Controle De Acesso Baseado Em Gestão De Riscos – Uma Abordagem Em Empresa De Capital Aberto

Felipe Pereira da Silva*

2017, v-1.0.0

Resumo

Em um cenário onde a execução dos processos são altamente dependentes de recursos de Tecnologia da Informação (TI), a forma de entrega dos acessos é elemento vital para garantia da proteção e confiabilidade das informações que viabilizam a execução das tarefas desses processos. Neste contexto, o sistema ERP de uma organização é item de configuração chave, demandando de sólido gerenciamento do controle de acesso, manipulação e armazenamento das informações. Este artigo aborda, no contexto de uma organização brasileira de capital aberto, o método de controle de acesso aplicado em conjunto com o processo de gestão de riscos, que juntos proporcionam uma visão singular sobre riscos diversos que podem ser até mesmo de fraudes financeiras. O acumulo de permissões, ou ainda, a concessão de acessos sem prévia análise dos riscos de segregação de função (SoD - Segregation of Duties) podem trazer consequências graves à organização. Neste intento, buscou-se uma contextualização de acordo com a legislação vigente, processos necessários, tomando como exemplo um sub processo da área financeira de uma organização fictícia que utiliza o sistema SAP.

Palavras-chaves: Análise de riscos, Controle de acesso, segregação de função.

Introdução

O controle de acesso é um dos principais vetores para garantir a integridade de um sistema de informação. Apoiado em dois princípios fundamentais: least privilege e need-to-know, é necessário para permitir que apenas pessoas autorizadas e responsabilizadas tenham acesso aos recursos. O uso desses recursos para desempenho das atividades é cada vez mais intenso e neste conjunto, os sistemas de informação são ativos essenciais para execução de atividades de processos que muitas vezes podem trazer perdas para a organização caso não esteja operando conforme o esperado. É necessário que a medida em que aumenta a demanda de execução de atividades por meio de sistemas, haja proporcionalmente aumento do nível de controle de acesso aos recursos, pois a combinação de permissões inadequada abre uma porta para práticas inadequadas, seja elas intencionais ou não. Controlar acesso significa, portanto, muito mais do que verificar se há aprovações em cada solicitação, é necessário que haja parâmetros adicionais que possibilitem uma visão dos riscos envolvidos a cada combinação de permissão.

*felipetsi@gmail.com

1 Segurança da Informação

Apoiada em três pilares básicos que buscam garantir que as informações estejam disponíveis sempre que necessário e que sejam acessadas e alteradas apenas por entidades autorizadas (Disponibilidade, Confidencialidade e Integridade), a segurança da informação tem a dinâmica missão de definir o padrão de acessos aos recursos com base nas necessidades da organização, abordando critérios para: identificação e interpretação das necessidades; limitação, concessão, remoção e monitoração de acessos. Sem o entendimento e o controle sobre o que é processado, armazenado e descartado, bem como o valor de cada tipo de informação no contexto do negócio, não se pode afirmar sobre a confiabilidade das operações executadas. Segurança da informação abrange todas as operações de uma organização, visando o aprimoramento dos processos com vistas a proteção dos ativos da organização, dosando os pesos e as medidas, conforme o nível de exposição e o valor de cada ativo, ou conjunto deles. O controle de acesso a sistemas de informação, demanda de parâmetros robustos sobre o gerenciamento das permissões de acessos.

2 Controle de Acesso

Este é um processo que precisa operar com alto nível de engajamento aos objetivos estratégicos da organização, definindo-se o nível de controle necessário. A norma NBR ISO 27001 (2013), em sua cláusula 9 do anexo A, coloca que para ser estruturado adequadamente, precisa contemplar uma política clara, documentada, aprovada e implementada. Discorre também sobre o gerenciamento dos acessos e responsabilidades dos usuários, tratando em um controle específico os acessos a sistemas, com a abordagem sobre a necessidade de segregação de função e responsabilidade das áreas para reduzir as oportunidades de modificações não autorizadas ou não-intencionais dos ativos da organização.

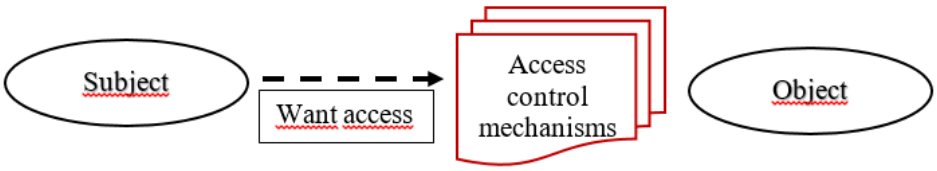

Figura 1 – Interação entre Subject e Object.

O controle de acesso trata como deve ocorrer a concessão, alteração e remoção da possibilidade de interação entre subject e object, a figura (**??**) ilustra esta relação. Conforme expõe GORDON (2015), a principal função é garantir que somente pessoas autorizadas estão permitidas em uma área controlada. GORDON (2015) apresenta quatro modelos para implementar e gerenciar acessos, diferenciando cada uma sobre a condição que irá determinar as permissões, são eles: Role-Based Access Control (RBAC), Rule-Based Access Control, Mandatory Access Control (MAC) e Discretionary Access Control (DAC).

- Role-Based Access Control (RBAC): controle de acesso baseado em papeis, ou funções que são exercidas pelos usuários dentro de uma organização.
- Rule-Based Access Control: aqui, o controle de acesso é de acordo com regras pré-definidas que determinam quais acessos serão permitidos.

- Mandatory Access Control (MAC): este modelo requer que o sistema auto gerencie o controle de acesso de acordo com a política de segurança implementada.
- Discretionary Access Control (DAC): controle de acesso são aplicadores de acordo com que determina o responsável (owner) da informação.

A escolha do melhor modelo a ser implementado depende de fatores tais como: cultura organizacional, nível de capacitação, orçamento, legislação regulatória e tecnologia disponível. Embora não haja um modelo que seja melhor em todas as circunstâncias, pois cada um tem a sua melhor aplicação dependendo do contexto, é possível expor que de uma forma geral, o modelo RBAC é mais adequado para controle em sistema ERP de empresas, visto que a implementação é com base nas funções desempenhadas pelas pessoas que operacionalizam as atividades dos processos. Importante observar que as permissões de acesso representam riscos, portanto é necessário que seja feita uma análise prévia a cada concessão de acesso aos recursos, a fim de que a existência de riscos seja verificada e devidamente endereçada, antes da concessão.

3 Gerenciamento de Riscos

Harris (2013) define que gerenciamento de riscos é o processo de identificação e avaliação de riscos, reduzindo-os a um nível aceitável por meio da implementação de mecanismos adequados. Em complemento, a norma NBR ISO 31010, diz que o processo de avaliação de riscos fornece informações com evidências para tomada de decisão sobre o tratamento dos riscos que podem impactar no atingimento dos objetivos da organização. Analisar riscos significa se antecipar a possíveis eventos que podem causar impactos na organização e assim tomar as devidas providências necessárias para que estes riscos estejam dentro de um nível aceitável. A própria norma define riscos como sendo incertezas sobre os objetivos da organização provocadas por influências de fatores internos e externos. A norma NBR ISO 31000 reforça que a gestão de riscos cria e protege valor para organização. Neste intento, o contexto do negócio contém os requisitos de operação tais como: desempenho, saúde e segurança de pessoas, conformidade legal e regulatórias, meio ambiente, entre outros. Esta definição deixa claro que muito além da implementação, a sustentação exige grande esforço alinhado com as mudanças do negócio, repetindo o ciclo reiteradas vezes. Dentre as ferramentas disponibilizadas na NBR ISO 31010, está a FMEA, que é utilizada para identificar as formas em que componentes, sistemas ou processos podem falhar em atender o objetivo. Harris (2013) reforça colocando que a FMEA é utilizada no gerenciamento de risco proporcionando um nível de detalhamento, variáveis e complexidade que influencia no entendimento do risco em um nível mais granular. Juntando a ótica do controle de acesso, com a da análise de riscos, cria-se uma ótica singular sobre os eventos possíveis de dano à organização, bem como o nível de proteção necessários para os ativos, atendendo assim aos requisitos do negócio.

4 Contexto Organizacional

O contexto de uma organização direciona como que as ações devem ser operacionalizadas a fim de garantir a longevidade do negócio, que precisa ter habilidades necessárias para lidar com os fatores internos e externos. De acordo com a norma NBR ISO 31000, a definição do contexto deve ser feita antes de realizar a concepção e a implementação do gerenciamento de riscos. Isso mostra que a gestão de riscos precisa estar contextualizada

de acordo com cada realidade. Ademais, toda gestão dos processos de TI precisa está sob um eficiente processo de governança, afim de manter o contexto atualizado e os processos alinhados com as necessidades da organização.

5 Governança de TI

A norma NBR 38500 apresenta que a estruturação da governança de TI no âmbito corporativo deve envolver essencialmente ações de avaliar, dirigir e monitorar, sendo executadas sob seis princípios: responsabilidade, estratégia, aquisição, desempenho, conformidade e comportamento humano, conforme ilustra figura (**??**). Esses princípios precisam ser considerados e em cada um, as ações de avaliar, dirigir e monitorar precisam ser executadas a fim de cobrir a abrangência do processo de governança.

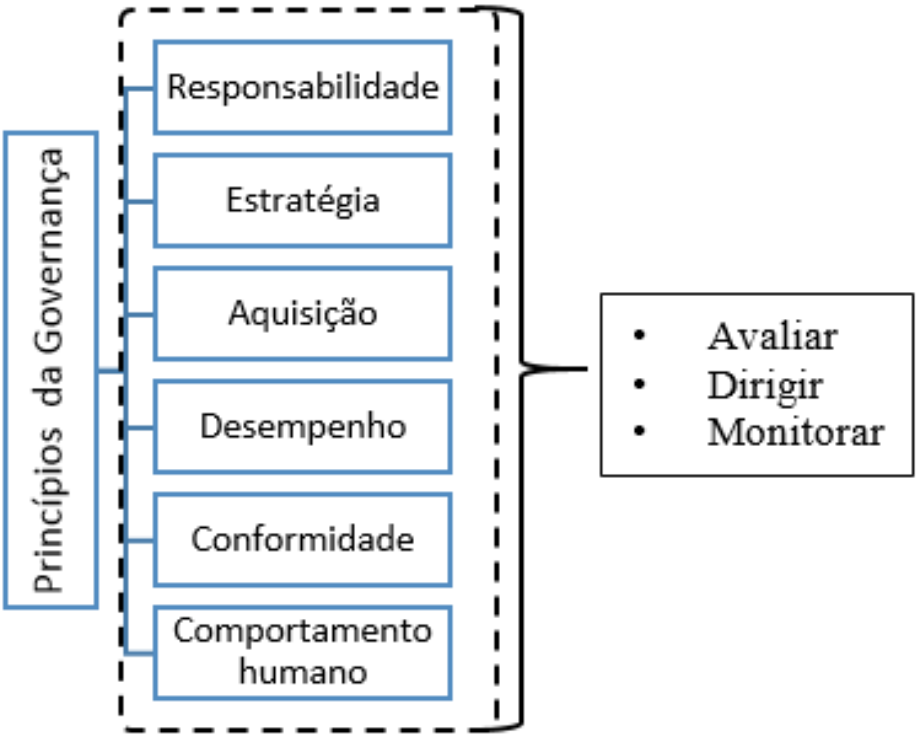

Figura 2 – Princípios da Governança de TI conforme a norma NBR 38500.

6 Requisitos Legais

No Brasil, as empresas de capital aberto se quadram na lei 6404, que dispõe sobre a operação das Sociedades por Ações. Esta lei define em seu artigo 176, que ao término de cada exercício social, a diretoria deverá elaborar e publicar uma demonstração financeira contendo o patrimônio da companhia e as mutações ocorridas, abordando:

- Balanço patrimonial;
- Demonstração dos lucros ou prejuízos acumulados;
- Demonstração do resultado do exercício;

- Demonstração dos fluxos de caixa;
- Se companhia aberta, demonstração do valor adicionado.

No artigo 177, parágrafo 3º, é colocado que a demonstração financeira deve ser expedida e auditada por auditores independentes autorizados pela Comissão de Valores Mobiliários (CVM), visando isonomia ao processo que é realizado por equipe especializada. A auditoria busca a partir dos números apresentados, identificar por amostragem como que é gerenciado os recursos que processam, armazenam e manipulam essas informações a fim de atestar ou apontar o nível de confiança na informação apresentada, ou mesmo expor as fragilidades existentes. Neste processo, o sistema ERP (no caso deste artigo o SAP) da organização é alvo de uma série de análises. Alguns possíveis problemas que podem ser encontrados são: acesso indevido, ausência de matriz de perfis, falha no controle acesso de super usuário, ausência de segregação de função no nível adequado, fluxo de aprovação inapropriado e ausência de revisão dos acessos. Esses pontos são muito representativos e por trás de cada um deles há riscos diversos, como de fraldes financeiras, por exemplo. Para entender o nível de complexidade de implementar o controle de acesso baseado em análise de riscos no sistema SAP, faz-se necessário entender a sua estrutura de acessos.

7 Estrutura de Acessos do SAP

O sistema SAP possui estrutura de acesso basicamente separada em quatro componentes: Função de Autorização, Transação, Objeto e Campo. Estes componentes representam acessos e estão distribuídos em diversos módulos e processos, como é possível observar na figura (**??**).

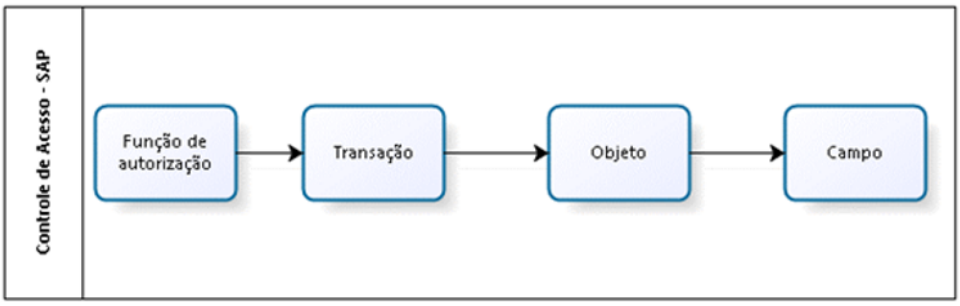

Figura 3 – Sequência de acesso no SAP.

Em essência, cada transação representa uma ação específica dentro do sistema, como por exemplo, a transação ME21N é para criação de pedido e a transação ME22N é para aprovação de pedido. São mais de 60.000 (sessenta mil) transações que representam ações de processos que são executadas no sistema. Um dos grandes desafios na gestão de acessos no SAP é manter o equilíbrio entre a permissão e a necessidade. Pode-se fazer uma analogia a uma gangorra, conforme figura (**??**) , onde o controle de acesso é o eixo, a necessidade e as permissão dos dois pesos que se contrabalanceiam. Quando um dos lados estiver desigual ao outro, significa uma falha no controle de acesso, portanto, essa possibilidade representa um risco. A medida em que há atribuição de responsabilidades para execução de tarefas às pessoas, há também a necessidade de concessão dos respectivos acessos, caso contrário um lado irá ficar desigual em relação ao outro e isso representa em termos práticos, impacto ao negócio, seja porque o usuário estará parado por não conseguir

acessar o sistema para desempenhar suas funções, seja porque o usuário estará com acessos além do necessário, representando um risco operacional.

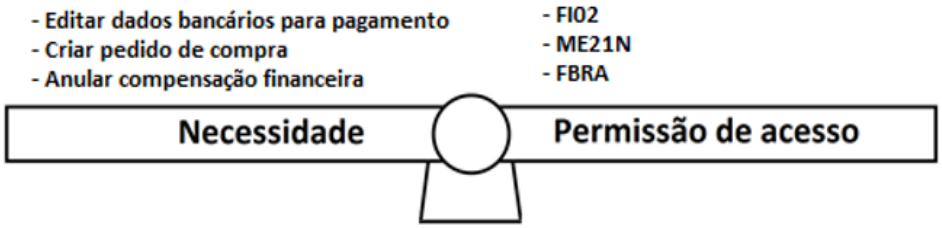

Figura 4 – Equilíbrio dos acessos.

Uma vez que os acessos representam funções que podem ser desempenhadas no sistema, se uma pessoa possui permissão para Solicitar e Autorizar um pedido, existe aí um risco que dependendo do tipo de solicitação e autorização pode-se viabilizar uma fraude financeira. Neste sentido, conforme mostra a tabela (**??**), diversos riscos de SoD surgem de acordo com a combinação dos acessos às transações e objetos do SAP.

Transação 1	Transação 2	Risco	Classificação
F-44	FI02	Criar uma conta de banco não genuína e criar pagamento para ela.	Alto
F-02	FBRA	Ajustar o balanço de filial usando a entrada de fatura do fornecedor e em seguida encobri-lo usando as entradas de diário.	Média
ME21N	ME51N	Risco da mesma pessoa requisitar um item e criar ordem de compra a partir desta requisição.	Média
ABSO	FB02	Pagar fatura e ocultá-la em um ativo que será depreciado com o tempo.	Alto
CO01	CO13	Processar ordem produzidas e confirmar produção de ordem	Baixo

Tabela 1 – Relação entre algumas transações do SAP e o risco.

Os riscos acima foram classificados de acordo com o impacto possível associado a cada risco, aplicando-se as seguintes classificações:

- Alto: risco estratégico, operacional e financeiro;
- Médio: Risco de fraude não financeira, conformidade e reputação;
- Baixo: Risco na cadeia de suprimentos.

Logicamente que dependendo do contexto da organização, a classificação de cada risco poderá variar, mas o cerne da questão é que quando se analisa o contexto diante do nível de exposição presente pela falta de parâmetros justos para controle dos acessos ao sistema SAP, o nível de exposição da organização é alto e esta fragilidade é exposta nos relatórios de auditoria financeiro, o que trás, além dos riscos de operações indevidas, as consequências por um baixo rendimento no resultado dessas auditorias, causando por exemplo: perda de acionista, perdas de capital de investimento e redução da credibilidade no mercado. Falcão (1995) enfatiza este aspecto colocando que a demonstração financeira pode significar o sucesso ou o fracasso quando em um determinado momento surja a necessidade de obter recursos junto a seus acionistas, investidores ou outras empresas interessadas apenas em manter um relacionamento comercial.

8 Criação dos perfis de acesso

Utilizando o modelo RBAC para criação dos perfis de acesso de acordo com as funções dos processos [1] da organização, é necessário que estes estejam adequadamente mapeados com o nível de detalhamento necessário. Utilizando notação BPMN (Business Process Model Notation) e como exemplo o macroprocesso "Gerenciar Recursos Financeiros", pode-se mapear os processos até chegar no nível das atividades/tarefas que são executadas. Cada tarefa terá uma transação correspondente e assim o perfil de acesso deve ser criado. Na figura (**??**) é possível observar um exemplo do mapeamento deste processo.

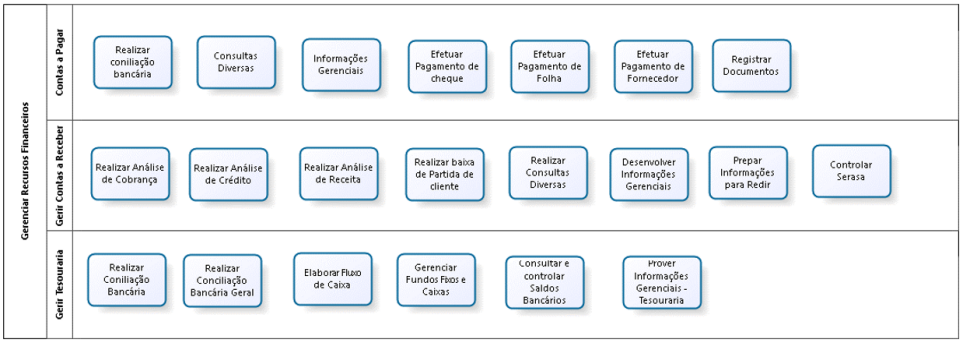

Figura 5 – Exemplo de um processo financeiro.

O principal ponto a ser observado no mapa de processo é que neste nível já é necessário que haja uma coerente distribuição de responsabilidades separadas pelas áreas, pois as falhas aqui já representarão riscos. Para cada processo, é possível criar uma visão de riscos inerentes a operação. Utilizando como exemplo o sub processo "Efetuar Pagamento de Fornecedor", apresentado na (**??**), para realização da análise de risco utilizando a ferramenta FMEA (Failure Mode Effect Analysis), ao levantar as atividades desse sub processo, tem-se 7 (sete) ações operacionais conforme mostra a (**??**), sendo todas elas realizadas por meio do sistema SAP. A execução dessas ações no sistema SAP envolve o uso de diversas transações. Cada transação é uma permissão de execução que compões o perfil de acesso de cada usuário.

Selecionando a atividade "Criar proposta de pagamento", é possível identificar dois riscos, conforme mostra (**??**), que são em essência modos de falha na execução do processo:

[1] Uma outra forma possível seria usar as funções que as pessoas desempenham ao invés do processo, se aproximando do cargo da pessoa.

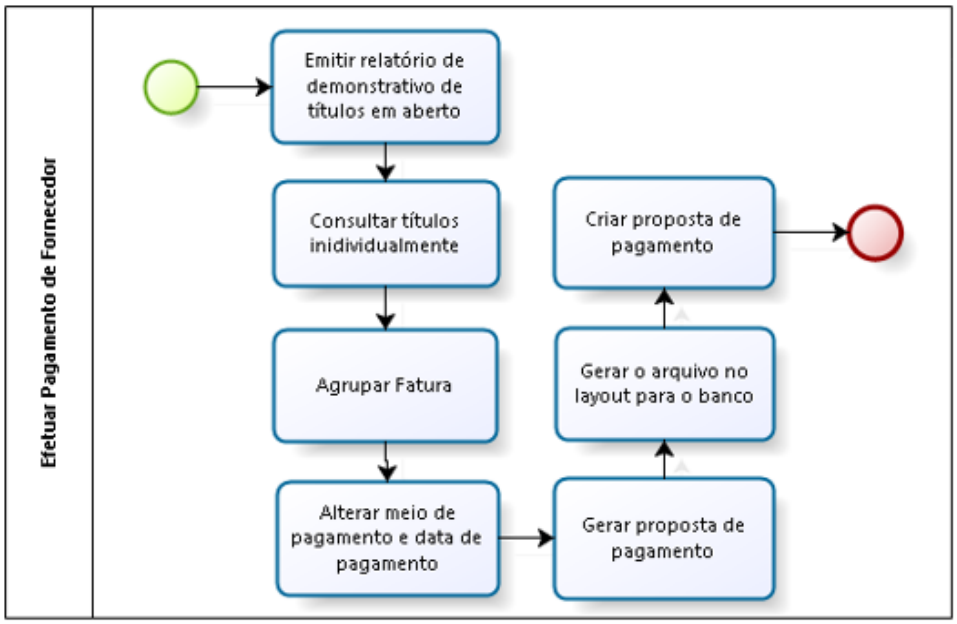

Figura 6 – Sub processo Efetuar Pagamento de Fornecedor.

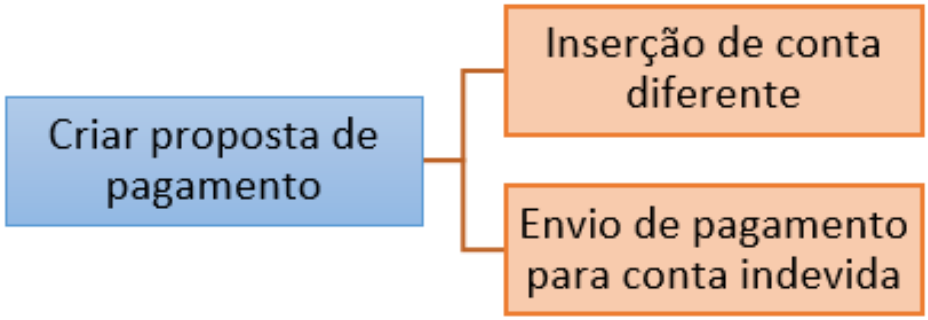

Figura 7 – Modos de falha “Criar proposta de pagamento".

Considerando esses modos de falha e aplicando a ferramenta FMEA para análise e avaliação dos riscos, é importante a identificação dos itens que envolvem está análise dentro do contexto de trabalhado. Neste sentido, a tabela (**??**) mostra a relação entre esses itens:

Item do FMEA (Visão NBR ISO 31010)	Referência neste estudo de caso
Componentes	Transações do sistema SAP
Modos de falha	Risco observado pela combinação de acessos
Efeito	Eventos possíveis no sistema SAP
Mecanismos de falha	Processo de controle de acesso
Como evitar falhas	Mecanismos de mitigação

Tabela 2 – Correção com os itens do FMEA.

Utilizando valores qualitativos para mensurar os riscos, foram definidas as seguintes

variáveis: a severidade (S) da falha, que representa o impacto, quantificando o resultado causado, também conhecido como efeito; a ocorrência (O) da falha, que quantifica a probabilidade de ocorrência; e a detecção (D) da falha, que quantifica a capacidade do modo de falha não ser detectada pelos controles do processo; o número de prioridade de risco (NPR), que representa o índice de priorização no tratamento do risco. A classificação dos fatores dessa análise, segue uma escala conforme tabela (**??**).

Severidade	Valor
Mínima	1
Pequena	2 e 3
Moderada	4 e 5
Alta	7 e 8
Muito Alta	9 e 10

Tabela 3 – Escala qualitativa utilizada na FMEA.

Em continuidade, os riscos descritos na tabela (**??**) foram identificados.

Modo de Falha	Efeito Potencial	S	Causa Potencial	O	D	NPR
Pagamento para conta bancária não autorizada	Manter conta bancária indevida e enviar pagamento para ela, causando perda de receita causada por fraude financeira interna.	10	Falha na concessão de acesso.	3	2	60

Tabela 4 – Matriz de risco do FMEA.

Cada modo de falha apresentado, representa um risco e o efeito potencial é a descrição do impacto que será causado se o risco se materialize. Em ambos os casos a classificação da severidade foi a mais alta (10) pois representa perdas que muitas vezes são irreparáveis em uma organização. No primeiro modo de falha, a classificação da ocorrência foi 3 porque é baixa a probabilidade de ocorrência de criação de contas fictícias, até mesmo porque a capacidade de detecção é consideravelmente boa, pois trata-se das contas que área financeira já possui catalogada, então caso surja alguma indevida, será provavelmente identificada. No segundo modo de falha, a probabilidade de ocorrência já é mais alta, visto que a quantidade de fornecedores é dinâmica e o controle é mais difuso, portanto a capacidade de detecção também é mais difícil.

9 Considerações finais

As grandes empresas de capital aberto estão sujeitas a níveis de controle cada vez mais exigentes, conforme há o aumento da dependência de recursos tecnológicos na geração, manipulação e armazenamento das informações do negócio. Controlar o acesso a essas informações é fator indispensável. Analisando o nível de cobrança das auditorias financeiras, é possível afirmar que é crescente o nível de evidências e análises realizadas nas operações

das organizações. Esta crescente se dá pela necessidade continua de amadurecimento dos processos de controle, que precisam estar protegidos contra ameaças do ambiente e suas evoluções. A aplicação do controle de acesso apoiado na análise de risco, apresenta considerável ganho sobre o nível de controle das informações de um sistema. Portanto, considerando os princípios: need-to-know e least-privilegie em um sistema com mais de 60.000 transações, é evidentemente necessário que a manutenção dos acessos seja apoiado em algum parâmetro que mensure o impacto de cada concessão, condicionando a atribuição de permissões não apenas por uma autorização do responsável, mas principalmente, à uma ciência sobre os riscos envolvidos, que passam a estar no rol de ações do processo de análise de riscos, que deverá criar medidas compensatórias a fim de minimizar as possibilidades de impactos negativos à organização.

Referências

- GORDON, ADAM, Official Guide (ISC)2 Guide to the CISSP (CERTIFIED INFORMATION SYSTEM SECURITY PROFESSIONAL) CBK, Fourth edition 2015;
- HARRIS, SHON, All in One CISSP - Sith edition, 2013;
- NBR IEC/ISO 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos;
- NBR IEC/ISO 31010:2012 – Gestão de Riscos – Técnicas para o processo de avaliação de riscos;
- NBR IEC/ISO 38500:2009 – Governança Corporativa de Tecnologia da Informação;
- NBR ISO 31000:2009 – Gestão de Riscos – Princípios e diretrizes.
- FALCAO, Eduardo. Divulgação em demonstrações financeiras de companhias abertas. Cad. estud., São Paulo , n. 12, p. 01-13, Sept. 1995 . Available from <http://www.scielo.br/scielo.php?scri 92511995000100003&lng=en&nrm=iso>. access on 30 Apr. 2017. http://dx.doi.org/10.1590/S1413-92511995000100003;