar nessa subclasse, a operação não será permitida, estão representados na cor amarela.

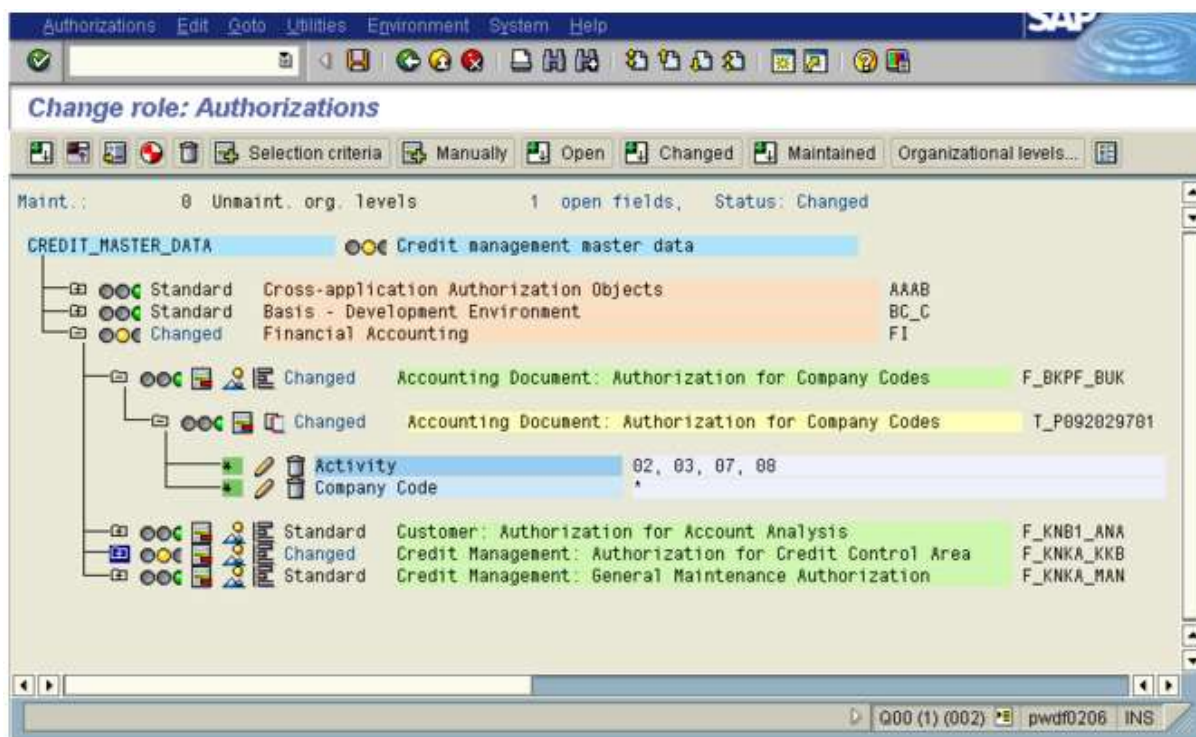
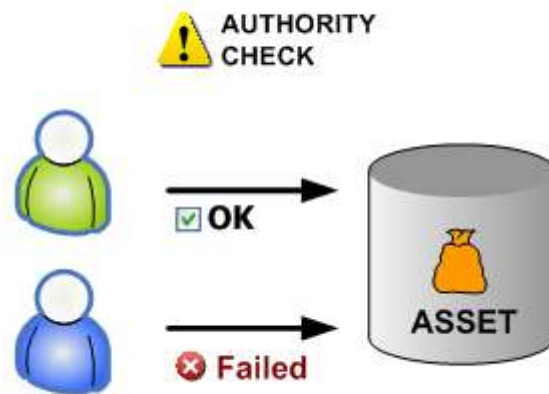


Figura 3 – Exemplo de uma Estrutura de Autorizações – Fonte:

<http://help.sap.com/saphelp_46c/helpdata/en/5c/deaa74d3d411d3970a0000e82de14a/content.htm>

Basicamente então, podemos entender que essa verificação é feita de forma transparente para o usuário final com uma única finalidade: verificar se o valor solicitado pelo usuário final consta em sua tabela de permissões. Caso a resposta seja positiva o acesso será disponibilizado, caso contrário uma mensagem de erro será apresentada.

Roles & Authorizations



© 2010 BIZEC.org - All rights reserved.

Figura 4 – Exemplo de uma Estrutura de Autorizações – Fonte:
<http://www.bizec.org/wiki/Roles_and_Authorizations>

4. ESTUDO DE CASO

Pegaremos como modelo, uma reestruturação de acessos da área Financeira de uma empresa com média de 30 funcionários com usuários ativos, tendo como seu ERP mandante o sistema SAP, aplicando-se a técnica de segregação de funções.

4.1 Principais Passos

Um dos primeiros passos, refere-se a análise de cenário atual. Como estão sendo feitas as atribuições de função dentro da área. Quais são os riscos existentes no cenário atual. Essas informações se tornam importantes, para que seja possível uma comparação de cenários após a finalização do projeto.

Posteriormente deve ser estabelecida uma meta, referente ao prazo de finalização do projeto. Assim distribuições de fases e tarefas poderão ser realizadas.

A modelagem dos perfis e seus testes requerem atenção e tempo, para que o número de falhas ou até mesmo esquecimentos seja o menor possível. O mais indicado é que se tenha reuniões semanais pré-alinhadas. Assim o profissional de T.I. terá seu tempo para criar os perfil e os técnicos operacionais terão tempo para realização dos testes. Em um reunião onde todos estejam presentes, apenas os pontos com falhas poderão ser discutidos. Assim o ganho de tempo e produtividade será maior. Incluir também um profissional da empresa contratada de auditoria também é importante, principalmente no início do projeto onde possivelmente as diretrizes não estejam tão claras.

O período da operação pré-assistida consiste no momento em que as novas funções sejam transportadas para produção mais 30 dias (prazo que poderá ser negociado). Essa operação consiste em pessoas da equipe de T.I. preparados para qualquer atendimento de tempo imediato (ou quase) para ajustes encontrados na operação. Os testes (tópico citado anteriormente) têm reflexo direto nessa fase. Pois melhores tenham sido realizados os testes, menores serão os ajustes pegos pela operação. Tendo em vista de que erros sejam pegos apenas na fase de operação, pode-se identificar falhas no momento de teste. Cenário este, não visto com bons olhos pelos usuários. Tendo em vista que muitas vezes um processo ficará indisponível até que sejam realizados os ajustes necessários.

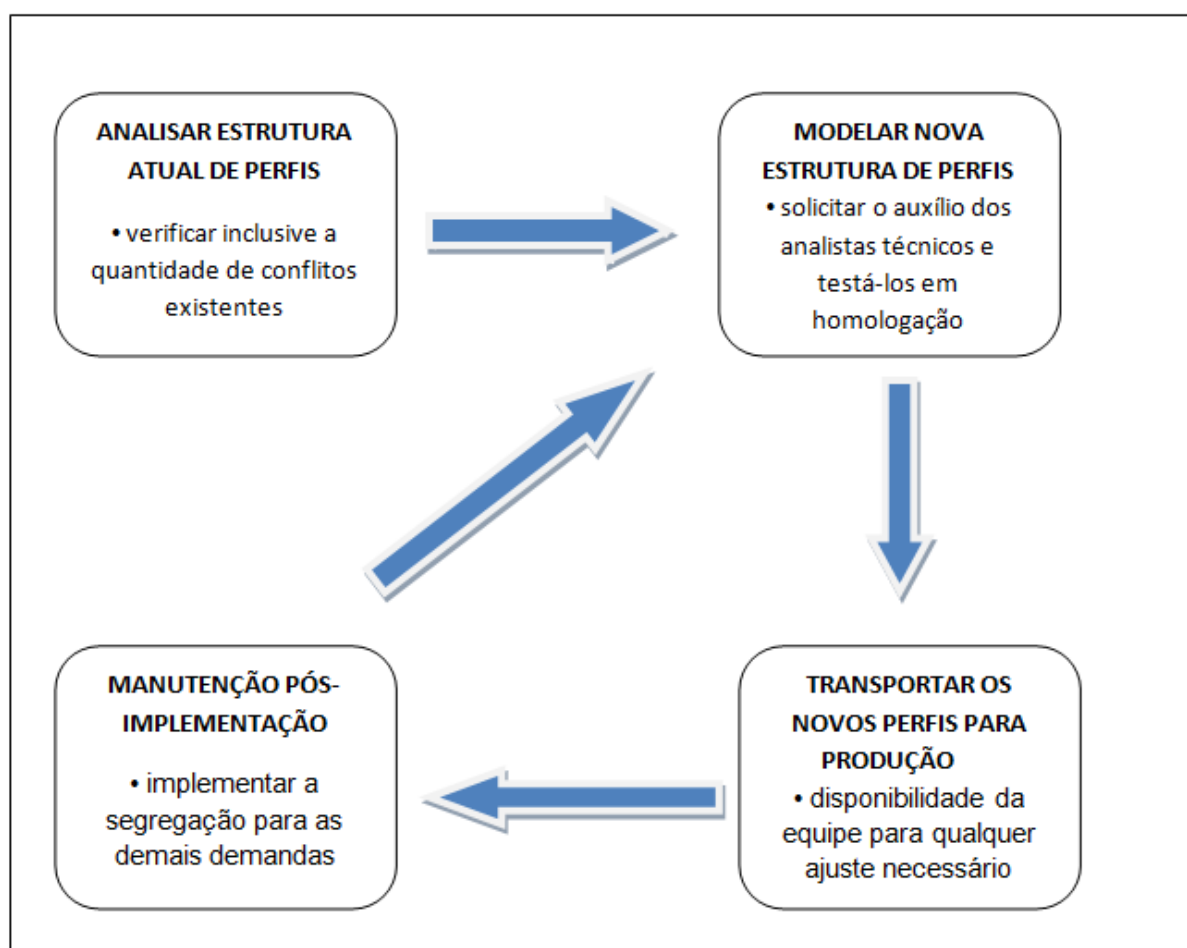


Figura 5 - Fluxograma das Etapas de Segregação de Função – Fonte: EMPRESA FOCO

4.2 Considerações sobre a Segregação de Funções

Segregação de funções, nada mais é do que separar as funções dentro de uma instituição. Através de políticas, normas, linhas de base, orientações e procedimentos, temos a certeza de que todos estão desempenhando exatamente o papel que deveria exercer dentro da organização. A probabilidade de erros maliciosos ou até mesmo erros ignorantes serão mínimos.

Um dos problemas que podemos citar quando estamos falando de segregação de função, refere-se ao fato de ter que lidar diretamente com o que já era costumeiro para os colaboradores. Principalmente quando são pessoas com mais tempo de empresa, que estão acostumadas a exercer inúmeras funções dentro do sistema. Quando é implantada a segregação de função, estamos falando de possivelmente modificar a rotina de determinados departamentos. Para que fique melhor o entendimento, vamos supor que um determinado colaborador antes

conseguisse fazer o inventário, o recebimento físico e o lançamento de um determinado material de estoque. Após ser implantada a segregação de função, possivelmente o usuário desse colaborador tenha acesso apenas a uma dessas atividades. Pois quem faz o inventário de um material, teoricamente não pode ser a mesma pessoa que faz o recebimento do mesmo material, devido ao fato de possíveis alterações em alguma das fases. Isso poderá gerar um pequeno estresse organizacional, pois agora ele dependerá de outras pessoas para dar andamento num processo que anteriormente dependia apenas dele.

Muitas empresas, quando aplicam o método de segurança de segregar as funções percebe que em algumas situações (ou até mesmo em determinadas áreas), não existem pessoas o suficiente para evitar todos os riscos. Ou seja, pode ser que hoje a instituição não possuía uma pessoa para realizar o inventário de um material, uma outra para realizar o recebimento físico e uma terceira para realizar o lançamento do material. Em situações desse tipo, a organização tem a opção de assumir ao risco. Analisando quanto relevante é essa situação para seu tipo de negócio.

4.3 Cenário anterior

Anteriormente tínhamos como cenário um departamento onde basicamente todos funcionários tinham os mesmos acessos no ambiente de produção. Isso ocorreu, porque muitos deles mudaram de função ao passar do tempo e seus acessos não foram revistos... Apenas foram adicionados permissões em seus perfis. Assim, quando uma nova pessoa entrava no departamento e solicitava o mesmo pacote de acessos de um outro colaborador, ele recebia não só os acessos da sua função mas também todos os anteriores daquele funcionário mais antigo. Se observarmos esse cenário, notaremos com facilidade a formação de uma tremenda “bola de acessos”... E com isso, quando juntamos permissões de funções diferentes temos um número alto de riscos no departamento. Pois o mesmo colaborador que dá a entrada de um determinado documento pode realizar todo o seu processo em seguida, fugindo assim dos princípios de segregação de função.

4.4 Proposta de melhorias

Como proposta inicial, iríamos revisar e documentar todos os riscos identificados no departamento estudado, Financeiro. Posteriormente, montaríamos pacotes de acessos para cada colaborador da área, visando é claro, diminuir o número de riscos para cada uma deles. Disponibilizaríamos esses novos perfis de acesso em ambiente de testes, para que pudessem ser validados pelos analistas técnicos que também trabalham no departamento em estudo. Depois de validados, transportaríamos todos os perfis para produção, vinculando cada perfil com seu usuário de acordo com a função de cada um.

4.5 Nova proposta de cenário

Para que facilita e melhore os entendimentos de ambas as partes envolvidas no projeto, diagramas da nova área poderão ser montados. No caso usado como exemplo abaixo, podemos entender como era a pretensão da nova estrutura após implantação da técnica de segurança.

Cada caixa de texto iniciada com “Y:” entende-se como uma função. Nada mais é do que o “pacote” de acesso que será atribuído ao usuário da empresa. Essa função é constituída de transações. Transações essas, que foram analisadas na matriz de conflito conforme dito anteriormente.

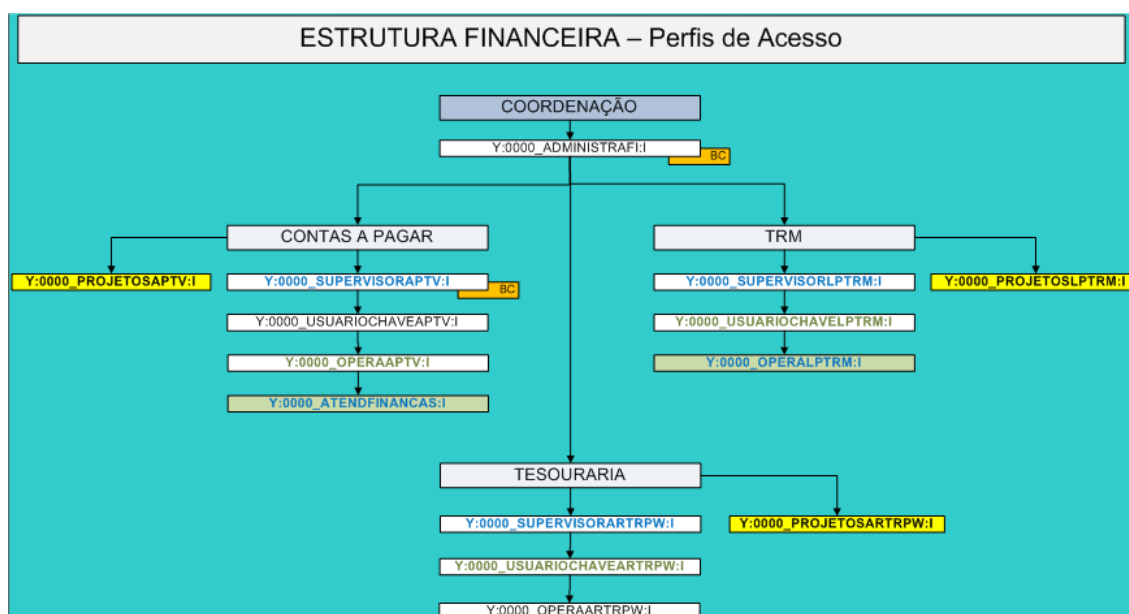


Figura 6 - Fluxograma Perfis de Acesso Área Financeira – Fonte: EMPRESA FOCO

Cada função será analisada de forma individual e processual. Informações tais como: quais transações cada função deverá conter, quem deverá ter este acesso, etc. deverão ser fornecidas e estudadas pela equipe de segurança (T.I.).

A utilização de funções existentes no sistema, como base para criação das novas funções também serão possíveis. Assim, pegaremos um modelo e removemos ou adicionaremos transações nele, não sendo necessária a criação de um perfil “do zero”.

03.12.2014 Saida dinâmica de lista 1

Num.transações selecionadas: 157 PROPOSTO - 107 TRANSAÇÕES

PERFIL	
PERFIL - ESPELHO	Y:0000_USUARIOCHAVETRM:I
NOME DO PERFIL	Y:0000_OPERALPTRM:I

ASSOCIAR COLABORADOR AO PERFIL EXISTENTE

INTEGRANTES		USUARIO
João Maria Silva		XX-3333X

Código de transação	Descrição
ZTRM_FUNDOS_DET	TRM - Relatório de Fundos Detalhado
ZTRM_FUNDOS_DIARIO	TRM - Relatório de Fundos (Diário)
ZTRM_FUNDOS_MENSAL	TRM - Relatório de Fundos (Mensal)
ZTRM_POSCONCEDENTE	TRM - Relatório de Posição Mensal
ZTRM_POS_DERIV_DIA	TRM - Rel. de Derivativos Diário
ZTRM_POS_DIA	TRM - Relatório de Posição Diária
ZTRM_POS_MENSAL	TRM - Relatório de Posição Mensal
ZTRM_MVTDIV_ESCAL	Relatório de Movimentação da Divida Escalonada
ZTRM_MVTDIV_MENSAL	Relatório de Movimentação da Divida Mensal
ZTRM_MVTDIV_DERIV	Relatório de Movimentação da Divida Derivativos
ZTRM_CAD_IND_SENS	Atualização Índices Rel. Sensibilidade

INserir TRANSAÇÃO NO PERFIL

Figura 7 - Modelo de um documento para criação de um perfil – Fonte: EMPRESA FOCO

4.6 Discussão e análise dos resultados

A conclusão do trabalho foi positiva, pois diminuimos o índice de colaboradores com acessos de risco. Para termos certeza do resultado positivo do trabalho, enviamos um questionário de questões relativamente simples para os colaboradores da área funcional em que aplicamos o estudo e um outro questionário para o analistas técnicos da área.

Os resultados dos funcionários operacionais foram os seguintes:

- 95% das pessoas questionadas, disseram que foram avisadas sobre o início do trabalho de revisão dos acessos da área;
- Uma em cada 5 pessoas disseram que notaram diferença depois da técnica ser implantada;
- Tivemos dois registros de pessoas que ficaram sem um acesso que seria indispensável para suas atividades.

Já para análise do ponto de vista dos analistas técnicos:

- Todos os envolvidos no projeto notaram melhoras no processo;

- Eles relataram que a porcentagem de reclamações foi mínima, conseguindo averiguar e contornar todo cenário apresentado;
- Não houve registros, onde tenha sido necessário inserir a gestão para aceitação do novo processo;
- Os analistas disseram que a manutenção de todo o departamento ficou muito mais fácil. Tais como: distribuição de novas tarefas, identificação de processos sendo executados de forma incorreta e atribuição de acessos para os novos funcionários da área.

Quando o projeto for finalizado, uma visão macro poderá ser extraída do sistema. Assim podemos tomar determinadas conclusões do reflexo causado numa reestruturação de uma determinada área como um todo da empresa.

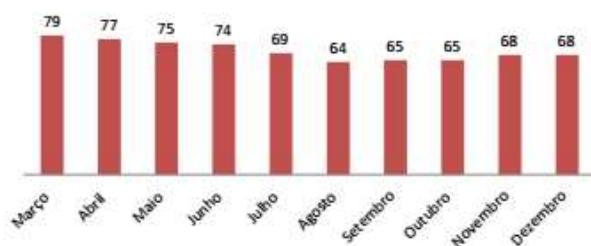
Conforme gráfico abaixo, podemos identificar qual o número de funções com conflitos, quantos usuários com esses conflitos identificados para tomarmos as melhores decisões.

Observe que há uma diferença entre usuários com conflitos e de funções com conflitos. Tendo em vista que funções nesse trabalho podem ser entendidos como um pacote de permissões, tomemos o seguinte exemplo: o perfil de “contas a pagar” é um único pacote que pode conter um conflito. Esse perfil poderá ser replicado para 5 usuários que trabalham nessa atividade... Assim, teremos 5 usuários com conflito e 1 perfil com um conflito.

Acompanhamento da quantidade de conflitos SAP ECC (2014)

Mês	Conflitos x Funções	Conflitos x Usuários	Total de Funções existentes	Funções com conflito	Total de usuários ativos existentes	Usuários com conflito	
Março	398	1924	353	79	1574	426	27%
Abril	360	1704	362	77	1589	294	19%
Maio	346	1736	364	75	1621	290	18%
Junho	325	1213	378	74	1717	288	17%
Julho	306	1355	385	69	1749	291	17%
Agosto	309	1571	392	64	1895	311	16%
Setembro	334	1465	414	65	1959	318	16%
Outubro	319	1461	418	65	1982	329	17%
Novembro	310	1304	426	68	2047	336	16%
Dezembro	296	1377	439	68	2051	339	17%

Quantidade de Funções com conflito (2014)



Quantidade de Usuários com conflito (2014)



Figura 8 - Acompanhamento de quantidade de conflitos SAP ECC – Fonte: EMPRESA FOCO

5. CONSIDERAÇÃO FINAIS

Através do trabalho apresentado, podemos concluir que quando o assunto for Segurança da Informação, toda atenção/precaução torna-se necessária. Sabemos que nos dias de hoje a informação contém um valor importantíssimo para as organizações como um todo. A cada dia temos um novo cenário, com uma nova necessidade, que requer uma nova análise. Assim, temos que ter ciência de que a área de segurança da informação sempre estará preparada para atender os novos cenários apresentados, sem perder seus princípios básicos da informação.

A utilização de segregação de função, não consiste apenas em preparar um cenário para atendimento de auditorias internas ou externas, ou até mesmo para a confiança de seus investidores no caso de empresas com capitais abertos... Mas sim na segurança de todo o processo executado dentro dela, barrando todo e quaisquer erro efetuado dentro de sua base de dados. Nada mais é, do que assegurar sua própria segurança.

Acreditamos que a área de segurança expandirá conforme as necessidades apresentadas no cotidiano empresarial. Não sabemos ao certo, qual será a melhor técnica de segurança a ser implantada para os próximos cenários, mas temos a ciência de que o que temos hoje como solução não nos atenderá em problemas futuros.

Entendemos que quanto mais poderes/permissões um determinado usuário possui no sistema, mais riscos ele está trazendo para a organização. Seja por falta de conhecimento ou até mesmo por malícia. A segurança por sua vez, visa barrar toda e quaisquer situação de incoerência e não conformidade, perante suas regras. Estamos vivendo em um cenário dinâmico dentro das organizações, onde temos a necessidade de acompanhá-las.

.....

6.REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação.

GIL, Antonio de Loureiro. Segurança em Informática. 5.ed, 2000.

REIS, Émilén Vilas Boas. domtotal. Disponível em <<http://www.domtotal.com/colunas/detalhes.php?artId=2023>>. Publicado em julho 2011.

GUIMARAES, Cristina Santos. ITFORUM 365. Disponível em <<http://www.domtotal.com/colunas/detalhes.php?artId=2023>>. Publicado em julho 2015.

HARRIS, Shon. CISSP EXAM GUIDE. 1.ed, 2013.

LIMA, Fabricio de Jesus Lima. UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ. Disponível em <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2516/1/CT_GESER_III_2013_03.pdf>Publicado em dezembro 2013.

FELEOL, Alex. Artigos. Disponível em <<http://alexfeleol.com.br/2012/06/23/os-tres-pilares-da-seguranca-da-informacao/>>. Publicado em junho 2012

Dicionário, Michaelis

Disponível em

<<http://michaelis.uol.com.br/moderno/portugues/index.php?lingua=portugues-portugues&palavra=função>>

Publicado em 2009

SILVA, Richard Flavio. ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO. Disponível em

< <http://www.teses.usp.br> >

Publicado em dezembro 2010.

Help Portal SAP. Artigos. Disponível em

<http://help.sap.com/saphelp_46c/helpdata/en/5c/deaa74d3d411d3970a0000e82de14a/content.htm>. Publicado em dezembro 2014