

Bruno Canever Schneider

GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO NO SISTEMA SAP

FACULDADE DE TECNOLOGIA DE SÃO PAULO
Departamento de Tecnologia da Informação

São Paulo/SP
2012

BRUNO CANEVER SCHNEIDER

GOVERNANÇA DA TECNOLOGIA DA INFORMAÇÃO NO SISTEMA SAP

Monografia apresentada à
Faculdade de Tecnologia de São Paulo,
como requisito parcial para obtenção do título de Especialista em
Tecnologia de Análise e Projeto de Sistemas
Orientador: Prof. Dr. Carlos Hideo Arima

FACULDADE DE TECNOLOGIA DE SÃO PAULO
Departamento de Tecnologia de São Paulo

São Paulo/SP
2012

DEDICATÓRIA

Dedico este trabalho à minha família, meus amigos e a todos que de alguma forma me auxiliaram a concluí-lo.

AGRADECIMENTO

Ao meu orientador, aos meus companheiros durante o
curso e aos meus pais.

BANCA EXAMINADORA

SUMÁRIO

Resumo	2
Abstract.....	3
Introdução.....	4
Identificação do Problema	5
Hipótese	5
Objetivo Geral.....	5
Objetivo Específico.....	5
Metodologia de Pesquisa	6
Estrutura do Trabalho.....	6
1. GOVERNANÇA DE TI	8
1.1. Lei Sarbanes-Oxley	11
1.2. Segregação De Funções	13
2. RISCOS	16
3. CONSTITUIÇÃO DA GOVERNANÇA DE TI NO SISTEMA SAP	20
3.1. Definição Dos Riscos e Transações Críticas.....	20
3.2. Definição Dos Usuários e Atividades.....	25
3.3. Criação Dos Perfis.....	29
3.4. Criação Das Regras no Sistema	34
3.5. Análise Dos Riscos.....	36
3.6. Remediação Dos Riscos	39
3.6.1. LIMPEZA TÁTICA DOS ACESSOS	40
3.6.2. REDESENHO ESTRATÉGICO DE PERFIS	40
3.7. Remediação No Sistema.....	41
3.7.1. EXCLUSÃO DA TRANSAÇÃO.....	41

3.7.2. EXCLUSÃO DO PERFIL	42
3.7.3. MUDANÇA NOS VALORES DOS OBJETOS	42
3.7.4. MUDANÇA NOS USUÁRIOS DEDITIDOS	42
3.8. Mitigação Dos Riscos	43
3.8.1. CONTROLES PREVENTIVOS.....	44
3.8.2. CONTROLES DETECTIVOS	44
3.9. Controles Mitigatórios No Sistema	46
3.10. Testes.....	47
3.11. Go-Live	49
3.12. manutenção das conformidades.....	51
3.13. Considerações Finais	53
CONCLUSÃO	56
REFERÊNCIAS	58
BIBLIOGRAFIA CONSULTADA	59

LISTA DE TABELAS

Tabela 1. Descrição das Principais Atividades no Processo	52
---	----

LISTA DE FIGURAS

Figura 1. Governança de TI Dentro da Governança Corporativa	6
Figura 2. CobIT e ITIL e sua separação pelos níveis da empresa.....	8
Figura 3. Matriz de Conflitos cruzando.....	20
Figura 4. Matriz com as transações que executam as funções.....	21
Figura 5. Lista dos acessos críticos com suas respectivas atividades.....	22
Figura 6. Exemplo de um organograma.....	23
Figura 7. Planilha com o mapeamento de uma área.....	24
Figura 8. Documentação dos Riscos no Sistema.....	32
Figura 9. Visão dos Conflitos na Ferramenta.....	34
Figura 10. Exemplo de um Plano de Testes.....	45
Figura 11. Tela mostrando a transação SU53.....	46
Figura 12. Transporte pelos ambientes do SAP.....	48

RESUMO

Este trabalho trata da gestão de controles internos das empresas para conseguir segregar as funções dentro dos departamentos, nas atividades que estão relacionadas à utilização do sistema SAP (System Application and Products in Data Processing), é cada vez maior a necessidade de separar a execução de algumas atividades nos sistemas, algumas delas podem ser fraudulentas e devemos evitar que possam ser executadas por somente um único usuário. É apresentado o processo de mapeamento das atividades, definição de quais delas apresentam algum risco para o andamento dos negócios, a lógica para criação de perfis no sistema, separando-as, e a maneira como elas são segregadas entre os usuários, seja por meio de exclusão de acessos ou controles. Tudo isso é documentado no sistema, com auxílio de uma ferramenta conjunta ao SAP. Após adequar todo o ambiente de Tecnologia da Informação, é necessário fazer a manutenção do que foi documentado, extrair relatórios periodicamente e testar os controles implementados. Essas são atividades essenciais de longo prazo, assim como a definição de novos riscos que possam surgir e a sua respectiva criação no sistema. Após essa primeira etapa do processo, a empresa passa a ter um conhecimento muito maior de suas atividades e do organograma das áreas, possibilitando o seu crescimento sem perder o controle das suas atividades.

Palavras-chave: governança de TI, riscos, segregação de funções, controle.

ABSTRACT

This work deals with the management of company's' internal controls, to segregate the duties within the departments, in activities that are related to the use of SAP system (System Application and Products in Data Processing), It is increasing the need of segregate the performance of some activities in the system, some of them can be fraudulent, and we should avoid that they can be performed by only one user. It is presented the process of mapping activities and define which of them present a risk to the business progress, as well as the logic for creating profiles on the system and how they are segregated between users, either through exclusion or access compensating controls. This entire process is documented in the system with the aid of a tool joint with SAP called Risk Analysis and Remediation. After adapting the whole environment of Information Technology, it is necessary to maintain what has been done on the system, extract reports periodically and test the implemented controls. These activities are essential in the long term, as well as the definition of new risks that may arise in and its creation in the system. After this first stage of the process, the company will have greater knowledge and control of their activities, allowing their growth without losing control of their activities.

Keywords: IT Governance, risks, segregation of duties, control.

INTRODUÇÃO

Uma das principais características dos sistemas ERP (*Enterprise Resource Planning*) é a integração dos dados, e isso pode se transformar em um problema para as empresas que implantam esses softwares sem considerar os seus aspectos de segurança e o controle das operações.

Normalmente, a empresa que utiliza o SAP realiza todos os seus processos por meio de seu ERP, e na maioria das vezes, ele baseia-se inicialmente no *template* oferecido durante a sua implementação, sendo que ele tem como objetivo somente auxiliar na instalação rápida, sem privilegiar qualquer aspecto de segurança, algo necessário atualmente.

De acordo com a sua utilização, a empresa verifica que alguns usuários não podem executar todas as suas funções com os acessos do *template*, logo, decidem liberar todas as transações de algum determinado módulo para um usuário específico. Assim, quando alguém houver problema na execução de uma atividade, basta entrar no sistema com esse outro usuário e proceder normalmente. Em alguns casos, pode ocorrer algo pior e a empresa colocar o acesso completo do módulo para todos os usuários com acesso ao sistema.

As empresas não se preocupam muito com a segregação de funções no sistema SAP, elas têm um grau elevado na confiança de que os seus usuários não conhecem suas reais permissões de acesso ao sistema e optam por não adotar qualquer controle, deixando as melhores práticas de segurança e controles de lado (Ernst & Young Digital Insights: Dados Sobre Segurança da Informação, 2005).

Nesses casos, se algum dos usuários com acesso completo ao sistema quiser cometer uma fraude, ele está habilitado, e como não há uma governança no ambiente de TI, quando a empresa perceber que essa fraude foi realizada, já será muito tarde.

IDENTIFICAÇÃO DO PROBLEMA

O sistema funciona, mas qual é o nível de segurança proporcionado a ele, para que possa minimizar a ocorrência de fraudes?

HIPÓTESE

Para avaliar essa situação, a empresa teria que controlar os riscos existentes por meio da segregação de funções em suas atividades relacionadas com o sistema SAP. Sendo assim, as ferramentas disponíveis e os modelos de governança já utilizados por algumas empresas, é possível estruturar o ambiente de Tecnologia da Informação para que haja controle sobre os riscos de operação existentes no sistema SAP, possibilitando a redução de ocorrência de fraudes.

OBJETIVO GERAL

O trabalho objetiva mostrar como a segregação de funções no sistema SAP faz com que a empresa controle melhor suas operações, sabendo-se quem é responsável por cada etapa do negócio e, também, de se adequar às normas regulatórias existentes, como a Lei Sarbanes-Oxley.

OBJETIVO ESPECÍFICO

Identificar os processos que o sistema SAP apresenta em relação aos aspectos de segurança e aos riscos que existem em todas as áreas da empresa que o acessam.

Verificar como a segregação de funções pode auxiliar na segurança dos processos informatizados, junto com uma metodologia adequada para reconhecimento dos riscos e acessos das áreas para auxiliar a empresa.

Analisar a forma como são documentados os riscos para fins de governança de Tecnologia da Informação conforme as normas e procedimentos regulados pela Lei Sarbanes-Oxley.

METODOLOGIA DE PESQUISA

A forma de pesquisa utilizada foi indutiva e explicativa, aprofundando o conhecimento da realidade dos riscos nas atividades desempenhadas pelas empresas no sistema SAP, mostrando como definir esses riscos e os benefícios que o investimento nesse processo traz para a empresa. O delineamento foi experimental, o processo foi planejado, implantado desde o início, e ao fim, é possível analisar os dados.

A pesquisa foi baseada nas normas ISO 27002 e no guia de boas práticas CobIT 4.1, que são referências para delinear as atividades da área de Tecnologia da Informação, definindo como o ambiente de TI deve estar organizado para que não ocorra possibilidade de qualquer impacto nas atividades financeiras da companhia.

O trabalho apresenta as técnicas recomendadas para segregar as funções no SAP, utilizando uma ferramenta que atua junto com ele, melhorando o desempenho do sistema. A análise de dados é quantitativa, pois é possível mensurar tudo que está sendo aplicado, comparar como o ambiente estava antes e como ele fica com as mudanças de perfil e definições de atividades e transações críticas.

ESTRUTURA DO TRABALHO

O trabalho é iniciado com uma explicação sobre a Governança de Tecnologia da Informação, comenta sobre o seu papel dentro da governança corporativa e sobre as metodologias que definem a maneira como ela deve estar estruturada. É apresentada a Lei SOX, mostrando seus principais aspectos e como ela é aplicada na área de TI. Após comentar sobre a Lei SOX, é explicada a segregação de

funções, quais motivos levam as empresas a adotá-la, e quais os principais benefícios conseguidos após sua implementação.

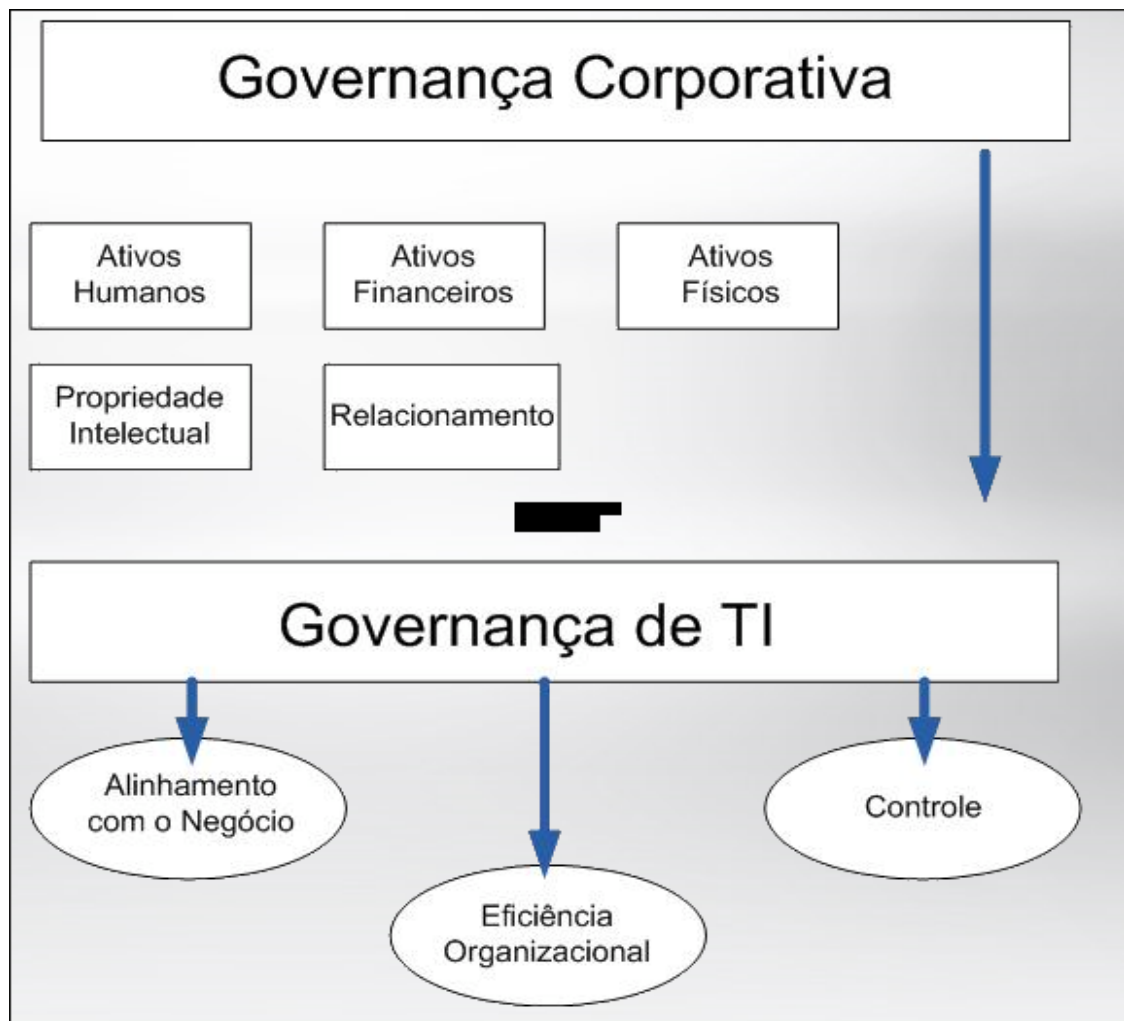
O próximo passo é a apresentação dos riscos, o conceito do que são eles e uma boa prática para geri-los. Controles e ferramentas que são utilizados e auxiliam nesse processo são comentados para completar a descrição da atividade.

No terceiro capítulo são apresentadas todas as etapas do processo, desde a definição das atividades e os riscos atrelados, seguindo com sua imputação no sistema, as escolhas dos responsáveis para que o sistema esteja operando da maneira mais segura possível em relação às fraudes e como efetuar a manutenção de tudo que foi definido.

1. GOVERNANÇA DE TI

Governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de governança corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade (IBGC, 2012).

Governança de TI é uma derivação da Governança Corporativa. A Tecnologia da Informação não é apenas uma área de suporte nas empresas, ela auxilia cada vez mais no desenvolvimento dos negócios, estratégias e objetivos. Preocupações técnicas e estratégicas fazem parte do cotidiano dos profissionais de TI. O conceito de governança de TI é um conjunto de diretrizes cujo objetivo é produzir ganhos de eficiência e eficácia na estrutura e nos processos relacionados à área.



Fonte: Ernst Young Digital Insights ERP, 2009

Figura 1. Governança de TI dentro da Governança Corporativa

Conforme figura 1, o grande desafio da TI é conciliar a necessidade de acompanhar a velocidade de transformação da tecnologia, conhecer as exigências dos clientes e estar em alinhamento com o negócio, para gerar informações sobre ele, de modo ágil e confiável, a fim de auxiliar na tomada de decisões da corporação e para atender todas essas exigências um modelo de gestão de recursos precisa ser adotado, visando não comprometer os resultados (Ernst & Young Digital Insights: Governança e Resultados, 2007).

A busca pelas melhores práticas de gestão ocupa, hoje, boa parte da agenda dos executivos das grandes corporações. Transparência, eficiência organizacional, maximização e retorno dos investimentos, adequação dos processos internos às leis

e normas internacionais, como Sarbanes-Oxley, são requisitos essenciais no mercado cada vez mais globalizado (Ernst & Young Digital Insights: IT Risk, 2010).

Um dos primeiros passos adotados pela governança de TI é a especificação de *Key Users*, funcionários considerados fundamentais em uma determinada empresa, para auxiliar na tomada de decisões. Com sua influência, eles auxiliam para que haja um comportamento desejado na utilização dos recursos de TI.

Para que não aconteçam problemas com a segurança da informação, a ISO 27999 sugere que a organização aprove um documento da política da empresa, expressando as preocupações da direção para a gestão da informação, visando aspectos como confidencialidade, integridade e disponibilidade. Garantindo que o acesso à informação é permitido somente àqueles com autorização para recebê-la, a mesma está completa e disponível sempre que for necessário.

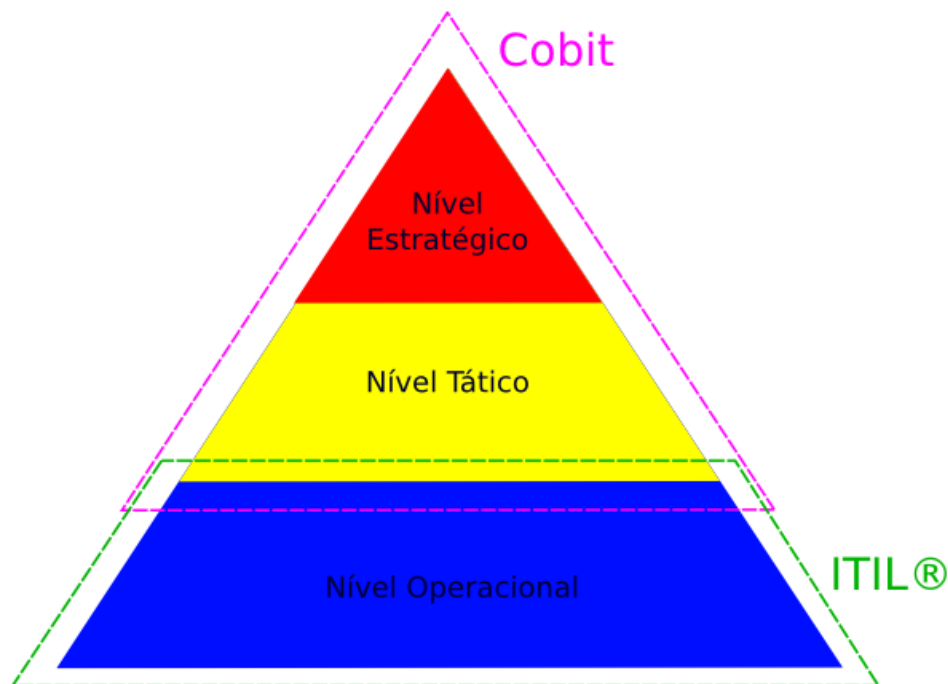
Em muitas corporações o processo de governança de TI se inicia com uma demonstração dos riscos envolvidos no controle inexistente do ambiente de TI, prejudicando a integridade das informações.

Consequências decorrentes de riscos da integridade da informação são difíceis de quantificar, mas deficiências na integridade da informação podem ter consequências importantes e de longo alcance para uma entidade, podendo ser muito caro em termos financeiros, de tempo e de recursos (IT Governance Institute, 2004).

Todo sistema está sujeito a falhas, erros e mau uso em geral. Tanto o computador como a mente humana são instrumentos para grandes realizações; porém, são capazes de cometer falhas. Devido à existência desse risco, administradores e proprietários de pequenas e grandes organizações, devem ter um interesse comum pela integridade dos sistemas computadorizados e pelas pessoas envolvidas no meio (Arima, 1994).

A Governança de TI é baseada nas metodologias CobIT e ITIL. O CobIT atinge mais os níveis estratégicos e táticos da empresa. Ele define Governança de TI como uma estrutura de relacionamentos entre processos para direcionar e controlar uma empresa, de modo a atingir objetivos corporativos, através da agregação de valor e risco controlado pelo uso da tecnologia de informação e seus processos. O ITIL é mais ligado ao nível operacional.

O CobIT define a metodologia de um modo mais voltado para os processos, tendo em vista a auditoria. Já o ITIL define com ênfase no suporte técnico, possibilitando gerenciar os serviços e verificar se estão de acordo com as necessidades da empresa (figura 2).



Fonte: <http://tectecnologia.files.wordpress.com/2009/11/itil-cobit.png>

Figura 2. CobIT e ITIL e sua separação pelos níveis da empresa

1.1. Lei Sarbanes-Oxley

A Lei Sarbanes-Oxley (SOX) determina a criação de um conjunto de procedimentos internos de mecanismos de auditoria e segurança confiáveis nas

empresas. Com isso, a área de Tecnologia da Informação se deparou com a oportunidade de construir um modelo de governança, considerando aspectos de prestação de contas e visando responder rapidamente àquilo que o negócio requer.

A Lei Sarbanes-Oxley (2002) foi aprovada pelo congresso norte-americano com o intuito de restabelecer a confiança dos investidores e a sustentabilidade das empresas, que estavam muito abalados pela série de escândalos financeiros que vinham ocorrendo. Todas as empresas de capital aberto tiveram que se adequar à lei para continuarem listadas no mercado das Bolsas de Valores.

Um dos aspectos da Lei Sarbanes-Oxley está englobado na seção 806, na qual são previstas medidas de proteção contra ações de retaliação aos empregados que recorrem ao sistema de denúncia de infrações com a intenção de apresentar provas sobre fraudes que ocorreram nas empresas.

O principal objetivo dessa lei é garantir a criação de métodos confiáveis para a auditoria e segurança no mercado corporativo. Controles devem ser determinados e cumpridos. Eles servem para monitorar os processos existentes e para auxiliar na segregação de funções, tornando mais difícil que haja alguma fraude e que quando ela vier a ocorrer, que seja facilmente identificada.

A seção 404 determina que os controles devem ser avaliados por uma equipe independente, ou seja, uma equipe de auditores. Durante o processo de auditoria eles executam processos completos no sistema, conferindo se os controles funcionam de acordo com o que foi elaborado e validado.

A área de TI está relacionada com todas as atividades realizadas pela empresa, logo, a seção 404 da SOX que foi apresentada anteriormente atinge principalmente essa área, pois faz com que as empresas invistam em controles internos, avaliando os riscos inerentes e riscos de controle. É necessário compreender como está estruturado o programa de controles internos da empresa e o processo de elaboração de demonstrações financeiras, mapear os sistemas que são responsáveis pela execução desses processos, identificar os riscos, projetar

controles para minimizar e monitorar esses riscos existentes, testar e documentar os controles, assegurar que eles estejam sempre atualizados, modificando quando for necessário para corresponder às alterações ocorridas.

A Lei também engloba conceitos importantes relacionados ao controle de acessos. É fundamental conhecê-los para compreender a parte de segregação de funções que é explicada nos próximos capítulos:

Existem as transações críticas: são todas as que podem alterar o demonstrativo financeiro e o balanço da empresa; e as transações conflitantes: aquelas que quando combinadas, independente de serem duas ou mais transações, possibilitam ao usuário alterar os dados financeiros da empresa.

Toda cadeia de comunicação da empresa deve estar adequada à Lei SOX, principalmente aquilo que é relacionado às informações financeiras. Colocar um controle de registros em prática é fundamental para que não ocorra discrepância nos valores finais no momento do fechamento.

O controle de acessos é um aspecto importante na SOX, para que possa existir um controle adequado. As melhores práticas de mercado indicam que seja realizada uma segregação de funções no sistema.

1.2. Segregação De Funções

Um dos principais temas abordados pelos profissionais responsáveis pela governança de TI, buscando se adequar aos padrões definidos pela Lei SOX é a segregação de funções nos sistemas.

Se no passado a proliferação de perfis foi a solução para manter a continuidade dos negócios, hoje ela tira o sono dos profissionais da área de TI. Para não correr o risco de dar acessos privilegiados aos usuários, ganham força nas

empresas os projetos sobre segregação de funções (Ernst & Young Digital Insights: Governança e Resultados, 2007).

A segregação de funções é um método para redução do risco de mau uso accidental ou deliberado dos sistemas. Convém que a separação da administração ou execução de certas funções, ou áreas de responsabilidade, a fim de reduzir oportunidades para modificação não autorizada, ou mau uso de informações ou de serviços, seja considerada. Onde for difícil a segregação, convém que outros controles, como monitorar as atividades, trilhas de auditoria e o acompanhamento gerencial, sejam considerados (ISO 27002).

Segregação de funções (SoD) é um dos assuntos mais comentados entre uma vasta gama de profissionais, desde *compliance* até os diretores executivos. Grande parte desse interesse na segregação de funções é devido, em parte, às exigências da Lei SOX, mas há um outro fator fundamental para isso, um princípio em que nenhum usuário do sistema deve ter acessos excessivos, possibilitando que ele faça a execução de transações que sejam consideradas conflitantes sem que elas sejam conferidas, e que haja um balanço. Permitir esse tipo de acessos representa um risco real ao negócio, e fazer a gestão desses riscos de forma pragmática e eficaz é mais difícil do que aparenta ser (Isaca Journal: SoD, 2009).

Em linhas gerais, a segregação de funções busca reduzir o acesso de funcionários de uma organização ao mínimo necessário para que ele possa executar suas atividades, tendo em vista que a maioria das invasões aos sistemas é feita por pessoal com acessos autorizados. Para piorar, o volume de usuários nas empresas e a complexidade dos sistemas de aplicação são cada vez maiores (Ernst & Young Digital Insights: IT Risk, 2010).

Convém que sejam tomados certos cuidados, para que as áreas nas quais a responsabilidade é de apenas de uma pessoa, não venha a ser alvo de fraudes que não possam ser detectadas. Recomenda-se que o início de um evento seja separado de sua autorização (ISO 27002).

Um programa eficiente de segregação de funções traz diversos benefícios às organizações, como por exemplo: identificar deficiências em operações financeiras, determinação de quais operações devem estar separadas, definição de uma estratégia para contornar os problemas existentes no sistema e auxílio para que no futuro a ocorrência de qualquer problema seja reduzida.

A empresa não precisa criar uma estrutura muito complexa para os perfis, ou sistemas de revisão caros para encontrar os casos de segregação de funções. Basta direcionar o foco às transações que oferecem algum tipo de risco ao sistema, e rapidamente são entendidas as questões relacionadas com os acessos e reconhecidas as maneiras como remediá-las ou mitigá-las.

2. RISCOS

O capítulo anterior tratou a governança de TI e o seu alinhamento com as estratégias do negócio, mas como saber se esse alinhamento está sendo executado de maneira correta? Como saber se os procedimentos são corretos?

Essas respostas só são possíveis por meio de um controle dos riscos existentes. Normalmente, risco é associado com algo negativo, mas ele é apenas relacionado com a incerteza de algum evento. Todas as atividades executadas apresentam algum risco.

A palavra “risco” deriva do italiano antigo *risicare*, que significa “ousar”. Neste sentido, o risco é uma opção, e não um destino. É das ações que ousamos tomar, que dependem de nosso grau de liberdade de opção, que a história do risco trata (Bernstein, 1996).

Devemos olhar a palavra “riscos” como se fosse uma etiqueta para “marcar” quais são as grandes preocupações e incertezas, assegurando sua presença na agenda dos executivos da organização.

Não se pode virar as costas para o problema dos riscos existentes no sistema. Na melhor das hipóteses, nada de errado ocorre, mas o sistema permite que isso ocorra.

Se tudo for uma questão de sorte, a administração do risco é um exercício sem sentido. Invocar a sorte obscurece a verdade, porque separa um evento de sua causa. Quando dizemos que alguém foi vítima de má sorte, eximimos tal pessoa de qualquer responsabilidade pelo ocorrido. Quando dizemos que alguém é sortudo, negamos a tal pessoa o crédito pelo esforço que pode ter levado ao resultado feliz (Bernstein, 1996).

Quando alguém corre um risco, aposta em um resultado que é consequência de uma decisão tomada, embora não se saiba ao certo qual é esse resultado. A

essência da administração dos riscos está em maximizar as áreas onde temos certo controle sobre o resultado, enquanto minimiza as áreas onde não temos absolutamente nenhum controle sobre o resultado e onde o vínculo de causa e efeito está oculto de nós (Bernstein, 1996).

Com o passar do tempo e as mudanças nos processos que as empresas realizam, novos riscos aparecem. A demanda pela administração dos riscos cresce junto com o número de riscos existentes. De acordo com Bernstein (1996), “O risco e o tempo são as faces opostas da mesma moeda, pois sem amanhã não haveria riscos. O tempo transforma o risco, e a natureza do risco é moldada pelo horizonte de tempo: o futuro é o campo de jogo”.

A aparição abrupta de novos riscos em áreas consideradas por tanto tempo estáveis, desencadeou uma busca de ferramentas de administração do risco, novas e mais eficazes. A ciência da administração dos riscos cria, às vezes, novos riscos, ainda que leve o controle a antigos riscos. A fé na administração dos mesmos encoraja a assumir riscos que, normalmente, não se assumiria. Normalmente, isso é benéfico, mas é preciso ter cuidado para não aumentar a quantidade deles no sistema (Bernstein, 1996).

Com os riscos sob controle, a área de governança de TI fica mais forte, demonstrando seriedade e comprometimento com os objetivos estratégicos, tornando mais eficiente o alinhamento entre TI e os negócios, fortalecendo a organização.

Sempre houve riscos nos sistemas, mas nunca lhes foi dada muita atenção, já que ninguém havia sofrido prejuízo por causa de possíveis fraudes. Isso mudou com o caso da companhia de energia norte-americana Enron, que manipulou seus balanços financeiros com a ajuda de empresas e bancos, visando o mercado de ações e acabou falindo, arrastando consigo a Arthur Andersen, que era a maior auditoria do mundo à época e possuía a responsabilidade de auditá-la.

Os especialistas em negócios são responsáveis por organizar e auxiliar as fases de reconhecimento dos riscos e das regras de construção do processo, visando identificar, classificar e documentar os potenciais riscos que podem vir a afetar os processos de uma determinada organização. Também cabe aos especialistas a tarefa de avaliar os controles de gestão de mudança dentro da solução (SAP Education, 2010).

A gestão de riscos está diretamente relacionada com os controles internos, definindo as normas, procedimentos, práticas e estruturas que possibilitam segurança para que a empresa alcance os seus objetivos. Caso haja algum problema, ele é detectado e corrigido.

Os controles existentes podem ser manuais e automáticos. Os manuais são executados por algum profissional da área e não há a utilização de qualquer software. Os automáticos são normalmente por meio de softwares, focando em operação e gestão de dados.

Os objetivos principais dos controles são: garantir o cumprimento das atividades no prazo estipulado e assegurar-se das normas legais, colaborar com o trabalho da auditoria, tanto a interna quanto a externa e ter a certeza de que não é possível executar fraudes sem que elas sejam percebidas.

Para facilitar a gestão dos riscos nas empresas que utilizam SAP, foi lançada recentemente uma ferramenta que vai agir conectada ao sistema, o GRC. Os módulos do SAP GRC auxiliam a empresa em relação aos riscos, governança e compliance. No trabalho, é apresentado o *SAP GRC Access Control* e seu módulo utilizado para a análise de riscos.

O *Risk Analysis and Remediation Control* é um dos produtos do *SAP GRC Access Control*, e auxilia as empresas a manter o cumprimento das normas definidas. Ele valida as autorizações de segurança dos seus empregados, para que elas correspondam somente ao seu papel e deveres. Essa ferramenta ajuda os clientes a gerenciar de maneira mais inteligente as autorizações que seus

empregados têm no ambiente de Tecnologia da Informação, permitindo exceções autorizadas e acelerando a resolução de violações, tudo isso reduzindo os custos.

Logo após a instalação do Risk Analysis and Remediation Control é necessário checar a configuração de alguns itens, tendo em vista o pleno funcionamento da ferramenta. O *job daemon* deve estar funcionando, pois é ele que possibilita a interface com o servidor, os conectores Java devem estar ativados, assim como o *User Management Engine*, pois é nele que ficam os perfis importados do sistema.

Se estabelece um programa corporativo de melhoria contínua que leva em consideração as lições aprendidas e as melhores práticas de monitoramento dos controles internos. São utilizadas ferramentas integradas e atualizadas quando apropriado, que permite a efetiva avaliação dos controles críticos de TI e a rápida detecção dos incidentes de monitoramento dos controles de TI (CobIT 4.1).

No próximo capítulo é explicado, passo a passo, como executar um processo completo de segregação de funções no sistema SAP, utilizando o *Risk Analysis and Remediation Control*, visando otimizar os negócios, com a redução de número de perfis no sistema, conhecimento das transações que apresentam mais risco e a documentação de todos controles existentes.

3. CONSTITUIÇÃO DA GOVERNANÇA DE TI NO SISTEMA SAP

Para começar, é definido o escopo entre quem for prestar o serviço e a empresa. É possível realizar o processo somente com algumas áreas, mas as outras continuam com os problemas de acessos existentes. Também é possível somente definir os riscos e utilizar a ferramenta, mas isso não minimiza completamente o número de perfis existentes no sistema. A ferramenta age somente nos perfis que apresentam risco. Caso algumas atividades não sejam consideradas de risco, o usuário continua a ter acesso, mesmo que não seja necessário para o cumprimento de suas atividades.

3.1. Definição Dos Riscos e Transações Críticas

O objetivo desta fase é obter uma compreensão do escopo das transações críticas e dos conflitos que existem nos processos críticos de negócios da companhia. Há também as transações que representam o maior risco de fraude para a organização, caso alguém possua acesso excessivo. Limiares são determinados com base nos riscos e impactos para a empresa em cada potencial conflito de segregação de funções (Ernst & Young Digital Insights: IT Risk, 2010).

É essencial que uma organização identifique os seus requisitos de segurança. Existem três fontes principais: avaliação de riscos dos ativos da organização, a legislação vigente, os estatutos, regulamentação e cláusulas contratuais que a organização tem que atender e, por fim, o conjunto de princípios, objetivos e requisitos para processar a informação que serve de apoio para as operações da empresa (ISO 27002).

A simulação dos riscos permite identificar os pontos vulneráveis e as principais ameaças para o ambiente corporativo. A fase de avaliação dos riscos deve ser completada com uma análise do impacto que eles causam para os processos do negócio. Isso possibilita delinear as estratégias adequadas e as medidas de controle necessárias (Ernst & Young Digital Insights: Governança e Resultados, 2007).

São mapeadas todas as áreas da empresa. Todos os acessos devem ser documentados. Essa parte do processo é fundamental. Erros nessa etapa ocasionam em problemas futuros. A empresa deve ter conhecimento de como definir os riscos, caso contrário acaba definindo uma infinidade de conflitos, e é demasiadamente caro para aplicar no sistema. É recomendável que primeiro sejam mapeadas todas as atividades de uma determinada área e somente após saber tudo que está sob sua responsabilidade, é que devem ser definidos os riscos.

Os resultados dessa avaliação ajudam a direcionar e determinar ações gerenciais e prioridades mais adequadas para um gerenciamento de riscos da segurança da informação. Auxilia também na seleção dos controles que são implementados para a proteção contra estes riscos (ISO 27002).

Para realizar essa etapa de acordo com a sugestão da Lei SOX, conforme explicado no segundo capítulo, além de definir quais são os riscos, conforme visto no capítulo 2, também é necessário documentar as transações que são consideradas críticas, mas que não se encaixam em nenhum caso de segregação de funções, pois pode ocorrer de algum processo crítico da empresa ser executado no SAP, mas não haver nenhuma outra atividade que conflite com ela. Nesses casos, deve somente ser documentado quais são as transações críticas e em qual processo ela está englobada.

Utiliza-se o mapeamento feito para que seja possível responder às seguintes perguntas: quais aplicativos são capazes de executar as operações definidas como críticas? Qual a maneira que eles são executados no sistema? A companhia deve mapear cada transação crítica e todos os acessos que são possíveis quando ela é utilizada. Deve mapear também qual é a aplicação que permite a sua execução (normalmente é no SAP ERP, mas podem-se encontrar alguns casos no SAP CRM, alguma empresa que identifique algum risco relacionado à manutenção de seus clientes). (Ernst & Young Digital Insights: IT Risk, 2010).

O ideal é identificar os riscos de autorização e aprovar as exceções existentes, também esclarecer e classificar os riscos em alto, médio e baixo, identificar novos riscos e as condições para monitorá-los futuramente (SAP Education, 2010).

Convém que as análises críticas sejam executadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações de riscos feitas anteriormente e das mudanças nos níveis de riscos que a direção considera aceitável para os negócios. As avaliações de risco são sempre realizadas primeiro em nível mais geral, como uma forma de priorizar recursos em áreas de alto risco, e então em um nível mais detalhado, para solucionar riscos específicos (ISO 27002).

Ao comparar dois casos de segregação de funções, é necessário analisar que cada conflito representa um risco diferente para a empresa e cada um deles deve ser avaliado de acordo com a probabilidade de um usuário executar as funções conflitantes. As empresas adotam muitos esquemas e notações para classificar os seus conflitos. As avaliações corretas e definições de como administrar cada um dos riscos classificados é um fator chave na prestação de benefícios em um processo baseado em riscos (Ernst & Young Digital Insights: IT Risk, 2010).

O melhor método para documentação inicial dessas atividades é criar uma matriz de conflitos. Todos os módulos do SAP apresentam suas transações críticas. Já há uma matriz pré-definida de riscos para cada um dos módulos, mas ela engloba somente alguns aspectos. As matrizes são muito diferentes de acordo com os processos e com o ramo de negócio das empresas. Elas devem utilizar a matriz global de riscos apenas como base para entender o processo. Após esse entendimento, o ideal é que eles customizem sua matriz de riscos, essa matriz deve utilizar algum modelo parecido com o da figura 3. Dependendo das atividades, algumas empresas montam mais de uma matriz, visando englobar detalhadamente algum processo que seja considerado de maior criticidade para eles.

Conflicts Matrix - Segregation of Duties								
	Management of Medical Benefits Master Data	Management of Hire Master Data	PnR (variable pay) Management	Manage Performance Evaluation (create, modify and terminate)	Compensation Management (Update HR Master Data)	Management Registered Hours (Update Time Data / Maintenance Hours)	Manage Off-Cycle Payment (Paid Vacation, Ticket, Transport, etc.)	Change FGTS (fund) balance
Management of Medical Benefits Master Data								
Management of Hire Master Data								
PnR (variable pay) Management								
Manage Performance Evaluation (create, modify and terminate)								
Compensation Management (Update HR Master Data)	23							
Management Registered Hours (Update Time Data / Maintenance Hours)								
Manage Off-Cycle Payment			10		27			
Change FGTS (fund) balance				15				

Fonte: Ernst Young Digital Insights ERP, 2009

Figura 3. Matriz de Conflitos cruzando

Esta etapa alimenta a análise de dados ao configurar os acessos. A parte de mapeamento é fundamental no processo, mas é nessa etapa que muitas vezes as empresas acabam encontrando problemas, pois há uma enorme falta de compreensão de todas as funcionalidades de uma determinada transação em um sistema. Na maioria dos casos, a transação é utilizada somente para algo específico, mesmo podendo executar diversas outras atividades.

Certamente ocorre também a identificação de algumas atividades críticas que podem ser executadas por meio de várias transações. É necessário que a empresa tenha conhecimento de todas elas, para que seja possível restringir o acesso ou então criar controles relacionados. Esse tipo de trabalho exige que a empresa passe a conhecer todas as maneiras que o sistema possibilita para que uma atividade seja executada.

Ao identificar as diversas atividades críticas que são feitas no sistema e quais todos os meios possíveis de executá-la é que começa a montagem da matriz de riscos, essa matriz é a base de como são definidos os acessos no sistema. As diversas funções mapeadas conflitam entre elas e isso é considerado crítico. Conforme apresentado no primeiro capítulo, riscos são uma oportunidade para perda física, fraude, interrupção de um processo ou perda de produtividade que pode

ocorrer quando um dos funcionários explorar uma condição específica. Uma mesma função pode estar englobada em diversos casos de riscos.

Um determinado usuário pode criar um vendedor fictício ou mudar os dados-mestres de um vendedor cadastrado no sistema, podendo iniciar uma compra com este vendedor e emitir o pagamento do mesmo, gerando uma fraude (Ernst & Young Digital Insights: IT Risk, 2010).

A figura 4 mostra o exemplo de uma matriz com a separação das atividades, as transações responsáveis por executá-las e o risco existente caso alguém possua esses acessos.

# SOD	Função 1	Transação 1	Função 2	Transação 2	Risco
SoD01	Executar Ajustes de Remuneração (Promoções e Aumentos Salariais)	ZHCM008, ZHCM009, ZHCM011, ZHRCM004, ZHCM010, PA40,	Processar Folha de Pagamento	PC00_M37_CALC, PA03, ZBRHR_TSAF023, ZBRHR_TSAF024, ZBRHR_TSAF025	Atualizações não autorizadas da base de pagamentos (Bônus, Promoções, Aumentos, etc.), seguida do processamento da folha de pagamento, resultando em dados inconsistentes a serem pagos aos funcionários.
SoD02	Processar Folha de Pagamento	PC00_M37_CALC, PA03, ZBRHR_TSAF023, ZBRHR_TSAF024, ZBRHR_TSAF025,	Exclusão do Cálculo da Folha de Pagamento	PU01, ZBRHR_SAF007, ZHPYM012, ZPHRCL_U0002	O colaborador poderia processar indevidamente a folha de pagamento e posteriormente excluir as alterações feitas de forma indevidas, resultando em perda financeira para a companhia.
SoD03	Executar Ajustes de Remuneração (Promoções e Aumentos Salariais)	ZHCM008, ZHCM009, ZHCM011, ZHRCM004,	Geração dos Arquivos/ Documentos para Pagamento (EDI)	PC00_M37_CDTA, PC00_M37_FFOU, ZBRHR015, PC00_M39_CIPE, ZBRHR_TSAF002	Atualizações não autorizadas da base de pagamentos, seguido do envio indevido para aprovação durante os primeiros passos do EDI, resultando em perda financeira para a companhia.

Fonte: Ernst & Young Digital Insights on Segregation of Duties, 2011

Figura 4. Matriz com as transações que executam as funções

A figura 4 mostra uma lista com os acessos críticos. Elas podem estar ou não atreladas a algum risco. São descritas as transações e as atividades que essa transação permite desempenhar. Isso torna mais fácil o processo de criação dos perfis no SAP.

ACESSO CRÍTICO	
TCODE	DESC
ABAV	Efetuar Baixa de Ativo
AFAB	Lançamento de Depreciação
AL11	Acessar diretório de contas para impressão
AS01	Criar / Modificar / Deletar Registro de Ativo Fixo
AS02	Criar / Modificar / Deletar Registro de Ativo Fixo
AS06	Criar / Modificar / Deletar Registro de Ativo Fixo
BP	Modificar Conta Contrato e Contrato
BUA1	Modificar Conta Contrato e Contrato
CAA1	Modificar Conta Contrato e Contrato
CAA2	Modificar Conta Contrato e Contrato
CJ01	Definição/Modificação de Projetos
CJ02	Definição/Modificação de Projetos
CJ30	Manutenção de Orçamentos de Projeto
CJ32	Aprovar Orçamento
CJ37	Manutenção de Orçamentos de Projeto
CJ38	Manutenção de Orçamentos de Projeto
CJ44	Processamento de Despesas Além do Orçamento
CJ45	Processamento de Despesas Além do Orçamento
CJ46	Processamento de Despesas Além do Orçamento
CJ47	Processamento de Despesas Além do Orçamento
CJ88	Estruturar Projetos
CJ8G	Estruturar Projetos
CJ9BS	Manutenção de Orçamentos de Projeto

Fonte: Ernst & Young Digital Insights, 2011

Figura 5. Lista dos acessos críticos com suas respectivas atividades

3.2. Definição Dos Usuários e Atividades

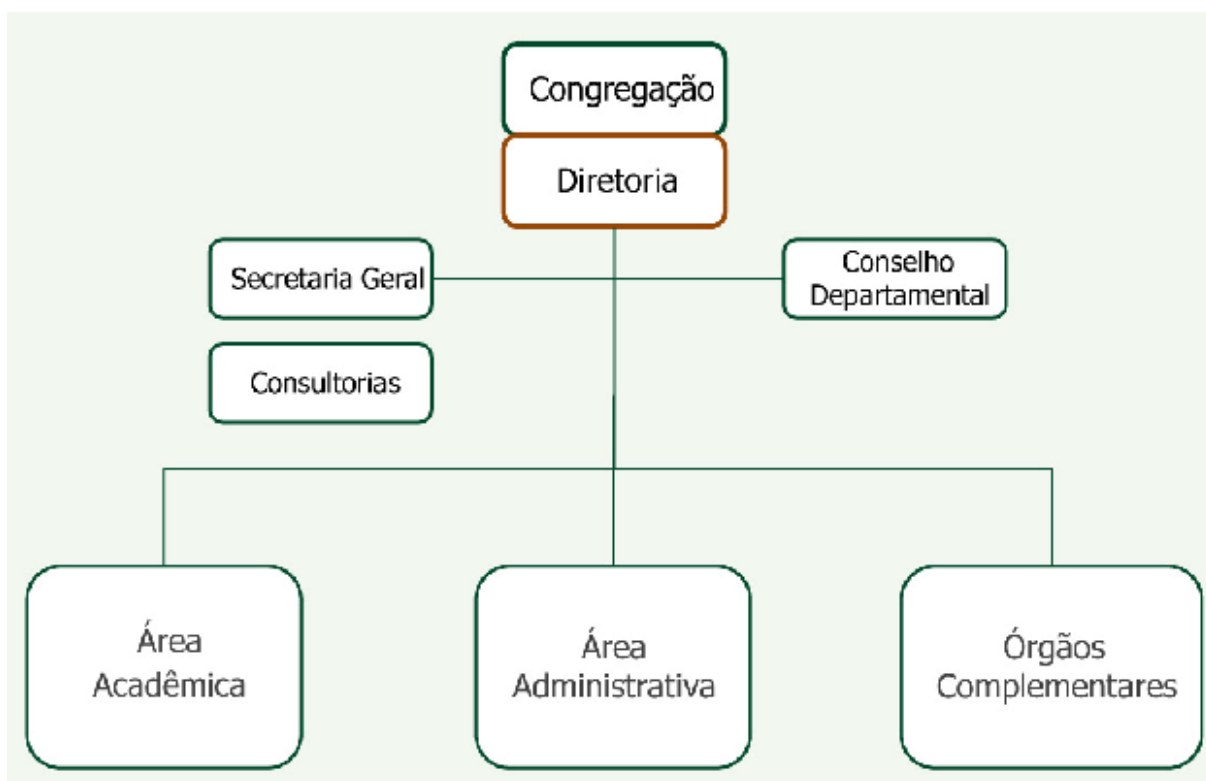
Após definida a matriz de conflitos, é recomendada passar nas áreas novamente e fazer o mapeamento dos usuários que acessam o sistema. Conforme explicado no início do capítulo, somente atuar sobre os perfis que eles possuem atualmente no sistema já solucionaria uma parte do problema, mas em muitas oportunidades os usuários têm perfis em demasia.

Esse processo melhora a qualidade de decisão do gerenciamento certificando-se de que as informações seguras e confiáveis sejam fornecidas e permite racionalizar os recursos de sistemas de informação para atender às estratégias de negócio de forma apropriada (CobIT 4.1).

Os perfis de acesso estão adequadamente construídos, de acordo com o modelo operacional da companhia, de maneira a segregar funções conflitantes e

concedendo apenas os acessos necessários para a execução das atividades de cada colaborador? (Ernst & Young Digital Insights: IT Risk, 2010).

São feitas reuniões com todas as áreas da empresa que participaram das definições de riscos, os *Key Users* de cada uma dessas áreas são responsáveis por identificar quais usuários devem executar cada uma das atividades. Durante essa etapa de designação, o *Key User* já pode ir segregando um pouco as funções, pois já sabe quais atividades foram consideradas críticas e quais as transações mapeadas para a área. Essa identificação das tarefas pode ser feita utilizando como base a estrutura organizacional da área, é só validar se há alguma mudança que deva ser feita. Na figura 6 há o exemplo do organograma de uma área.



Fonte: http://www.medicina.ufmg.br/conheca_fm/imagens/organograma_macro.jpg

Figura 6. Exemplo de um organograma

Os usuários são separados por *Job Positions*. Cada uma delas é representada no SAP por um perfil composto. Os usuários só têm a mesma *Job Position* quando o acesso deles no sistema for idêntico, caso haja diferença em um objeto de autorização já teremos duas *Job Position* diferentes.

É muito importante que as *Job Position* não sejam definidas com os nomes dos cargos que as pessoas têm nas respectivas áreas. Em algumas oportunidades, pode haver um Analista Junior e um Analista Sênior na mesma área, e que ambos sejam responsáveis pela mesma gama de atividades, logo, o acesso deles é idêntico. Caso seja definido que essa *Job Position* será nomeada como “Analista Sênior”, a empresa oferece ao Analista Junior a possibilidade de processá-la futuramente, pois ele está executando atividades que não condizem com o seu cargo, e o seu salário está defasado.

Outro benefício dessa divisão por *Job Position* é percebido quando há a migração de algum funcionário para outra área da empresa, ou quando algum novo empregado que acessará o sistema for contratado, ao invés de pegar vários perfis que já existem no sistema e atribuir a esse usuário. É necessário somente definir as atividades de qual *Job Position* ele é encarregado de executar. Basta atribuir aquele perfil composto a esse usuário.

Após terminar a conclusão do mapeamento, é montada uma planilha, conforme apresentado na figura 7. Após montá-la é feita uma análise nela: primeiramente são identificadas quais as transações críticas que foram solicitadas, e para quais usuários elas foram designadas, depois é somada a quantidade de *Job Position* que a acessam, e isso auxilia a definição de uma lógica para criação no sistema, visando criar o menor número possível de perfis que atendam as atividades da área.

Transação	Descrição	Gestor	Administrativo	Engenheiro	Técnico	Soma	Atividade Crítica
CJ01	Criar plano estrutura projeto			1		1	Definição/Modificação de Projetos
CJ02	MODIFICAR PLANO ESTRUTURA PROJETO		1	1	1	3	Definição/Modificação de Projetos
CJ03	Exibir plano estrutura projeto		1	1		2	
CJ40	Modificar plano de projeto			1		1	
CJ88	APROPR.CST.REAL: PROJETOS/DIAG.REDE			1	1	2	Estruturar Projetos
CJE0	EXECUTAR RELATÓRIO DE HIERARQUIA	1	1	1	1	4	
CJ13	PROJETOS: PART.INDIV.CUSTOS REAIS	1	1	1	1	4	
CJ15	PROJETOS: PART.INDIV.COMPROMISSO		1	1	1	3	
CJ18	PROJETOS: PART.INDIV.ORÇAMENTO		1	1	1	3	
CN22	MODIFICAR DIAGRAMA DE REDE		1	1	1	3	Liberção/Modificação de Diagrama de Rede
CN23	Exibir diagrama de rede		1	1		2	
CN25	CONFIRMAR DIAGRAMA DE REDE		1	1	1	3	
CN27	CONFIRMAÇÃO COLETIVA DE PEPS		1	1	1	3	
CNS42	SÍNTESE: DEFINIÇÃO PROJETO		1	1	1	3	
CNS47	SÍNTESE: TAREFA/ELEMENTOS			1	1	2	
CNS52	Síntese: componentes			1	1	2	
F-65	Entrada preliminar			1		1	Pré-lançamento Documento no GIL
FB03	Exibir documento		1	1		2	
FS10N	Exibição de saldos			1		1	

Fonte: Ernst & Young Digital Insights, 2011

Figura 7. Planilha com o mapeamento de uma área

Existem transações que devem ser comuns a todos os usuários para que não haja problemas iniciais de acesso no SAP. Essas transações ficam em um perfil comum, que é atrelado a todos os usuários.

Há transações de Tecnologia da Informação que muitas vezes não são listadas nos acessos críticos, mas que não devem ser atribuídas a usuários de qualquer outra área. São as transações *Basis*, que englobam atividades ligadas à manutenção de usuários (PFCG, SU01, AL08), manutenção de mandantes (SCC4, SCCL), aplicação de notas (SE37, SE38), aplicação de *request* (SCC1, SE09) e administração de sistema (SM01, AL11 e principalmente a SE16, que verifica todas as tabelas do SAP).

Usuários com acesso direto ao menor nível de segurança devem ser analisados cuidadosamente. Isto representa uma potencial falha de segurança desde que usuários possam ser capazes de ganhar os direitos de acesso sem seguir o processo de administração de usuário padrão (Ernst & Young Digital Insights: Governança e Resultados, 2007).

Convém tomar cuidado nas áreas onde a responsabilidade é de apenas uma pessoa, para que não venham a ser alvo de fraudes que não possam ser detectadas. Recomenda-se que o início de um evento seja separado de sua autorização. É importante segregar atividades que requeiram cumplicidade para a concretização de uma fraude, por exemplo, emitir um pedido de compras e confirmar o seu recebimento. Se existe o perigo de conluíus, então é necessário o planejamento de controles, de modo que duas ou mais pessoas necessitem estar envolvidas, diminuindo dessa forma a possibilidade de conspirações (ISO 27002).

Esse tipo de situação pode ocorrer em empresas onde não há muita gente na força de trabalho ou onde as responsabilidades do departamento são compartilhadas e todo mundo acaba servindo de *back-up* para os outros. Nesses casos, é muito comum achar departamentos em que todos os usuários têm os acessos idênticos, possibilitando que eles executem todos os processos que estão designados àquele departamento.

Essa análise pode detectar os mesmos usuários em diversos conflitos relacionados ao mesmo processo. Caso chegue nesse cenário, a companhia deve colocar uma ênfase especial no uso de controles mitigatórios, conforme será visto ainda nesse capítulo. Essa questão é muito importante para reduzir os encargos da força de trabalho. Muitas vezes, quando um empregado responsável por algum processo chave sai da empresa e não é substituído, as suas funções acabam sendo designadas para outro usuário que já possui algumas atividades sob sua responsabilidade (Ernst & Young Digital Insights: IT Risk, 2010).

Aquilo que antes já apresentava alguma segregação no modelo dos acessos, acaba apresentando uma grande quantidade de conflitos que precisam de controles. Empresas inteligentes avaliam a segregação das funções de acordo com as atividades dos seus usuários e planejam os seus acessos de acordo com o que há à disposição.

O término do processo de mapeamento resulta em uma fonte de registros mestre, que é o primeiro passo no entendimento dos acessos conflitantes no sistema. A fonte de registros mestre é uma visão simples da população de usuários e todos os direitos de acessos associados a eles (Ernst & Young Digital Insight: IT Risk, 2010).

3.3. Criação Dos Perfis

Após todas as definições da matriz, é hora de começar a colocar os dados no sistema. Começa pela criação dos perfis simples, sem que haja qualquer conflito neles. A nomenclatura utilizada nesses perfis é alinhada com os responsáveis da empresa. Também é interessante utilizar a criação de perfis específicos quando há algum nível organizacional nos objetos. As restrições de acesso são definidas nos níveis organizacionais. Separando-as não se faz necessária a criação de um mesmo perfil com transações diversas vezes.

O *SAP BusinessObjects Access Control* oferece um produto específico para criação de perfis no sistema: o *Enterprise Role Management* (ERM), onde os perfis podem ser criados e modificados, e são automaticamente transportados para o *Risk Analysis and Remediation*, para que possa ser feita a análise. Eles também podem ser criados diretamente no SAP, por um processo mais rápido que o do ERM. Basta efetuar a criação pela transação PFCG, como o SAP está ligado ao *Risk Analysis and Remediation*, eles já podem ser analisados logo após a criação.

É recomendável que durante o processo de criação dos perfis eles sejam separados de acordo com o seu nível organizacional, que são os objetos nos quais serão definidas as restrições dos acessos. Caso três usuários distintos utilizem a mesma transação, mas acessem empresas diferentes, por exemplo, eles terão o mesmo perfil de transações, mas cada um terá um perfil específico com os níveis organizacionais definidos. Na nomenclatura deles devemos colocar o final 00 nos perfis de transação e nos perfis de nível organizacional deve ser colocado AA, AB e assim por diante (Isaca Journal: SoD, 2009).

Pode não parecer ter tanta importância essa separação dos níveis organizacionais, mas no caso de uma incorporadora com cinquenta obras, em que há um funcionário diferente que faz o acesso para imputar dados de cada obra, ao invés de criar cinquenta perfis de transações diferentes, é possível criar somente um perfil de transações e outros para os níveis organizacionais, tornando o controle mais prático.

Em muitas oportunidades, há diversos níveis organizacionais nas empresas, com valores que não estão documentados. Foi colocado apenas o valor asterisco * (que permite acessar todos os valores) em alguns objetos, para não manter esse amplo acesso é necessário rastrear os usuários que acessam esse nível organizacional. Esse rastreamento é feito por meio da transação TRACE.

A nomenclatura dos perfis deve conter especificações que permitam identificar a qual área ele pertence. Isso deve ser alinhado com a direção da empresa, pois em muitas oportunidades há perfis semelhantes no sistema, mudando

somente a nomenclatura. Esse processo ocorre para tornar mais fácil e lógica a segregação de conflitos futuramente.

Também é importante que durante a criação dos perfis, sempre que for solicitada alguma transação de criação, seja ela de materiais, ordem de venda etc., os valores para modificação e exibição também devem ser colocados. Durante o período de testes eles serão solicitados e isso já evita esse retrabalho. O contrário não é válido, aqueles que só visualizam devem continuar somente com esse acesso, pois somente visualização não é considerada uma atividade crítica.

Ao definir como é feita a criação dos perfis, mesmo em uma determinada atividade que possibilita criação, modificação e visualização, e que não é considerada crítica, recomenda-se criar um perfil somente com esses acessos, pois caso outro usuário da área necessite dessas atividades, já há um perfil separado (Isaca Journal: SoD, 2009).

Por causa do grande impacto que pode ser decorrente da maneira como os níveis organizacionais são separados, ela só é recomendada nas situações em que a empresa tem plena consciência de como será feita essa etapa. O *Risk Analysis and Remediation Control* elimina os casos de falso positivo baseado nos níveis organizacionais, essa parte é analisada por meio de relatórios extraídos (SAP Education, 2010).

Já há o conhecimento de quais atividades são críticas e quais as transações que permitem executá-las. Os perfis simples são criados, separando todos os conflitos que possam existir. Transações críticas só ficam no mesmo perfil simples caso sejam responsáveis pela execução da mesma atividade. Por exemplo: as transações F-63 (Pré-editar fatura do fornecedor) e F-65 (Entrada Preliminar) normalmente são consideradas como transações críticas, mas, caso um usuário precise de ambas, elas podem ser colocadas em um mesmo perfil, pois a atividade das duas é relacionada ao Pré-lançamento de documentos contábeis.

É necessária também muita atenção às transações de liberação (ME28, ME29, ME54, ME55, ML85, entre outras). É crucial que elas sejam designadas

somente ao gestor da área e só devem ser designadas a outros usuários caso o próprio gestor aprove. Isso deve ser documentado por e-mail, pois é necessário ter uma evidência para ser apresentada à auditoria depois.

Os perfis que fazem parte de atividades críticas serão criados separadamente, como já definimos anteriormente. Ao terminar a criação desses perfis sobram as transações que não foram consideradas críticas na análise feita com os responsáveis pelas áreas. A criação desses perfis deve ser feita de acordo com o tipo de acesso que cada uma das transações possibilita executar. Deve ser criado um perfil para os relatórios, um para as visualizações e assim por diante. É muito importante não exceder o número de quarenta transações por perfil, pois pode acabar ocorrendo algum problema decorrente ao elevado número de transações em um perfil.

Em situações nas quais existem várias transações que não foram consideradas críticas no mapeamento, e cada uma delas foi designada para uma *Job Position*, é recomendável falar com o responsável pela área, para analisar se é possível colocar essas atividades para todos os funcionários, permitindo a criação de somente um perfil no sistema e que é atribuído a todas *Job Position* mapeadas nessa parte.

Perfis sem configuração e modelos de segurança são muitas vezes a fonte de conflitos de segregação de funções. Por exemplo, algumas aplicações estão configuradas para a máxima agilidade e flexibilidade, em outras palavras, qualquer um pode fazer qualquer coisa. Enquanto isso cria um método fácil de utilização e um sistema flexível, ele também pode resultar em controles deficientes, caso os acessos não estejam separados por meio da customização de perfis. Muitas empresas desenvolveram aspectos de segurança nos perfis sem considerar as transações críticas que deveriam ser segregadas. A empresa deve olhar para o menor nível de segurança que compõe uma determinada função para entender quais transações um usuário deve executar. Entretanto, os perfis podem ser aproveitados para uma correta segregação de funções conflitantes, criando um conhecido modelo de perfis efetivos, estabelecendo assim uma aplicação coerente do modelo por meio de

controles de aplicações de segurança. Só esse ajuste no desenho dos perfis já corrige facilmente diversos conflitos, deixando somente os mais difíceis para outras estratégias (Ernst & Young Digital Insights: IT Risk, 2010).

Essa separação torna mais fácil a análise na ferramenta que é feita em uma etapa posterior. Deve-se analisar somente os perfis compostos (*Job Position*) e verificar como estão os acessos críticos neles, pois os conflitos que poderiam existir em perfis simples já foram segregados nessa etapa.

Terminada a criação dos perfis simples é só começar a colocá-los em um perfil composto (que também pode ser chamado de *Job Position*, para facilitar o entendimento nas áreas) e atribuí-los aos usuários de teste. Posteriormente, são esses perfis compostos que são atribuídos aos usuários em produção, substituindo os perfis que eles possuem atualmente no sistema.

Esses perfis e usuários devem ser criados em ambiente de desenvolvimento e depois transportados para um ambiente de testes. Só depois de prontos é que devem ser transportados para produção.

Também é necessário criar os usuários para a equipe que presta o suporte aos testes. Quando os perfis e as regras já estiverem definidas, o perfil que é atribuído a esses usuários já é definido no começo do processo. Esse usuário deve ser criado somente no ambiente de desenvolvimento, impossibilitando que qualquer mudança venha a ser realizada diretamente no ambiente de testes.

É essencial entender quais controles são necessários para administrar o acesso de prestadores de serviços aos recursos de processamento da informação. Geralmente, convém que todos os requisitos de segurança resultantes do acesso de prestadores de serviços ou dos controles internos, sejam refletidos nos contratos firmados com estes (ISO 27002).

Convém que o acesso de prestadores de serviços à informação e aos recursos de processamento da informação, não seja permitido até que os controles

apropriados sejam implementados e um contrato definindo os termos para conexão ou acesso seja assinado (ISO 27002).

As atividades de desenvolvimento e teste podem causar sérios problemas, como por exemplo: modificações não autorizadas total ou parcial de arquivos ou do sistema. Convém que seja avaliado o nível de separação necessário entre o ambiente de produção, de teste e de desenvolvimento, para prevenir problemas operacionais. Convém que uma separação semelhante, também seja implementada entre as funções de desenvolvimento e de teste. Nesse caso, é necessária a existência de um ambiente confiável e estável, no qual possam ser executados os testes e que seja capaz de prevenir o acesso indevido do pessoal de desenvolvimento. A separação dos recursos de desenvolvimento, de testes e operacionais é bastante desejável para a redução do risco de modificação acidental ou acesso não autorizado ao software operacional e dados dos negócios (ISO 27002).

Após a atribuição dos perfis compostos aos usuários de teste, eles já estão prontos para utilização, mas antes será iniciada a utilização do *Risk Analysis and Remediation*.

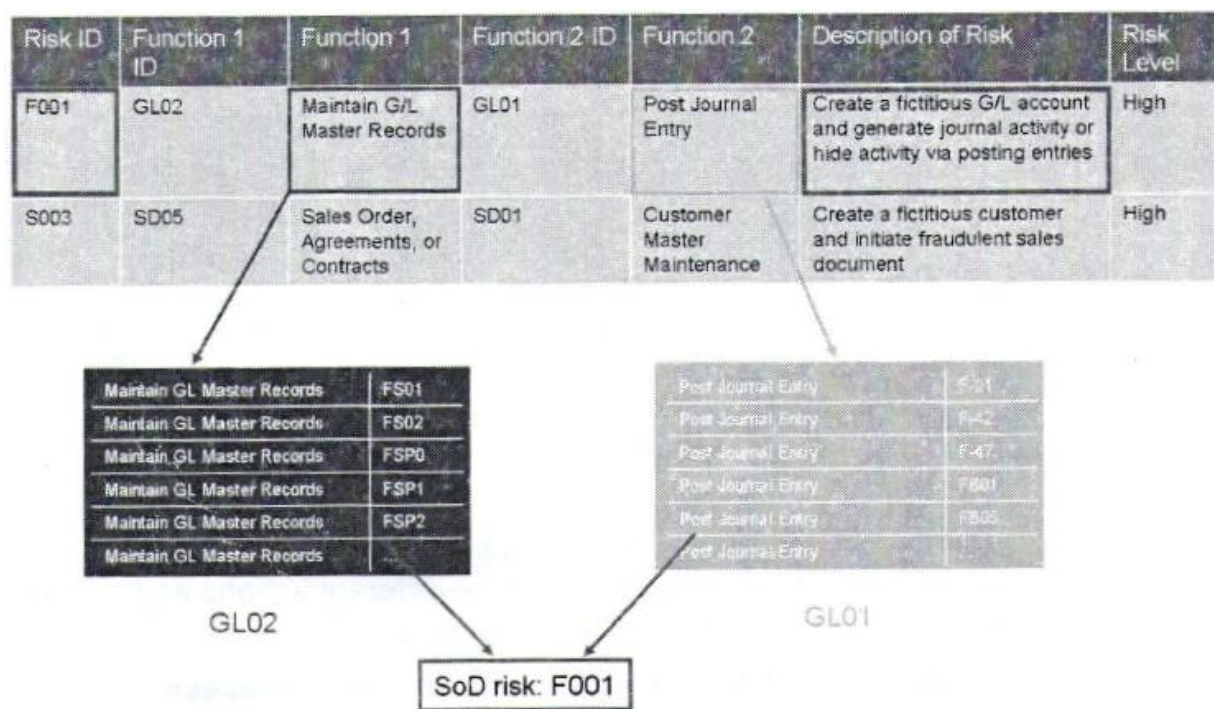
3.4. Criação Das Regras no Sistema

Utilizando a matriz de riscos já definida nas etapas anteriores, inicia-se a criação dos riscos no sistema *Risk Analysis and Remediation Control*.

Primeiro dado colocado nele é referente a qual processo a função está relacionada e, se essa regra é aplicada para todos os usuários do sistema. Isso já cria uma identificação para o risco que é criado. Após isso são criadas as funções referentes ao processo e quais as transações que possibilitam a execução delas.

O *Risk Analysis and Remediation Control* já gera automaticamente as regras para as permutações das diferentes ações e permissões das funções combinadas. A

figura 8 mostra a tela do software em que há o risco e as transações responsáveis pelas atividades. O conjunto de regras entregue providencia uma lista de riscos de segregação de funções, que foi acumulado das melhores práticas, clientes e experiência própria SAP. É necessário conferir se essas regras são aplicáveis para a empresa que está utilizando o software. Isso é somente uma recomendação (SAP Education, 2010).



Fonte: SAP Education, 2010

Figura 8. Documentação dos Riscos no Sistema

Os riscos podem ser definidos de acordo com a transação, pelos valores colocados para os objetos ou até mesmo valores simples que são colocados nos campos dos mesmos. De acordo com a explicação anterior. Na maioria dos casos, é recomendável que uma determinada transação só seja considerada crítica, caso o valor de seus objetos seja um ou dois, que possibilitam criação e modificação no sistema. Conforme visto anteriormente, o valor três não deve ser considerado crítico, pois permite somente a visualização.

É necessário que haja um controle de todas as mudanças que são feitas nas funções e nos riscos. A auditoria solicita a documentação com as mudanças que

foram feitas recentemente nas regras, para que seja possível verificar se o que está implementado é realmente eficiente.

Os relatórios mostram os *logs* de mudanças realizadas para funções e para definição de riscos. Além de mostrar qual usuário foi responsável pela realização dessas mudanças, a possibilidade de saber ou não quem as executou é determinada durante a configuração.

Também há a possibilidade de comparar duas regras, é só colocá-las no sistema e extrair o relatório que possibilita compará-las.

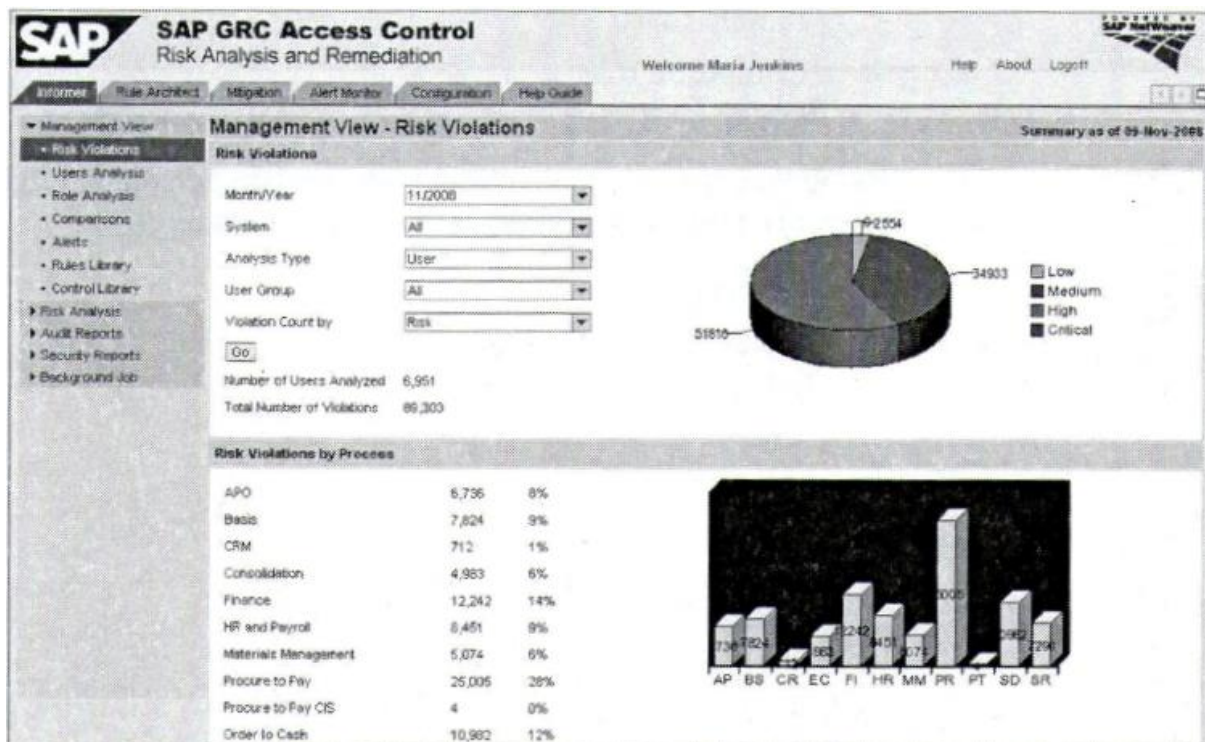
3.5. Análise Dos Riscos

O especialista em lidar com a gestão dos riscos precisa melhorar os processos de verificação dos riscos atualmente no sistema, e estimar o esforço necessário para a limpeza dentro da organização (SAP Education, 2010).

A fase de testes se baseia em dados de definição dos negócios e as fases de definição técnica para produzir uma análise dos usuários com conflitos de segregação de funções. Os resultados destacam os conflitos de segregação de funções em vários aspectos – por usuário e por perfil e (ou) por grupos de usuários – e mostra a extensão dos conflitos entre os usuários da companhia. Essa análise, em combinação com as definições de negócios e técnicas, serve como um pacote de conformidade de testes aberto para a gestão, auditoria e regulamentação (Ernst & Young Digital Insights: IT Risk, 2010).

A análise pode ser feita por perfis simples, compostos ou por usuário. Como os perfis simples já foram construídos de modo a separar os possíveis conflitos, e cada usuário está atrelado a um perfil composto (*Job Position*), só é necessário fazer uma avaliação: a do perfil composto que foi atribuído ao usuário.

A visão gerencial na aba *Informer* do *Risk Analysis and Remediation* mostra de maneira compacta os riscos de violação agrupados pelo tempo em que foram extraídos, grau de severidade e referentes aos processos de negócios, uma tela semelhante a que é mostrada na figura 9 (SAP Education, 2010).



Fonte: SAP Education, 2010

Figura 9. Visão dos Riscos no Risk Analysis and Remediation

O relatório por violações de segregação de funções apresenta duas visões: a quantidade de violações pelo nível dos riscos e outra pelos processos. O relatório de usuário também pode ser extraído com duas visões: uma mostrando todos os casos de conflitos na segregação de funções que há nele, e outra que apresenta os acessos críticos que esse usuário possui.

Também é possível extrair relatórios que mostram como anda o processo de remediação dos conflitos, passo que será explanado posteriormente, mostrando quantos casos de um determinado conflito havia em um mês e quantos há no mês seguinte e também qual o percentual de evolução houve na remediação daquele caso (SAP Education, 2010).

Com esses relatórios, a empresa tem conhecimento de como está a situação da segregação de funções de acordo com o mapeamento de usuários e a definição dos riscos que foi feita. Próximo passo é a ação tomada em cima desses dados, visando reduzir ao menor número possível os conflitos no sistema.

É interessante selecionar no ambiente de desenvolvimento todos os perfis que há no sistema atualmente (caso eles estejam idênticos aos de produção), excluindo os perfis atrelados para os usuários de teste e rodar esses relatórios para eles. Após obter os dados, fazer as comparações do sistema atualmente e do sistema de acordo com o mapeamento, visando aspectos como: quantidade de perfis no sistema, quantidade de perfis que apresentam conflitos de segregação de funções, usuários com conflitos e quantidade de conflitos por usuários em média. Só essa primeira comparação já mostrará a discrepância de valores, após as últimas etapas do processo essa diferença será ainda maior.

Pode-se executar remediação e mitigação dos conflitos. Elas podem ser feitas em qualquer ordem, mas com o uso do *Risk Analysis and Remediation Control* é mais fácil que o primeiro passo seja a remediação, para que depois seja realizada a mitigação somente com os riscos reduzidos ao menor número possível (SAP Education, 2010).

A fase de mitigação pode ser concluída junto com a fase de remediação; ou dependendo dos objetivos e prazo para o cumprimento, a mitigação pode ser feita depois, quando os riscos já estiverem bem reduzidos (Ernst & Young Digital Insights:IT Risk, 2010).

Convém que a política de análise crítica e avaliação seja responsável por sua manutenção e análise crítica, de acordo com um processo definido. Convém que esse processo garanta que a análise crítica ocorra como decorrência de qualquer mudança que venha a afetar a avaliação de risco original, tais como um incidente de segurança significativo, novas vulnerabilidades ou mudanças organizacionais ou na infraestrutura técnica (ISO 27002).

3.6. Remediação Dos Riscos

Para alcançar um bom resultado no processo de segregação de funções da organização, é necessário reestruturar os direitos de acesso no SAP. A simulação das funcionalidades no *SAP BusinessObjects Access Control* faz com que isso seja fácil a verificação de perfis e os conceitos de autorização (SAP Education, 2010).

O propósito da fase de remediação é determinar alternativas para eliminar os problemas relacionados aos perfis. Um plano de remediação deve ser documentado pelos administradores de segurança (SAP Education, 2010).

O objetivo da fase de remediação é a correção permanente dos conflitos de segregação de funções. As técnicas para a segregação de funções envolvem: um redesenho dos perfis com transações conflitantes, limpeza dos perfis, readequação dos usuários e implementação de ferramentas para o controle da segregação de funções. Uma combinação de pessoas, processos e mudanças tecnológicas ajudam a sustentar um controle efetivo e as conformidades. Não há nenhuma prática pré-definida ou método para remediar os conflitos. Cada cenário é único, baseado no grau de complexidade e na extensão dos conflitos em cada ambiente (Isaca Journal: SoD, 2009).

Investimento na remediação atingindo pessoas, processos e tecnologia que regem o processo de segregação de funções podem, potencialmente, produzir redução de riscos para o negócio, menor incidência de recursos de controle, não ocorrência de multas regulamentares, economia nas horas de consultores e um melhor controle do ambiente (Isaca Journal SoD, 2009).

As iniciativas de remediação geralmente caem em duas categorias: uma limpeza tática dos acessos de usuários e um redesenho estratégico de perfis. O componente tático representa os itens que podem ser abordados rapidamente, enquanto o desenvolvimento de perfis tipicamente envolve um conjunto completo de mudanças em pessoas, processos e tecnologia. A escolha de caminhos táticos ou estratégicos não obriga a empresa a escolher somente um deles, muitas

companhias acabam escolhendo os dois, que são executados em prazos definidos (Ernst & Young Digital Insights: IT Risk, 2010).

O mapeamento feito para definir quais as *Job Positions* de cada um dos usuários de uma área, auxilia muito nessa etapa. Com a criação dos perfis de acordo com os acessos que eles devem ter, não há o risco de que haja atividade atrelada aos usuários que não deveriam realizá-las.

Outro benefício do mapeamento dos acessos é que o *Key User* responsável por informar as atividades de cada um dos usuários é o mesmo que define quais são as medidas tomadas para remediar os conflitos. Com o documento gerado após o mapeamento ele já tem uma visão clara de como funciona a sua área e de qual maneira ele pode proceder para mudança de alguns acessos.

O primeiro passo é analisar os relatórios extraídos do sistema, que mostram qual a extensão dos conflitos e os esforços necessários para remediá-los, depois definir qual metodologia utilizar especificamente naquela violação.

3.6.1. LIMPEZA TÁTICA DOS ACESSOS

Limpeza tática dos acessos dos usuários é referente ao processo de revisão dos perfis ou modelo de segurança, para avaliar se ambos os lados das transações conflitantes são necessárias para que o usuário execute seu trabalho. Esse processo de limpeza requer que a companhia faça a análise dos perfis com conflitos entre eles, para que seja definido se será excluída alguma transação neles (Ernst & Young Digital Insights: IT Risk, 2010).

3.6.2. REDESENHO ESTRATÉGICO DE PERFIS

Em alguns casos, as transações são vitais para a área e devem ser separadas para que não sejam executadas pelo mesmo usuário. Isso ocorre nessa etapa de redesenho estratégico de perfis. Uma atividade designada para um usuário é colocada para um outro, para eliminar o conflito existente (Ernst & Young Digital Insights: IT Risk, 2010).

3.7. Remediação No Sistema

Após definir quais as medidas tomadas é só passá-las ao sistema. Há diversas possibilidades como:

3.7.1. EXCLUSÃO DA TRANSAÇÃO

Se a transação for excluída do perfil, todos os usuários que a acessam perdem esse acesso. Em muitas oportunidades a transação está causando conflitos para alguns usuários, mas não para outros.

A transação deve ser excluída de um perfil somente após a análise completa de todos os usuários que possuem esse acesso. Caso nenhum deles precise mesmo da transação, ela pode ser excluída. Caso contrário, deve-se criar um novo perfil no sistema, excluindo a transação selecionada e colocá-lo para esses usuários que apresentavam conflito (SAP Education, 2010).

Quando os perfis foram criados no sistema, a nomenclatura atribuída visava facilitar justamente essa parte do processo. A análise dos perfis será restrita somente à área em que foi identificado o conflito.

Caso seja necessário criar novos perfis, é preciso verificar quais *Job Positions* sofrem mudanças. Pois uma diferença no acesso já caracteriza um novo perfil composto. Com a mudança aplicada, é necessária a criação de, ao menos, uma

nova *Job Position* no sistema (Ernst & Young Digital Insights: Governança e Resultados, 2007).

3.7.2. EXCLUSÃO DO PERFIL

Como os perfis com atividades críticas são criados separados do resto, em alguns casos o perfil terá somente uma transação, eliminando a transação o perfil também será eliminado. Em outros casos, pode haver várias transações responsáveis pela execução de uma mesma atividade. Deve-se analisar se ela será ou não excluída desse perfil, sempre lembrando que qualquer diferença nos acessos já gera uma nova *Job Position*.

3.7.3. MUDANÇA NOS VALORES DOS OBJETOS

É possível corrigir alguns casos de conflitos na segregação de funções somente modificando os valores dos objetos. Caso a análise mostre que o usuário não precisa dos valores que lhe permitam criar ou modificar em uma determinada atividade, é só ir ao sistema e excluí-las, deixando somente o valor de visualização. Assim o risco terá sido resolvido.

Os valores de objeto podem variar de acordo com o nível organizacional também. Não é muito comum a ocorrência desse tipo de conflito, mas se for definido que algum acesso em específico é crítico, ele será acusado quando forem tirados os relatórios. Então, é possível retirar o acesso ao nível organizacional, mas é mais fácil a criação de controles para documentar o acesso a ele.

3.7.4. MUDANÇA NOS USUÁRIOS DEMITIDOS

Embora usuários expirados e demitidos ainda estejam no domínio de acessos lógicos, examinar a lista de usuários demitidos nas listas de Recursos Humanos é fundamental. Esse passo reduz o número de usuários para analisar futuramente,

pois estabelece a população de usuários que serve de base para analisar os conflitos na segregação de funções, podendo ajudar a reduzir os custos de licença (Ernst & Young Digital Insight: IT Risk, 2010).

3.8. Mitigação Dos Riscos

Após executar o processo de remediação, boa parte dos conflitos que existiam já estão resolvidos. Mas se ainda há alguns, eles passam pela última etapa do processo, a fase de mitigação.

Devido às restrições organizacionais, nem todos os riscos podem ser evitados por meio das atividades de remediação. Como consequência, é necessário encontrar controles mitigatórios para tratar adequadamente os riscos remanescentes. Eles são requeridos quando não é possível segregar as funções somente com os processos de negócio (SAP Education, 2010).

Pode ser necessário que o processo de seleção dos controles, seja executado um determinado número de vezes, para proteger as diferentes partes da organização ou sistemas de informação isolados (ISO 27002).

Mitigação olha para cada um dos conflitos de segregação de funções identificados e pergunta: “qual o controle que está em operação para reduzir o risco residual de um determinado caso de conflito na segregação de funções, de modo que isso não represente uma ameaça significativa para os negócios?” Em outras palavras, a empresa pode identificar algum controle existente que sirva para prevenir ou detectar atividades não autorizadas ou fraudulentas? (Ernst & Young Digital Insights: IT Risk, 2010).

Os controles são considerados otimizados quando a direção estabelece um programa corporativo de melhoria contínua que leva em consideração as lições aprendidas e as melhores práticas de monitoramento dos controles internos. A organização utiliza ferramentas integradas e atualizadas, quando apropriado, que

permite a efetiva avaliação dos controles críticos de TI e a rápida detecção dos incidentes de monitoramento dos controles de TI (CobIT 4.1).

Mitigação não resolve ou corrige o conflito; em vez disso, ela permite que o conflito exista no sistema e cria ou cita controles existentes que compensam o acesso excessivo aos riscos. Quando a empresa opta por mitigar um conflito de segregação de funções, ela aceita o risco associado com aquele conflito e tenta compensar, por meio da utilização de aplicações, dependências de Tecnologia da Informação ou controles manuais (ou combinações dos mesmos). (Ernst & Young Digital Insights: IT Risk, 2010).

Os controles servem para que haja registro de todas as atividades no sistema. Mesmo no caso da ocorrência de alguma fraude, ela está com suas evidências lá. Essas informações possibilitam que a empresa possa processar quem agiu de má fé e ter provas para isso. Lembrando que sempre aquele que está acusando deve apresentar provas para incriminar o acusado, que precisa apenas provar sua inocência no caso.

Por exemplo: em um escritório, uma pessoa precisa executar duas atividades do processo de negócio, que causam um conflito de segregação de funções. Há diversos tipos de controles mitigatórios que podem ser colocados em prática. Eles se dividem em:

3.8.1. CONTROLES PREVENTIVOS

Minimiza a probabilidade ou o impacto de um risco antes que ele eventualmente ocorra. Configurações, customização de objetos, saídas de usuário, segurança e fluxo de trabalho são exemplos de controles preventivos (Isaca Journal: SoD, 2009).

3.8.2. CONTROLES DETECTIVOS

Alerta quando o risco ocorre e permite que a pessoa responsável inicie as medidas corretivas. Relatórios de atividades, revisão orçamental, revisão do planejado com o atual, logs técnicos e alertas são exemplos de controles detectivos (Isaca Journal: SoD, 2009).

Quando alavancar os controles mitigatórios, a gestão deve desenvolver uma análise que passe por cada conflito para documentar a existência de determinados controles-chave que mitigam o risco relacionado com aquele conflito em particular. Gestão e os auditores podem avaliar a força dos controles mitigatórios e concluir o nível apropriado de confiança para ser colocado nos controles, para gerir os riscos em um nível aceitável. Este aspecto importante da abordagem dos riscos permite à gestão aceitar que certos conflitos existam com seus níveis toleráveis pré-definidos de riscos, determinando assim o limiar de risco residual (Isaca Journal: SoD, 2009).

Convém que os controles sejam selecionados e implementados para assegurar que os riscos são reduzidos a um nível aceitável. Os controles podem ser selecionados a partir de um conjunto de controles. Ou novos controles podem ser desenvolvidos para atender às necessidades específicas, quando apropriado. Convém que os controles sejam selecionados baseados nos custos de implementação em relação aos riscos que são reduzidos e as perdas potenciais se as falhas na segurança ocorrerem (ISO 27002).

Não há só um controle que pode resolver um risco. Programar um balanço de controles preventivos e detectivos ajuda a gerenciar os riscos caso algum controle falhe e auxilia o uso de abordagens baseadas no risco. Enquanto não há um número ideal de controles, uma boa regra é: melhor ter um controle bem desenvolvido do que dez que não resolvem o problema para o risco do conflito (Ernst & Young Digital Insights: IT Risk, 2010).

É necessário assegurar que os controles de Tecnologia da Informação estejam atualizados assim que se faça uma modificação, para corresponder às alterações realizadas nos controles internos ou nos processos de elaboração de

demonstrações financeiras e monitorar permanentemente a eficácia desses controles (Isaca Journal: SoD, 2009).

A matriz de conflitos deve documentar de maneira precisa porque cada controle mitiga um risco específico dos conflitos. Essa documentação permite que a gestão lide com os riscos de modo mais eficaz e serve como uma maneira de justificar para os auditores como esses controles mitigam os conflitos de segregação de funções.

3.9. Controles Mitigatórios No Sistema

Primeiro passo é definir os responsáveis por cada etapa dos controles mitigatórios e quais atividades serão controladas. O controle é aprovado e há a definição de como ele é monitorado e qual o responsável pelo monitoramento. É necessário garantir que os monitores executem os controles na periodicidade definida. Eles devem também realizar as ações identificadas no controle para identificar aquelas que são inapropriadas (SAP Education, 2010).

Próximo passo é criar uma unidade de negócio e designar monitores para cada uma. Depois disso é criado o controle. O passo mais fácil para criá-lo no sistema é especificar um ID, usando a área de negócio, usuário ou perfil e uma sequência numérica. A nomenclatura dos riscos deve ser definida junto com os responsáveis da empresa, à mesma maneira como foi executada a definição para nomear os perfis que foram criados no sistema.

Após definir o ID do controle no sistema é definido a sua descrição e qual o objetivo desse controle, respondendo às perguntas: quem, por que, o que e com que frequência na definição. Atribuir a uma área de negócio e um dos aprovadores que foram designados no sistema anteriormente. Assim, saberemos quais áreas estão englobadas naquele controle mitigatório e os funcionários responsáveis por aprová-la.

Depois que o controle foi aprovado e está sendo executado, é necessário que ele seja monitorado. O responsável pela aprovação do controle em uma determinada área designa qual funcionário é responsável por monitorar cada um dos controles que foram designados àquela área. Ele define quem extrai cada um dos relatórios e com que frequência esse procedimento de controle deve ser executado.

Alertas também podem ser criados como controles mitigatórios temporários. Esses usuários podem acusar quais usuários estão acessando diversas atividades conflitantes. Ele ajuda a garantir a eficácia dos controles mostrando atrasos nos relatórios iniciais.

Os alertas são programados para avisar o acesso a alguma atividade crítica no sistema, fazendo com que o responsável por aquele risco receba um e-mail ou alguma outra notificação sempre que alguém acessar. Os monitores podem solicitar que alertas sejam programados de acordo com suas necessidades para execução do trabalho.

3.10. Testes

Após terminar os processos de remediação e mitigação, os perfis que precisam ser testados já estão prontos para o transporte ao ambiente de testes. Deve ser definido com a gerência da empresa quais usuários serão testados por cada funcionário. Caso quatro usuários tenham a mesma *Job Position* não é necessário que todos executem os testes, inclusive, há casos em que o gestor da área prefere fazer os testes de todos os usuários para validar se está tudo conforme o mapeado.

A empresa deve providenciar um e-mail para a equipe de suporte e informá-lo a todos os funcionários que fazem os testes. É enviado a cada um deles um Plano de Testes, contendo todas as transações que eles devem testar, separados pelo perfil em que elas estão. Conforme executam os testes eles marcam se foram aprovadas ou se deu algum erro.

TERMO DE HOMOLOGAÇÃO DOS PERFIS DE ACESSO

Departamento	Aprovador 1	Aprovador 2
BEN - Benefícios	Fernanda Gomes	

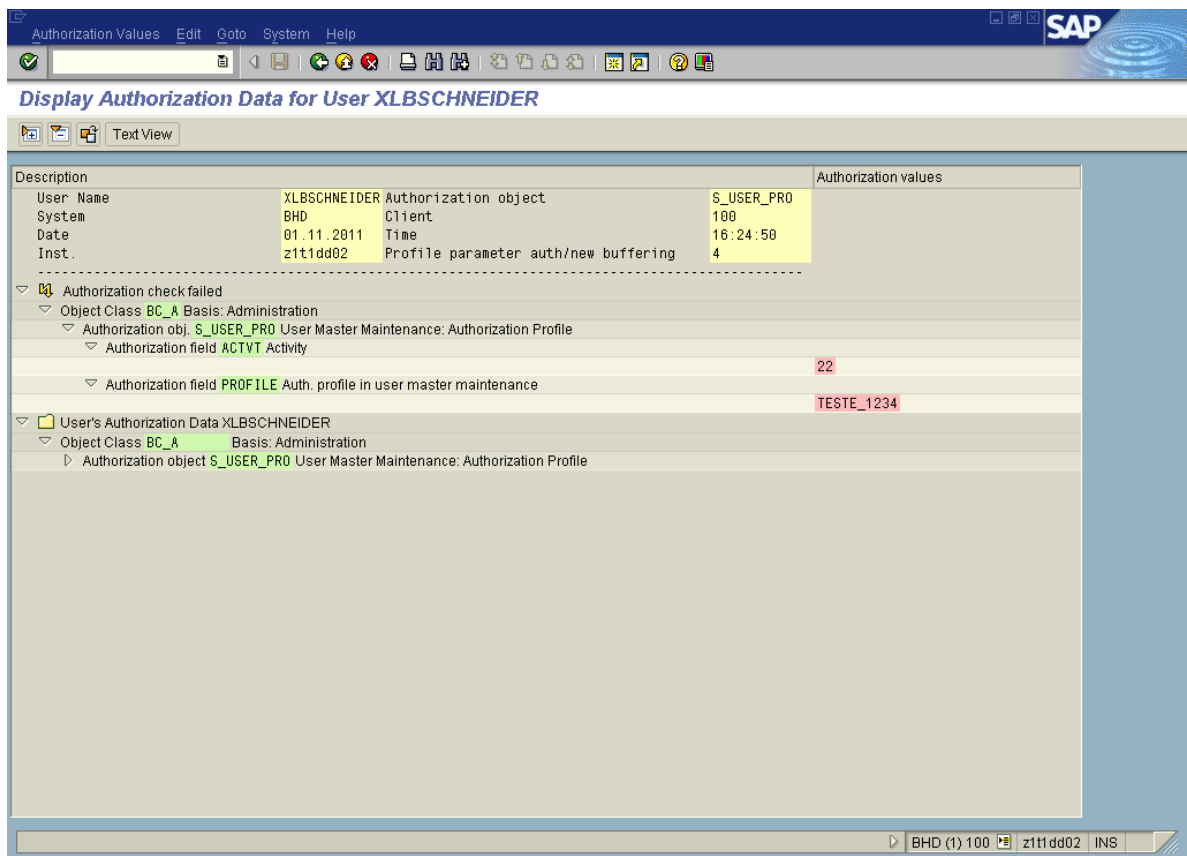
Perfil	Descrição	Usuário de teste	Senha
ZAMERRHRSBES_BEN_GERAL_00	Benefícios - Perfil Geral	EYT01	

Transações	Descrição	Status 1	Status 2	Status 3	Status 5
PA20	Exibir dados mestre HR	OK			
PC_PAYRESULT	Exib.resultados cálculo flh.pgto.	OK			
PC00_M37_CALC_SIMU	Simulation payroll accounting	RP	RP	OK	
PC00_M37_CEDT	Folhas de Pagamento	NT			
PC00_M99_CwTR	Programa rubricas salariais	RP	OK		
S_PH0_48000510	Ad hoc query	OK			
SM37	Síntese da seleção de jobs	OK			
SOST	SAPconnect ordens de envio	OK			
ZBRHR_RE_001	Período Contábil Reembolso Exp.	EX			

Fonte: Ernst & Young Digital Insights on Segregation of Duties, 2011

Figura 10. Plano de Testes

Caso haja algum problema na execução das atividades os usuários devem executar a transação SU53 (análise da verificação de autorização), que deve estar no perfil geral. Tirar um *print screen* dessa tela de erro, igual a tela apresentada na figura 11, e enviar para o e-mail da equipe de suporte, para que ele possa ser resolvido. É necessário definir o período de testes e quanto tempo um acesso deve demorar a ser corrigido. Todas as correções devem, sem exceção, ser feitas no ambiente de desenvolvimento e transportadas para o de testes, caso contrário, já terá divergências nos ambientes ao fim desses testes.



Fonte: http://abapbrasil.files.wordpress.com/2010/04/clip_image0043.jpg

Figura 11. Tela da transação SU53

A solicitação pode envolver um valor de objeto, um programa ou até mesmo a inclusão de uma transação. Caso seja algum acesso considerado crítico, é necessário que o *key user* da área aprove a inclusão do valor solicitado. Com a aprovação do ponto focal, deve ser simulada a inclusão do valor para a *Job Position*. Caso apareça algum conflito novo por causa disso, todo processo de remediação e mitigação deve ser discutido com a área para que seja definido o que é feito com esse acesso.

3.11. Go-Live

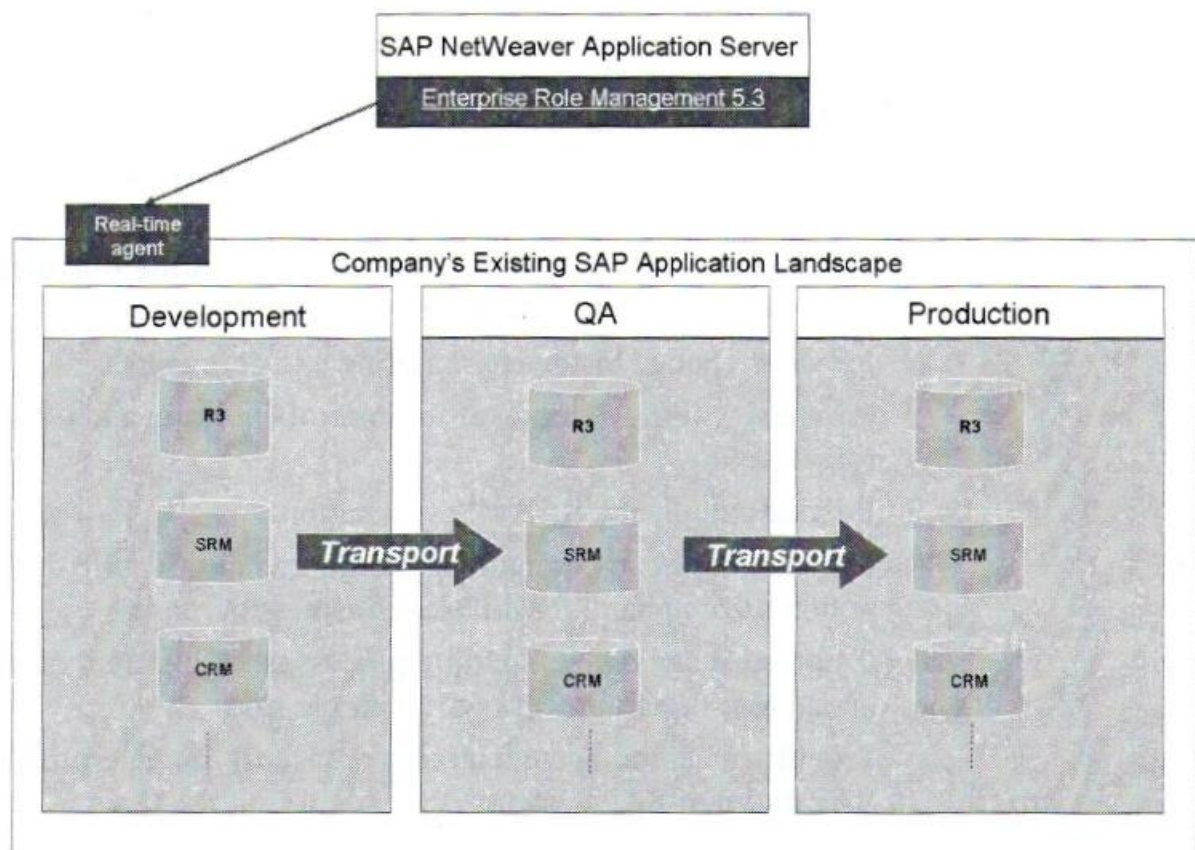
Após todas as alterações e aprovações dos planos de testes está tudo pronto para ser passado ao ambiente de produção. É definido junto aos responsáveis da empresa quais as melhores datas para subir os perfis ao ambiente produtivo. Recomenda-se sempre segregar as áreas e as *Job Position*, para que cada dia suba

um ou dois usuários de uma área e os outros continuem com seus acessos normais, assim, caso haja algum problema isso não impacta nas atividades.

O tempo que a equipe deve prestar suporte também é definido no início do processo, conforme explicado no início desse capítulo. Assim que acabar o período de suporte, a empresa deve ter uma equipe direcionada para atender esses casos de solicitação de acesso. É fundamental que durante o *GO-live* todas as mudanças solicitadas e aprovadas sejam feitas no ambiente de desenvolvimento e transportadas. Os ambientes devem estar semelhantes.

A separação dos ambientes de desenvolvimento, teste e produção é importante para se alcançar a segregação de funções envolvidas. Convém que as regras para a transferência de software em desenvolvimento para produção sejam bem definidas e documentadas (ISO 27002).

A figura 12 apresenta uma lógica para o fluxo de transporte pelos ambientes no SAP.



Fonte: SAP Education, 2010

Figura 22. Transporte pelos ambientes do SAP

3.12. Manutenção Das Conformidades

A organização planeja garantir a manutenção das conformidades. A fim de alcançar um crescimento rápido, pretende avaliar o *Risk Terminator* como uma medida possível para aumentar a consciência dos riscos no desenvolvimento dos perfis e no processo de atribuição aos usuários, assim como para forçar uma melhor documentação das razões para ativar as atividades críticas dentro do sistema (SAP Education, 2010).

A gestão eficaz de desempenho de TI exige um processo de monitoramento. Esse processo inclui a definição de indicadores de desempenho relevantes, informes de desempenho sistemáticos e oportunos e uma pronta ação em relação aos desvios encontrados. O monitoramento é necessário para assegurar que as

atividades corretas estejam sendo feitas e que estejam em alinhamento com as políticas e diretrizes estabelecidas (CobIT 4.1).

O *Risk Terminator* deve ser configurado. Para isso basta acessar a transação /n/VIRSA/ZRTCNFG e configurar os itens desejados.

Na primeira configuração é só colocar que ele será conectado com o *Risk Analysis and Remediation*. Na segunda é confirmada a utilização de RFC, que permite ao *Risk Terminator* fazer as análises quando ocorre a mudança de algum dado mestre de usuário. Logo após é configurado o *plugin* com a transação PFCG, ele possibilita que todas as mudanças feitas por meio dessa transação sejam analisadas, tanto mudanças feitas nos perfis quanto na atribuição deles aos usuários. Após isso são habilitados os *plugins* para as transações SU01 e SU10, que possibilitam analisar os perfis dos usuários que foram mudados por meio dessas transações e analisar os seus conflitos. A SU01 para usuários específicos e SU10 para usuários em massa. Por fim, é possível solicitar que seja interrompida a criação de perfis caso haja algum conflito de segregação de funções e o usuário é obrigado a colocar um comentário explicando porque aquilo está sendo feito.

Para manter controle efetivo sobre o acesso aos dados e serviços de informação, convém que o gestor conduza em intervalos regulares de tempo um processo formal de análise crítica dos direitos de acessos dos usuários (ISO 27002).

Após todas as configurações essa parte do processo está terminada. Agora o sistema está de acordo, os riscos foram segregados em sua grande maioria e os que sobraram estão sendo controlados. As ferramentas estão configuradas para prestar o suporte necessário, e é só manter o procedimento e continuar normalmente os trabalhos.

A governança de TI pode ser considerada otimizada quando há um entendimento avançado, que aponta para o futuro, das questões voltadas à governança de TI e suas soluções. Os processos têm sido bem refinados, no nível das melhores práticas do seu segmento de indústria, a partir dos resultados do

aprimoramento contínuo e da modelagem de maturidade. Todos os problemas e desvios têm sua causa raiz analisados, e ações eficientes são sistematicamente identificadas e executadas. A TI é utilizada de forma otimizada, integrada e extensiva para automatizar o fluxo de trabalho e disponibilizar ferramentas para a qualidade e efetividade. Os riscos e retornos dos processos de TI são definidos e balanceados. As atividades de governança de TI são integradas ao processo de governança corporativa (CobIT 4.1).

3.13. Considerações Finais

Sempre existirão conflitos de segregação de funções nos sistemas utilizados pelas empresas. Deve ser feito o máximo possível para evitá-los, mas sempre há a possibilidade de que dois usuários responsáveis por uma determinada atividade possam agir em conluio e concretizar uma fraude. Caso ela ocorra é necessário que isso esteja registrado no sistema para que ambos possam ser identificados.

Qualquer novo processo que seja criado, assim que for colocado no sistema, provavelmente apresenta algum conflito de segregação de funções. Assim que houver conhecimento de como esse processo é feito no sistema, é possível notar as atividades conflitantes e determinar se as funções são segregadas entre alguns usuários ou se há controles.

Segregação de funções continua a ser uma parte integrante dos controles internos de uma empresa. Enquanto o nível apropriado de necessidades de esforço e ênfase necessita ser colocada no cumprimento das segregações de funções, as empresas também devem continuar a lutar pela simplicidade e precisão na execução dos seus controles. A segregação de funções apresenta um desafio único para o cumprimento dos controles, uma vez que requer um estreito alinhamento dos negócios e dos *stakeholders* para avaliar, mitigar, reduzir e monitorar os riscos de fraude ou inexatidão dos materiais (Ernst & Young Digital Insights: IT Risk, 2010).

Gastar dinheiro em aplicações e ferramentas por si só não vai resolver um processo ineficiente. À mesma maneira, esperar melhoria ao longo do tempo sem um foco contínuo nos riscos que estão sendo abordados ou nos valores que estão sendo protegidos não é uma conformidade sustentável ou uma estratégia de Tecnologia da Informação. A gestão deve dar um passo atrás e perguntar o que a empresa está tentando realizar por meio dessa segregação de funções. Uma iniciativa de segregação de funções baseada em riscos pode permitir o cumprimento e também demonstrar o real valor do negócio reforçando os controles enquanto melhora, agiliza e redesenha de maneira eficiente os processos chaves e os processos de TI (Ernst & Young Digital Insights: IT Risk, 2010).

Esse processo traz benefícios para diversas áreas da empresa. Por exemplo, a área de negócios terá um processo padronizado para que sejam concedidos os acessos dos usuários ao SAP e suas respectivas aprovações. Para a área de controles internos e auditoria há um maior nível de controle nos acessos ao sistema, pois já estão definidas as Job Position e as regras de segregação de funções também já estão documentadas. As áreas de TI e de Segurança da Informação também se beneficiam, pois o número de perfis existentes no sistema diminui muito, facilitando sua administração e revisão.

Conseguir padronizar o ambiente de TI é um passo muito importante para que a empresa obtenha êxito em seu ramo de atividade. O SAP BusinessObjects Access Control ainda possibilita uma grande facilidade na extração de relatórios mostrando como estão os riscos no sistema, acessos dos usuários, perfis compostos, entre outros.

Investir nesse processo faz com que a empresa esteja preparada para crescer nos próximos anos. Novas atividades que a empresa passa a fazer e que são executadas no SAP facilmente estão documentadas no sistema, assim como os seus riscos e quais usuários possuem esses acessos.

Para finalizar, a tabela 1 apresenta uma descrição das principais atividades e vocábulos relacionados ao processo de segregação de funções.

Tabela 1. Descrição das Principais Atividades Relacionadas ao Processo

Atividade	Descrição
Mapeamento	Coletar todos os dados referentes aos acessos feitos pela área
Job Position	Perfil composto(formado por dois ou mais perfis simples), condizente com as atividades desempenhadas por um determinado usuário, pode haver mais de um usuário em uma Job Position. Caso haja uma transação diferente no perfil composto, já é necessário criar outra Job Position
Transações	Códigos que permitem ao usuário desempenhar determinadas atividades no sistema SAP, trasações são compostas de objetos e formam perfis simples.
Matriz de Riscos	Matriz definida junto ao cliente de quais processos feitos pela empresa estão sujeitos a ocorrência de fraudes. Isso define quais atividades são separadas quando os perfis simples forem criados
Período de Testes	Período no qual os perfis definidos são testados em ambiente de qualidade, para que possa ser corrigido qualquer erro existente, teste não é feito em produção para não impactar diretamente nas atividades dos funcionários
Go-Live	Momento em que os perfis já foram testados e são colocados no ambiente produtivo, podem ocorrer novas requisições de acesso, por isso é necessário escalonar bem quando os perfis sobem e sempre ter alguém para prestar suporte.
SoD (segregation of duties)	Separação de duas funções que são consideradas conflitantes na matriz de riscos. Ideal é que cada uma delas seja executada por uma Job Position diferente ou que haja algum controle para documentar caso não seja possível separá-las.
Lei SOX	Lei aprovada em 2002 nos E.U.A., ela definiu as diretrizes para a definição dos conflitos nos sistemas e sua respectiva separação. Com as diversas fraudes que ocorreram, era necessário fazer com que o mercado voltasse a acreditar nas empresas, então essa lei foi aprovada.

CONCLUSÃO

O trabalho explica os procedimentos para realizar a segregação de funções no sistema SAP das empresas, com a utilização do GRC Access Control para auxiliar no processo. Foram descritas, de maneira geral, todas as etapas relacionadas a ele. De acordo com o que foi descrito no primeiro capítulo, a Lei SOX define que um dos principais objetivos da governança de TI nas empresas é garantir que as atividades críticas sejam segregadas entre os usuários de uma determinada área e controles sejam definidos para assegurar que essa segregação realmente ocorra, conforme foi explicado no terceiro capítulo. O ambiente de TI nas empresas deve adequar-se às necessidades identificadas para que isso seja realizado. Garantir a eliminação das possibilidades de fraudes, ou, na pior das hipóteses, que haja uma documentação de tudo que foi feito, é o principal objetivo desse processo.

A pesquisa foi baseada nas situações encontradas nas empresas que utilizam o software e cuidam do processo e documentação da segregação das funções no sistema. Todas as empresas que aderem a esse processo obtêm êxito com o passar do tempo, sempre aperfeiçoando os controles, os testando e garantindo que estão adequados às funções pelas quais são responsáveis no sistema. Simular os controles no ambiente de testes é primordial para que não ocorram problemas quando eles estiverem no ambiente produtivo. A empresa que passa por esse processo objetiva um ambiente produtivo seguro em relação às fraudes, por isso, é fundamental ter a consciência de que a implementação dos controles pode ser considerada cara, mas deixar o sistema passivo de fraudes é algo pior.

Com a implementação do *Risk Analysis and Remediation* e das ferramentas de controle, a empresa atinge a maturidade nesse processo de segregação de funções. A empresa deve buscar sempre a identificação de novos riscos e como controlá-los, sem esquecer aqueles existentes no sistema. Esse deve ser o foco da empresa a partir do momento em que seu SAP está completamente segregado e controlado. Tornar a extração e análises dos relatórios algo cotidiano na empresa é

essencial para a sequência desse processo. A busca por novas ferramentas de controle também deve ser um assunto abordado.

A empresa pode mensurar a efetividade desse processo pouco tempo após sua realização. Com as atividades segregadas, os gestores têm um controle maior de quem está realizando cada etapa e já podem planejar como uma nova atividade atribuída à área será desempenhada pelos seus subordinados.

REFERÊNCIAS

ABNT. NBR/ISO/IEC 27002. *Tecnologia da Informação: Código de prática para a gestão da segurança da informação*. 2006.

ARIMA, Carlos H. *Metodologia de Auditoria de Sistemas*. SP: Érica, 1992.

BERNSTEIN, Peter L. *Desafio aos Deuses: A Fascinante História do Risco*. RJ: Campus, 1997.

Ernst & Young Digital Insights. *Dados Sobre Segurança da Informação*. Cleveland-OH, 2005

Ernst & Young Digital Insights. *Governança e Resultados*. Cleveland-OH, 2007

Ernst & Young Digital Insights. *IT Risk*. Cleveland-OH, 2010

Isaca Journal. *Segregation of Duties*. Cleveland-OH, 2009

IT Governance Institute. *Control Objectives, Management Guidelines, Maturity Models*. ISACF, Information System Audit and Control Foundation. CobIT 4.1. Rolling Meadows-IL, 2007

SAP Education Brasil. *GRC 300 SAP Business Objects Access Control – Implementation and Conf*, 2010

Instituto Brasileiro de Governança Corporativa: *Governança Corporativa*. 1995. Disponível em: <[HTTP://www.ibgc.org.br/Secao.aspx?CodSecao=17](http://www.ibgc.org.br/Secao.aspx?CodSecao=17)> Acesso em: 19/02/2012

BIBLIOGRAFIA CONSULTADA

ANDERSON, George W. *Sams Teach Yourself SAP in 24 Hours*. Indianapolis-IN: Sams, 2011.

FERNANDES, Aguinaldo A. & ABREU, Vladimir F. *Implantando a Governança de TI – da Estratégia à Gestão dos Processos e Serviços*. Rolling Meadows-IL: ISACA, 2009.

HOLAND, Holly A. & BROADY, Denise Vu: *SAP GRC for Dummies – Don't Drown in GRC alphabet Soup!*, 2008.

IT Governance Institute. *Managing Enterprise Information Integrity – Security, Control and Audit Issues*. Rolling Meadows-IL: ISACA, 2004.

LAROCCA, Danielle: *SAP R/3 – Ferramentas de Relatórios*. RJ: Ciência Moderna, 2000

PRITCHARD, C. L. *Risk Management – Concepts and Guidance*. Arlington-VA: ESI International, 2001

SANTOS, José L., SCHMIDT, Paulo; GOMES, José M. *Fundamentos de Auditoria Contábil*. SP: Atlas, 2006

SAP Education Brasil: *GRC 330 SAP Business Objects Process Control 3.0 – SAP Governance, Risk, and Compliance*. 2010

SAP Education Brasil: *GRC 340 SAP Business Objects Risk Management – SAP Business Objects – Business Intelligence*. 2010

SEVERINO, A. J. *Metodologia do Trabalho Científico*. SP: Corte & Morales, 1996

WEILL, Peter & ROSS, Jeanne W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston-MA: Harvard Business Press, 2004