Segregação de Funções na Prática: Abordagem Funcional e Sistêmica
Por Maicon Gabriel Bitencourtt

Por mais simples e essencial que pareça, você pode afirmar com segurança que na sua empresa há um nível suficiente de Segregação de Funções (*Segregation of Duties - SoD*)? A resposta pode se tornar ainda mais complexa quando consideramos todas as variáveis envolvidas na implementação de uma estrutura de segregação, não acha?

Elementos como risco, atividade, transação, abordagem sistêmica, funcional, função, perfil, revisão periódica e acesso são apenas alguns dos termos que influenciam diretamente o formato de uma estrutura de Segregação de Funções. Assim, a depender do apetite de risco da companhia, pode ser necessário um nível de conforto maior, o que exigiria, por consequência, um controle mais rigoroso em relação ao tema. É por essa razão que responder à pergunta inicial pode se mostrar uma tarefa complexa.

Neste material, vamos explorar os principais conceitos e abordagens adotadas no mercado quando tratamos de Segregação de Funções, oferecendo informações que podem ajudar você a avaliar se a sua empresa realmente dispõe de um ambiente de controle adequado.

Antes de nos aprofundarmos em alguns desses conceitos, vamos recapitular o significado de Segregação de Funções. Seu objetivo fundamental é evitar a concentração de atividades em uma única pessoa ou área, de modo a minimizar possíveis conflitos de interesse, reduzindo o risco de erros e/ou fraudes. Frameworks e entidades como COSO, Instituto de Auditores Internos (IIA), IBGC, ISACA e COBIT reforçam a importância do SoD para o fortalecimento dos controles internos e da governança corporativa.

Definição de Segregação de Funções segundo o glossário do ISACA: *"Um controle interno básico que previne ou detecta erros e irregularidades ao atribuir responsabilidades [...] a pessoas diferentes."*

Definição de Conflito de Interesse, de acordo com o glossário do IIA: "*Qualquer relacionamento que seja ou pareça ser contrário aos melhores interesses da organização. Um conflito de interesses prejudicaria a capacidade de uma pessoa de desempenhar suas funções e responsabilidades de forma objetiva."*

Conceitos Fundamentais

Para construir uma estrutura de Segregação de Funções (SoD) realmente eficaz, é fundamental compreender alguns elementos-chave que definem como as atividades operacionais se relacionam com as permissões de acesso nos sistemas corporativos (ERPs, CRMs etc.). Assim, apresentaremos a seguir quatro conceitos essenciais: Atividade, Transação/Tela, Função e Perfil.

Atividade

"Atividade" é, em essência, a ação ou conjunto de ações que compõem um processo ou fluxo operacional. Quando falamos de SoD, o grande cuidado que devemos ter é identificar, além de todas as atividades relevantes para o processo, os potenciais riscos decorrentes do conflito dessas atividades. Por exemplo, a atividade de emissão e a de aprovação de requisições de compra são conflitantes, pois podem expor a companhia a riscos de conflitos de interesse. Nesses casos, a matriz de SoD deve classificar tais atividades como conflitantes, indicando a necessidade de controles compensatórios ou da separação efetiva dessas tarefas.

Tela ou transação

Em sistemas corporativos, as “transações” ou “telas” são as interfaces pelas quais o usuário interage para executar as atividades, sendo cada transação/tela normalmente dedicada a uma operação ou conjunto de operações. No contexto de SoD, cada atividade mapeada deve ter a respectiva transação vinculada, facilitando a futura identificação de potenciais conflitos. Por exemplo, em um módulo de compras, a tela “Criar Pedido” pode permitir cadastrar requisições, enquanto a tela “Aprovar Pedido” concede poderes para autorizar a execução do processo. É comum também que essas “telas” sejam representadas por códigos (ou “transações”) em alguns ERPs. Quando esses acessos se encontram concentrados em um único usuário, a organização passa a ter um ponto de atenção que precisa ser endereçado para evitar riscos operacionais ou fraudes.

Função

A “função” (também chamada de Role em alguns ERPs) agrupa um conjunto de atividades pertinentes a um determinado papel organizacional (posição ou cargo). Tomemos como exemplo a função de “Analista de Compras”: neste caso, seriam atribuídas a esse papel as atividades (transações) que permitem criar e editar requisições de compra, enquanto a função de “Supervisor Financeiro” se encarregaria de aprová-las. Definir funções coerentes com as atribuições de cada cargo impede que uma só pessoa detenha permissões conflitantes.

Perfil

O “perfil” de acesso delimita de forma mais detalhada como, onde e até que ponto um usuário pode exercer suas atividades. Ele pode restringir valores máximos para aprovação de compras, delimitar o acesso a filiais específicas ou até limitar a visualização de determinados relatórios. Assim, ainda que um colaborador possua a função de “Analista de Compras”, o perfil pode bloquear a criação de requisições para uma determinada unidade de negócio. Quando combinados ao uso de funções bem estruturadas, os perfis criam uma base sólida para a SoD, alinhada às políticas de governança e aos princípios de controle interno.

De maneira sintética, poderíamos resumir cada um dos 4 conceitos em:

1. **Atividade (Task)**: a ação específica (ex.: “Criar pedido de compra”).
2. **Transação (ou Tela)**: onde aquela atividade é executada dentro do ERP (ex.: “Formulário X” no Oracle, T-code Y no SAP).
3. **Função (Role)**: o conjunto de atividades que um determinado papel (por exemplo, “Analista de Compras”) pode executar.
4. **Perfil (Profile)**: regras adicionais que delimitam *como* e *até onde* a Função pode atuar (limites de aprovação, restrição por filial, etc.).

É importante ressaltar que a nomenclatura e o detalhamento de cada conceito podem variar de acordo com a arquitetura e a parametrização de cada ERP. Em algumas soluções, como o Oracle Cloud, além dos Roles é comum existirem Privilégios ou camadas adicionais de segurança, enquanto em outros sistemas, como SAP, as transações são representadas por T-codes.

Essas diferenças de terminologia e estrutura não alteram o objetivo fundamental da Segregação de Funções, mas exigem que as empresas adaptem suas matrizes e metodologias de SoD à realidade técnica de cada plataforma, garantindo a efetividade dos controles internos.

Assim, no contexto atual, em que processos são cada vez mais apoiados por sistemas de informação e ERPs, a Segregação de Funções pode ser mapeada e analisada sob duas perspectivas:

1. **Abordagem Funcional (ou Não sistêmica):** Foca na separação de tarefas no dia a dia operacional.
2. **Abordagem Sistêmica:** Trata do mapeamento, definição e conformidade dos perfis e acessos dentro dos sistemas.

Abordagem Funcional (Não Sistêmica)

Na abordagem de mapeamento de segregação de funções funcional, ou não sistêmica, a atenção está voltada para a divisão de papéis e responsabilidades que também excedem processos sistêmicos, observando o processo "de ponta a ponta", por exemplo:

- O responsável por cadastrar fornecedores não deve ser o mesmo que aprova contratos.
- A equipe que executa um pagamento não pode ser a mesma que contabiliza o documento.

O foco é entender, no fluxo operacional, quem faz o quê, identificando possíveis pontos de conflito e definindo controles compensatórios quando for inviável a separação total. Ou seja, há um foco no mapeamento das atividades e funções ao longo dos processos operacionais, por meio da análise de fluxogramas, organogramas, políticas internas e entrevistas com gestores. Uma vez que se sabe quem executa cada tarefa, passa-se a verificar onde podem ocorrer conflitos.

De forma prática, a utilização de uma matriz de segregação de funções proveniente da abordagem funcional acaba sendo uma importante ferramenta para a segunda (controles internos) e a terceira (auditoria interna) linha, pois permite de forma mais ágil a revisão e a validação da conformidade sobre aquilo que está descrito em políticas, procedimentos e organogramas.

Abordagem Sistêmica

Já a abordagem sistêmica contempla no mapeamento também a identificação e conciliação das atividades com as transações/telas dos sistemas ERP. O objetivo, no longo prazo, é não só utilizar a matriz como uma ferramenta de apoio à segunda e à terceira linha, mas também desenvolver a construção e a revisão de funções e perfis de acesso sem que transações conflitantes sejam acumuladas. O sucesso da abordagem sistêmica passa pela elaboração de uma matriz de segregação que relacione, para cada processo (contas a pagar, faturamento, compras etc.), quais transações não podem coexistir no mesmo perfil.

Cabe destacar que existem ferramentas voltadas para "*Identity and Access Management (IAM)"* ou soluções de "*Governance, Risk and Compliance (GRC)*" que ajudam a automatizar a concessão de acessos, entretanto, a eficácia dessa abordagem depende do monitoramento constante e de políticas bem definidas, garantindo que a matriz seja atualizada conforme surgem novas necessidades ou mudanças nos processos organizacionais.

O ideal é que as empresas não vejam as abordagens sistêmica e funcional como excludentes, mas sim como complementares. Mesmo que o sistema seja robusto em termos de controle de perfis e acessos, ainda há procedimentos manuais ou específicos de cada área que precisam ser analisados. Da mesma forma, a verificação manual de fluxos não substitui a necessidade de restringir acessos no nível sistêmico, evitando que usuários com permissões inadequadas executem etapas críticas.

Revisão de Acessos

Além disso, a adoção de regras de segregação, sejam elas sistêmicas ou não sistêmicas, não garante por si só a perenidade de um ambiente de controle efetivo. É fundamental realizar revisões periódicas de acessos para verificar se as permissões concedidas continuam alinhadas às funções e responsabilidades de cada colaborador. A revisão de acessos busca identificar se há riscos materializados de acúmulo indevido de funções ou perfis, bem como assegurar que os colaboradores possuam apenas os acessos indispensáveis para exercer suas atividades.

Em termos práticos, podemos destacar três atividades principais nessa revisão:

- **Mapeamento das Funções e Perfis**: Identificar todas as funções (roles) e perfis ativos, comparando-os com a estrutura organizacional e a matriz de SoD.
- **Validação**: Avaliar se os acessos dos membros da equipe continuam condizentes.
- **Tratamento de Exceções**: Quando não for possível remover um acesso potencialmente conflituoso, estabelecer controles compensatórios, como aprovação em duplas ou revisões independentes.

O ideal é que essas revisões sejam feitas em uma periodicidade pré-definida (trimestral, semestral ou anual), de acordo com o nível de risco e a criticidade das funções. Também é importante manter registros das revisões realizadas, além das justificativas para eventuais exceções, contando com as aprovações dos responsáveis. Isso facilita a comprovação de aderência às boas práticas e a normas regulatórias.

É comum também se fragmentar a atividade de revisão de acessos por módulos de sistema, delegando a um ponto focal (*key user*) a responsabilidade de identificar quem possui (ou não) os devidos acessos, uma vez que, a depender do tamanho da organização, essa atribuição seria sensível e até complexa de ser realizada pela equipe de TI.

Conclusão

Retomando a pergunta inicial: “Você pode afirmar com segurança que sua empresa possui um nível suficiente de Segregação de Funções?”. A resposta requer um entendimento profundo tanto dos processos manuais quanto das configurações e perfis em sistemas. Mais do que simplesmente implantar uma série de regras, a SoD exige o comprometimento de todos os níveis organizacionais e uma cultura forte de governança.

Quando bem estruturada, a Segregação de Funções ajuda a proteger a empresa contra fraudes, conflitos de interesse e falhas operacionais, contribuindo para a construção de um ambiente de controle interno robusto e confiável. Investir na combinação das abordagens e acompanhar periodicamente a eficácia dessas medidas são passos fundamentais para mitigar riscos e garantir a transparência dos processos.

Se a sua organização busca fortalecer o ambiente de controle interno, nós, da Berkan Consultoria e Auditoria, contamos com a expertise e as ferramentas necessárias para aprimorar seus processos de governança corporativa e fortalecer a atuação da segunda e da terceira linha na mitigação de riscos, oferecendo soluções personalizadas às necessidades da sua organização.

Entre em contato para descobrir como podemos colaborar e agregar valor às suas operações. Juntos, transformaremos desafios em oportunidades e construiremos um ambiente de controles internos mais robusto, sustentável e alinhado aos objetivos estratégicos de sua empresa.

Referências

- COSO (Committee of Sponsoring Organizations of the Treadway Commission) – Internal Control – Integrated Framework
- IIA (The Institute of Internal Auditors) – International Professional Practices Framework (IPPF)
- ISACA – COBIT Framework
- IBGC (Instituto Brasileiro de Governança Corporativa) – Publicações sobre Governança e Controles Internos