Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

RAFAEL FERREIRA DE ALMEIDA

ANÁLISE DE RISCOS PARA MELHORAR O PROCESSO DE MUDANÇAS NAS APLICAÇÕES BANCÁRIAS EM PRODUÇÃO

Brasília
2014

RAFAEL FERREIRA DE ALMEIDA

ANÁLISE DE RISCOS PARA MELHORAR O PROCESSO DE MUDANÇAS NAS APLICAÇÕES BANCÁRIAS EM PRODUÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança

Orientador: Prof. Gilberto Oliveira Netto

Brasília
2014

RAFAEL FERREIRA DE ALMEIDA

ANÁLISE DE RISCOS PARA MELHORAR O PROCESSO DE MUDANÇAS NAS APLICAÇÕES BANCÁRIAS EM PRODUÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Rede de Computadores com Ênfase em Segurança

Orientador: Prof. Gilberto Oliveira Netto

Brasília, ___ de Dezembro de 2014.

Banca Examinadora

_____

Prof. _____

_____

Prof. _____

Dedico este trabalho a meus pais, pelos seus exemplos de vida, pelas oportunidades que me deram e pelas grandes batalhas que enfrentaram para garantir minha educação.

AGRADECIMENTOS

Agradeço a todas as pessoas que contribuíram de alguma forma na construção deste trabalho. Alguns deles foram: a minha amiga Lucianna Braga, aos professores Gilberto Oliveira e Francisco Javier e aos meus pais Vera Lúcia e Joaquim Francisco.

RESUMO

Como forma de melhorar a segurança das informações em sistemas financeiros bancários, após a implantação de mudanças nas aplicações em produção, este trabalho trouxe um estudo que propôs verificar se era possível utilizar a análise de riscos no processo de gerenciamento de mudanças dos ambientes tecnológicos de desenvolvimento dos sistemas. Ele buscou demonstrar que tendo o conhecimento dos riscos, é possível controlá-los, evitando que as mudanças mal planejadas sejam implantadas em ambiente de produção, o que diminuirá a probabilidade de ocorrência de falhas e erros nos sistemas e também de prejuízos aos clientes e a instituição. A atividade de análise de riscos envolveu as tarefas de identificar os sistemas mais críticos para o negócio, os eventos potenciais e suas consequências para organização e para área de tecnologia, a probabilidade de ocorrência de alguma das ameaças, de priorizar os riscos identificados, e por último, de comunicar as partes interessadas. Além disso, este trabalho também trouxe um exemplo de aplicação da análise de riscos, com o objetivo de gerar produtos que pudessem ser utilizados no processo de gerenciamento de mudanças. Após estes estudos, concluí-se que é viável usar a análise de riscos antes de implantar as mudanças de aplicações bancárias no ambiente de produção, como tentativa de mitigar os riscos e a probabilidade de ocorrência de falhas e erros nos sistemas.

Palavras-chave: Segurança da Informação. Análise de Riscos. Ameaças. Riscos. Gerenciamento de Mudanças.

ABSTRACT

As a way of improving information security in financial banking systems after the implementation of changes in production applications, this paper proposed a study that brought verify if it was possible to use risk analysis in the process of change management of technological development environments systems. He sought to demonstrate that having knowledge of the risks, you can control them by preventing poorly planned changes are implemented in the production environment , which will reduce the probability of occurrence of faults and errors in the system and also damage to customers and the institution. The activity risk analysis involved the tasks of identifying the most critical systems for business, potential events and their consequences for the organization and technology area, the probability of occurrence of any threats, prioritize the identified risks, and finally, to inform interested parties. Moreover, this work also brought an example of application of risk analysis in order to generate products that could be used in change management process. After these studies , we conclude that it is feasible to use risk analysis before deploying the changes in banking applications in the production environment , in an attempt to mitigate the risks and the probability of failures and errors in systems.

Key words: Information Security. Risk Analysis. Threats. Risks. Change Management

LISTA DE FIGURAS

LISTA DE FLUXOS

LISTA DE QUADROS

SUMÁRIO

INTRODUÇÃO

Diante da turbulência nos mercados internacionais, desencadeada pela crise que se instalou no segundo semestre de 2008, as instituições financeiras brasileiras se mantiveram firmes diante de um cenário global de profunda instabilidade. Mais do que isso, os bancos brasileiros estiveram presentes na lista dos maiores do mundo, sustentados por estratégias de crescimentos consistentes e que inspiram organizações de outros países.

O trabalho feito até aqui pelas instituições bancárias brasileiras está marcado por diversas conquistas e desafios superados, que servem de experiência para continuarem progredindo na economia global.

Sabe-se que nesse setor nada é previsível, que os novos cenários da indústria financeira vão exigir estratégias muito consistentes e como forma de acompanhar esse avanço é preciso se preparar.

Sendo a Tecnologia da Informação (TI) o conjunto de todas as atividades e soluções providas por recursos de computação, é necessário fazer uso dos recursos de TI de maneira apropriada, ou seja, é preciso utilizar ferramentas, sistemas ou outros meios que façam das informações um diferencial competitivo.

Hoje a economia mundial é baseada na Tecnologia de Informação, e isso requer das organizações um conhecimento para coletar, trabalhar, interpretar e gerenciar estes recursos. O desenvolvimento e o domínio destas habilidades serão fundamentais para as organizações buscarem uma posição melhor no mercado em relação aos seus concorrentes, sendo necessário um empenho na constante busca por inovação.

Em um mundo onde a competição, a evolução e a mudança desempenham papel importante para inovação e desenvolvimento das organizações, a gestão de segurança da informação é elemento fundamental para o sucesso, e isto vale também para as instituições financeiras.

Dentre os diversos assuntos tratados pela gestão da segurança da informação, um dos principais elementos que direcionam as ações é o

gerenciamento de risco, iniciado com a implementação de um processo de análise de risco.

Diante desse cenário, no qual o valor da informação é vital para instituição e para o processo de tomada de decisão, se não houver um alinhamento entre a TI e às estratégias do negócio, com o objetivo de melhorar a comunicação interna, identificar riscos e acompanhar as mudanças impostas, a qualidade dos serviços prestados para os usuários, clientes e fornecedores será comprometida, e consequentemente irá propiciar vulnerabilidades nos sistemas, perda de mercado e prejuízos financeiros e de imagem.

Tema

A segurança da informação no processo de gerenciamento de mudanças de aplicações bancárias em ambiente de produção.

Problema

Nos últimos anos temos nos deparado com várias falhas de sistemas nas instituições financeiras bancárias do Brasil, estas, na maioria das vezes, são atribuídas à área de tecnologia, o que gerou desconfiança por parte dos clientes, prejuízos financeiros e de imagem à instituições.

Algumas dessas falhas foram divulgadas por importantes empresas de comunicação. Dentre as principais notícias, destacam as seguintes:

- “Vários clientes da Caixa Econômica Federal se depararam nesta semana com um limite acima de R$ 14 bilhões no cheque especial. O problema foi registrado em contas de pessoas jurídicas [...].” (GLOBO.COM, 2013).
- “[...] correntistas do Banco do Brasil alegaram que ao acessar o serviço com seu *login* e senha conseguiam ver dados de outros

usuários - como saldos, aplicações e resumo de operações financeiras.” (INFOR.ABRIL, 2013).

- “Bolsa Família [...], várias famílias pobres que têm direito de participar do programa tiveram benefícios bloqueados ou cancelados em função de falhas ou conflitos cadastrais de dois sistemas de informática [...].” (IG.COM, 2013).
- “Brechas de segurança teriam exposto na internet os dados de milhões de clientes do Banco do Brasil e Bradesco, além de outros serviços financeiros.” (EXAME.ABRIL, 2013).
- “Clientes do Bradesco e Caixa enfrentam filas após falha no sistema. Transações bancárias não puderam ser realizadas na sexta-feira; no 1º dia útil depois do incidente, clientes precisam ter paciência.” (CORREIO BRASILIENZE, 2013).
- “Sistema do BB sai do ar e clientes ficam sem serviço. O sistema do Banco do Brasil saiu totalmente do ar neste domingo, deixando clientes sem acesso a serviços como caixa eletrônico, Internet banking e compras com cartões de débito desde as primeiras horas da manhã.” (TERRA, 2013).
- “Clientes com conta investimento no banco receberam comunicado errado sobre encerramento do serviço. A Caixa Econômica Federal atribuiu a uma falha de tecnologia o envio de cartas comunicando um fato errado aos clientes [...].” (EXAME.ABRIL, 2011).

Baseado nos fatos citados surgiu a seguinte questão: Como diminuir a probabilidade de ocorrência de falhas e erros nos sistemas corporativos das instituições financeiras bancárias e garantir a segurança das informações após as implantações de mudanças?

Proposta

Como tentativa de resolver o problema encontrado, propõe-se utilizar a análise de riscos no processo de gestão de mudanças, com o propósito de identificar

e evitar falhas e erros nos sistemas, nos processos de desenvolvimento dos sistemas e no próprio processo de gestão de mudanças.

A atividade de análise de riscos quando aplicada no ambiente de desenvolvimento de sistemas, possibilita identificar: os sistemas mais críticos da organização, os módulos mais importantes e críticos dos sistemas, os principais processos envolvidos no desenvolvimento e implantação de mudanças, as ameaças e vulnerabilidades, a probabilidade e o impacto na ocorrência de uma ameaça.

Essa atividade exige que os produtos identificados sejam analisados, possibilitando reconhecer, avaliar e priorizar os riscos.

A análise baseia-se nas ameaças identificadas, nas probabilidades delas ocorrerem e ocasionarem prejuízos às organizações e/ou clientes e na gravidade dos prejuízos. Já a priorização é fruto da avaliação do risco, com o objetivo de criar um *ranking* dos riscos identificados e avaliados de acordo com o seu grau de criticidade.

E por último, a atividade de análise de riscos recomenda que os riscos sejam comunicados aos tomadores de decisões e outras partes interessadas, que irão utilizar todas as informações obtidas através das atividades anteriores para discutir a forma adequada de tratar ou aceitar os riscos.

Então, com os produtos gerados na análise de riscos, o objetivo é utilizá-los no processo de gestão de mudanças, para melhorar seu próprio processo, e principalmente, para verificar se as demandas[1] entregues estão aptas para serem implantadas em produção.

Este estudo visa mostrar que utilizando a análise de riscos no processo de gestão de mudanças, as ocorrências de falhas e erros atribuídos à área tecnológica irão diminuir consideravelmente, entregando mudanças de qualidade em produção, e evitando a implantação daquelas mal planejadas.

[1] Demanda: É uma solicitação de serviço criado pela área gestora e enviado a área de tecnologia.

Justificativa

Primeiramente a ideia de realizar esse estudo surge devido a várias divulgações nos últimos anos, de problemas nos sistemas das instituições financeiras bancárias do Brasil, que na maioria das vezes, foram atribuídas a falhas tecnológicas, conforme apresentado nos itens anteriores deste trabalho.

Outro fator, que também motivou para o desenvolvimento deste estudo foi que, como funcionário de uma grande instituição financeira bancária, diariamente nós nos deparamos com várias falhas, entre elas: falhas de sistemas que não são divulgadas à população pelos meios de comunicação, e sim, comunicadas pelos clientes à ouvidoria e aos canais de atendimento, e falhas nos processos de desenvolvimento e implantação de mudanças.

Além desses citados, outro fator importante é que, a análise de riscos irá propiciar a exposição dos riscos e impactos negativos, no negocio e na tecnologia, aos gestores do negócio e gerentes de TI. Estes poderão utilizar essas informações para traçarem planos estratégicos de melhorias nas áreas de tecnologia das instituições financeiras bancárias.

E com os estudos realizados até o momento, pode-se perceber também que, a atividade de análise de riscos é parte do processo de gestão de riscos, que, depois de iniciado, a gestão de risco é um processo cíclico que contempla atividades de análise, planejamento, implantação, controle e monitoramento. Por outro lado, a análise dos riscos é executada de forma esporádica, periodicamente ou sob demanda e, até a realização da análise seguinte, os resultados oferecerão uma visão temporária dos riscos avaliados, servido como parâmetro para todo o processo de gestão de riscos.

O processo de gestão de riscos, quando implantado, poderá trazer benefícios a todo ambiente de desenvolvimento de sistemas, principalmente aos processos existentes, como por exemplo: melhoria dos processos, agilidade no desenvolvimento dos sistemas, qualidade dos *softwares*, proatividade, entre outros.

Outro ponto importante é que, no âmbito acadêmico, o trabalho poderá contribuir fornecendo conteúdo para pesquisas relacionadas a instituições financeiras bancárias e análise de riscos, e servirá como estudo preliminar sobre o

tema, de modo que as pesquisas subsequentes possam ser concebidas com uma maior compreensão e precisão.

Objetivo Geral

Definir se é possível usar a análise de riscos para melhorar o processo de mudanças nas aplicações bancárias em produção, como tentativa de diminuir a probabilidade de ocorrência de falhas e erros atribuídos à área tecnológica, e como consequência, diminuir as vulnerabilidades nos sistemas, perda de mercado e prejuízos financeiros e de imagem da instituição.

Objetivos Específicos

- Apresentar os principais conceitos encontrados na análise de riscos e na segurança da informação.
- Descrever o propósito, os objetivos e as atividades do processo de gestão de riscos;
- Descrever brevemente sobre o ambiente de desenvolvimento de sistemas das instituições financeiras bancárias e sobre os principais processos encontrados nesse ambiente.
- Descrever o funcionamento do processo de gestão de mudanças;
- Exemplificar a aplicação da análise de riscos no processo de gestão de mudanças.

O presente estudo não tem a pretensão de identificar todos os riscos envolvidos no desenvolvimento e na mudança de aplicações bancárias para o ambiente de produção. Mas sim, de conscientizar os responsáveis da área tecnológica e de negócio, sobre a importância de conhecer e tratar os riscos do ambiente de desenvolvimento, pois caso isso ocorra, o percentual de falhas atribuídas à área tecnológica poderá ser reduzido consideravelmente.

Referencial Teórico

Antes de prosseguir, primeiramente é necessário entender um pouco sobre segurança da informação.

> A segurança da informação não está restrita a TI. Na verdade a segurança da informação faz parte de um universo de governança estratégica de empresa que planeja os riscos, as políticas de acesso e os usos da informação da empresa. Quando nos referimos ao termo “informação”, estamos nos referindo aos dados da empresa e informações de negócio que podem ser identificadas como “ativos estratégicos” da empresa. Esses ativos estratégicos podem ser relativos tanto a informações simples quanto a informações críticas para a continuidade [...]. (FREITAS, 2010, p.189).

Em um artigo publicado por Dorow (2010), o mesmo diz que um dos acontecimentos mais conhecidos relacionados à mitigação de riscos é o Acordo de Basiléia I de 1988 que ocorreu na cidade de Basiléia na Suíça. “O acordo de Basiléia tem o objetivo de fixar índices, criando uma padronização financeira mundial, tendo como objetivo diminuir o risco operacional, e consequentemente o risco das instituições financeiras ‘quebrarem’”. Neste mesmo artigo, o autor relata que a segunda versão do acordo de Basiléia, a de 2004 (Basiléia II), trouxe algumas melhorias que impactaram a TI, como: “capacidade de armazenamento de dados, integridade das transações, segurança, contingência, planejamento da capacidade, integridade na emissão de relatórios, entre outros”.

Percebe-se então que já faz algumas décadas que os estudiosos estão analisando as instituições financeiras com o objetivo de criarem acordos e garantir a segurança do sistema bancário mundial.

Conforme o *site* do Banco do Brasil, o principal objetivo do acordo de Basiléia II é “fortalecer a estabilidade do sistema financeiro mundial por meio do aprimoramento das práticas de gestão e governança dos riscos nas instituições financeiras com o aperfeiçoamento do Acordo anterior (Basiléia I)”.

O acordo de Basiléia II foi baseado em três grandes premissas, e uma delas trata-se do estímulo à adoção das melhores práticas de gestão de riscos, o qual exige das instituições financeiras consideráveis investimentos em tecnologia da informação, desenvolvimento de ferramentas de gestão, governança corporativa, cultura de risco e ajustes nas práticas de gestão.

Com o novo acordo publicado em 2004, o BACEN teve que se preparar para implantação. E de acordo com as publicações no *site*, “A implementação do Novo Acordo de Capital da Basileia no Brasil está sendo feita de forma gradual”.

Duarte Júnior et al. (2001, p.15-16), apud Matias (2012, p. 29) procuraram analisar a evolução da gestão dos riscos operacionais no Brasil e no mundo, estabelecendo os aspetos cruciais para seu desenvolvimento nas instituições financeiras brasileiras e também estabelecendo uma base comparativa para a evolução futura do mercado financeiro brasileiro. Nessa análise, os autores visam uma efetiva gestão dos riscos operacionais, na qual diziam que “Além da pressão reguladora, sinalizada pelo Novo Acordo de Capitais do BIS[2], a expectativa de perdas decorrentes de falhas humanas, tecnológicas, de processos internos ou sistêmicos é motivadora dessa reestruturação nas funções de gestão de riscos”.

De acordo com Figueiredo (2001, p. 24), apud Matias (2012, p. 21) a “intensidade dos riscos varia entre instituições de acordo com o tamanho, complexidade, volume de negócios e serviços, qualidade de seus recursos tecnológicos e humanos”. E que o objetivo da categorização dos riscos “é facilitar a identificação e o mapeamento dos riscos quer seja por produtos, processos, serviços ou unidades de negócios”.

Em um artigo publicado na revista DevMedia, escrito por Espinha e Sousa (2007), traz a análise de risco como “um instrumento de priorização das ações que devem ser tomadas pelas empresas para mitigar (reduzir as chances de ocorrência) os riscos identificados durante a fase de diagnóstico”. Nesse mesmo artigo, os autores citam também que:

> Toda oportunidade de sucesso sempre carrega consigo uma possibilidade de falha, cabendo a cada empresa avaliar a relação risco versus retorno e determinar se “estar” sujeito a esta perda é aceitável, se este evento é muito grave, ou ainda se o procedimento para a mitigação não oferece um retorno satisfatório. (ESPINHA; SOUSA, 2007).

Na visão de Peltier (2005), apud Ohtoshi (2008, p. 24) a gestão de riscos é um processo que, em geral, busca um equilíbrio entre a realização das oportunidades de ganhos e a minimização das vulnerabilidades e das perdas.

---

[2] BIS - Em 1930 foi criado o BIS (*Bank for International Settlements*), o Banco de Compensações Internacionais (www.bis.org). O BIS é uma organização internacional que fomenta a cooperação entre os bancos centrais e outras agências, em busca da estabilidade monetária e financeira. Disponível em: <http://www.bcb.gov.br/?BASILEIA>

> Gestão de risco é o processo que permite aos gestores de negócios equilibrarem os custos operacionais e econômicos das medidas de proteção para obter ganhos protegendo os processos de negócios que apoiam os objetivos de negócio ou missão da organização. Gestão de risco é o processo total usado para identificar, controlar e minimizar o impacto de eventos incertos. O objetivo da gestão de risco é reduzir o risco no desempenho de algumas atividades ou funções a um nível aceitável e obter a aprovação da alta direção. (PELTIER, 2005 apud Ohtoshi, 2008, p. 24)

Para fazer a gestão dos riscos, é imprescindível que os riscos sejam identificados e a análise seja feita. Segundo a norma ABNT NBR ISO/IEC 17799 (2005:06) convém que as análises de riscos "identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização". E que os resultados "orientem e determinem as ações de gestão apropriadas, as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra os riscos".

A análise de riscos é conhecida mundialmente e recomendada por diversas metodologias, guias e organizações do mundo. Nos parágrafos seguintes são apresentadas algumas.

Os modelos de qualidade de *software* mais conceituados atualmente, como CMMI[3] e MPS.BR[4], trazem em seus guias o processo de gerência de riscos, com o propósito de identificar, analisar, tratar, monitorar e reduzir continuamente os riscos em nível organizacional e de trabalho. Em ambos os modelos, o processo é requisito essencial para empresa atingir um determinado nível de maturidade.

Outra organização bastante conhecida mundialmente é a Organização Internacional para Padronização ou ISO. Dentre as inúmeras normas que esta organização apresenta, estão as normas ISO/IEC 27001, 27002 e 27005. Estas normas foram preparadas para prover um modelo que estabeleça, implemente, opere, monitore, analise criticamente, mantenha e melhore um Sistema de Gestão de Segurança da Informação (SGSI). As normas abordam a necessidade de ter a gestão de riscos e também fornecem diretrizes para o processo de gestão de riscos de sistemas de informação de uma instituição.

---

[3] CMMI - O "Capability Maturity Model® Integration" (CMMI) é uma abordagem de melhoria de processos que fornece às organizações elementos essenciais de processos eficazes, Disponível em: < http://www.sei.cmu.edu/cmmi/> Acesso em: 03 mar. 2014

[4] MPS.BR - É um programa mobilizador que foi criado em 2003 pela Softex para melhorar a capacidade de desenvolvimento de software nas empresas brasileiras. Disponível em: < http://www.softex.br/mpsbr/mps/mps-br-em-numeros/> Acesso em: 10 mar. 2014.

Para finalizar, temos o mercado de “melhores práticas” de governança em gestão de TI, que, dentre os vários modelos disponíveis, se destacam: o COBIT e o ITIL. Estes modelos trazem em seus guias e livros que, a essência da governança de TI está no valor, no risco e no controle, e que, sem o conhecimento e gerenciamento destes três itens, não será possível ter as informações precisas e disponíveis para tomada de decisões nas empresas. Em ambos os modelos, a gestão do risco é um dos pilares da governança, e seu conceito é garantir que as falhas não coloquem em risco os objetivos estratégicos da organização.

Procedimentos metodológicos

No trabalho foi utilizada a pesquisa de natureza explicativa, do tipo estudo de caso, e os dados foram coletados por meio de análise documental e observação participante.

Devido ao tema ser pouco explorado, era necessário formular uma proposta precisa e operacionalizável para tornar o problema mais esclarecido, ou seja, passível de investigação mediante experimentos. Além disso, as pesquisas deram suporte a todas as fases da elaboração do trabalho, auxiliando na definição do problema, na determinação dos objetivos, na construção da proposta, na fundamentação da justificativa, na elaboração das análises e na conclusão do estudo.

Com o auxilio das técnicas citadas anteriormente, para atingir o objetivo principal deste estudo, foram realizadas pesquisas bibliográficas na literatura relacionada à segurança da informação, principalmente nos modelos de referencia em gerenciamento de processo, projetos e desenvolvimento de *software* e também nas normas técnicas brasileiras.

E na tentativa de gerar uma proposta testável, passível de verificação da sua validade, foi utilizada a metodologia de análise qualitativa de riscos, o qual é atribuído uma escala de atributos qualificadores, descrevendo a magnitude das consequências potenciais (Baixo, Médio e Alto) e a probabilidade dessas consequências ocorrerem. Em seguida, foi realizada a avaliação das consequências, avaliação da probabilidade dos incidentes, determinação do nível de risco e

avaliação do risco. E por último, foi demonstrada a utilização da análise de riscos no processo de gestão de mudanças.

Estrutura do Trabalho

O trabalho foi divido em quatro capítulos, no primeiro são apresentados os principais conceitos e termos encontrados na análise de riscos e na segurança da informação. O segundo trás o propósito, os objetivos e as atividades do processo de gestão de riscos. No terceiro, é feita uma breve descrição sobre o ambiente de desenvolvimento das instituições financeiras e dos principais processos encontrados nesse ambiente, dando destaque ao processo de gerenciamento de mudanças. No quarto e último capítulo, é mostrado um exemplo de aplicação da atividade de análise de risco e apresentado o estudo sobre a utilização dessa atividade no processo de gerenciamento de mudanças dos ambientes de desenvolvimento.

1 CONCEITOS BÁSICOS E PRINCIPAIS TERMOS

A seguir serão apresentados os conceitos básicos encontrados na segurança da informação e na análise de riscos e os principais termos da área de estudo. O entendimento desses conceitos é importante para atingir o objetivo do trabalho e contextualizar os leitores a respeito do tema.

1.1 Segurança da Informação

Como citado anteriormente, para Diógenes e Mauser (2011, p.2, 3) a segurança da informação é a prática de assegurar que os recursos que proliferam informação sejam protegidos contra quebra de confidencialidade, comprometimento da integridade e contra a indisponibilidade.

Para esses mesmos autores, a confidencialidade, a integridade e a disponibilidade são os três pilares de alicerce para obter a segurança da informação e o primeiro passo para ter projetos de segurança em TI bem sucedidos.

Os três pilares representam os principais atributos que orientam a análise, o planejamento e a implementação da segurança para um determinando grupo de informações que se deseja proteger.

Cada pilar tem suas funções específicas, conforme as definições a seguir:

- Confidencialidade: Trata-se da prevenção do vazamento de informação para usuários ou sistemas que não estão autorizados a ter acesso a tal informação. Exemplo: um número de cartão vaza para outras fontes que não tinham autorização de ter aquele número.
- Integridade: Trata-se da preservação do dado na sua forma íntegra, ou seja, sem sofrer modificações através de fontes não autorizadas. Exemplo: uma mensagem transmitida é interceptada e modificada antes de chegar ao destinatário.
- Disponibilidade: Trata-se da manutenção da disponibilidade da informação, ou seja, a informação precisa estar disponível quando

se necessita. Exemplo: ao tentar fazer uma transação bancária, o sistema encontra-se indisponível.

Os outros atributos também importantes para obter a segurança da informação, são:

- Não repúdio: Trata-se da garantia de que o emissor de uma mensagem não possa, posteriormente, negar sua autoria. Exemplo: uma transação eletrônica gerada por uma assinatura digital.
- Autenticidade: Trata-se de uma informação que é proveniente da fonte que ela foi anunciada e que não seja alvo de modificações ao longo do processo. Exemplo: o controle de acesso por biometria.
- Confiabilidade: Trata-se da capacidade de um sistema realizar e manter o seu funcionamento independentemente das circunstâncias.

Já a ISO 27002 (2005, p.ix), trás o tema segurança da informação como a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar os riscos, maximizar o ROI e as oportunidades de negócio.

A norma também descreve que para obter essa segurança, é necessário a implementação de um conjunto de controles, incluindo políticas, processos, procedimentos, estruturas de organizações e funções de *hardware* e *software*. E que estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

O risco de segurança da informação é um termo bastante utilizado no processo de gestão de riscos. Este está associado ao potencial das ameaças em explorar vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, consequentemente, causar dano a uma organização.

De acordo com a ISO 27002 (2005, p.xi), é essencial que uma organização identifique os seus requisitos de segurança da informação, e para isso, existem três fontes principais:

I. A primeira é obtida a partir da análise de riscos para a organização, levando-se em conta os objetivos e as estratégias de negocio. Por meio da análise de riscos são identificadas as ameaças e vulnerabilidades aos ativos, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio (análise de riscos).

II. A segunda é a legislação vigente, os estatutos, a regulamentação e as causas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviços têm que atender, além de seu ambiente sociocultural (Requisitos legais).

III. Já a terceira é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações (Requisitos de Negocio).

Conforme os objetivos do trabalho, o foco será no primeiro princípio. E o subtópico seguinte, irá tratar os conceitos e termos relacionados a análise de riscos.

1.2 Análise de Riscos

Conforme descrito na norma ISO 27005 (2011), a análise de riscos é uma atividade do processo de gestão de riscos em que são identificados os riscos e seus componentes – ativos, ameaças, oportunidades, vulnerabilidades, probabilidade e consequências (impacto). E que a probabilidade de ocorrência do cenário de risco e suas consequências devem ser avaliadas, resultando em um nível de risco. Esse risco é então avaliado segundo critérios pré-definidos que determinarão a sua importância para a organização.

Então, entende-se que a atividade de análise de risco tem o objetivo de compreender a natureza do risco e determinar o nível de risco.

De acordo com o Guia PMBOK (2013) o risco é um evento ou uma condição incerta que, se ocorrer, poderá ter efeitos positivos ou negativos em pelo menos um objetivo estratégico da organização.

E o nível de risco, segundo a norma ISO 27005 (2011) é a magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades.

Nessa mesma norma, na seção de termos e definições, diz que a consequência é o resultado de um evento que afeta os objetivos, podendo ser, por exemplo, a perda da confidencialidade, da integridade ou da disponibilidade dos ativos, condições adversas de operação, reputação afetada, prejuízo etc. Já a probabilidade é a chance de algo acontecer.

Para determinar o nível de riscos e gerar uma lista de riscos com níveis de valores designados, primeiramente a análise de riscos irá avaliar e atribuir valores para a probabilidade de um evento ocorrer e para a consequência desse evento. Em seguida, a combinação desses dois valores possibilitará classificar o risco como, prioridade baixa, média ou alta.

Cada risco é classificado de acordo com a sua probabilidade de ocorrência e impacto em um objetivo, se realmente ele ocorrer.

Porém, para realizar a avaliação das consequências e das probabilidades, primeiramente é necessário identificar os riscos. Nessa etapa, a coleta de alguns dados será necessária para realizar as análises e as avaliações, como: Identificar ativos, ameaças, vulnerabilidades e consequências.

A norma ISO 27005 (2011) diz que uma metodologia para análise pode ser qualitativa ou quantitativa, ou uma combinação de ambos. A análise qualitativa é frequentemente utilizada primeira, para obter uma indicação geral do nível de risco e revelar os grandes riscos, se baseado em estimativas de impacto. Já a quantitativa, se necessário, poderá ser efetuada posteriormente, para buscar um nível baixo de detalhamento do risco. Neste caso, é necessário utilizar dados históricos de incidentes, para gerar números.

Após a etapa de identificar, analisar e priorizar os riscos é gerada uma lista de riscos avaliados, ordenados por prioridade de acordo com os critérios de avaliação de riscos. Essa lista é então utilizada pelos tomadores de decisões (gestores) para analisarem a melhor estratégia de mitigar os riscos a um nível aceitável ou aceitar os riscos.

As normas ISO 27002(2005) e ISO 27005 (2011), e o Guia PMBOK (2013) trazem algumas definições para completar o entendimento de todos os termos utilizados na análise de riscos, que são:

- Evento: Ocorrência ou mudança em um conjunto específico de circunstâncias. Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas e em algumas vezes pode ser referido como um incidente ou um acidente.
- Ativo: Qualquer coisa que tenha valor para a organização.
- Ameaça: Causa potencial de um incidente indesejado, que pode resultar em um dano para o sistema ou organização.
- Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorado por uma ou mais ameaças.
- Mitigar riscos: É uma estratégia de resposta ao risco, com o objetivo de reduzir a probabilidade de ocorrência, ou impacto do risco.
- Aceitar riscos: É uma estratégia de resposta pelo qual decide reconhecer o risco e não agir, a menos que o risco ocorra.

O tópico seguinte irá detalhar o funcionamento do processo de gestão de riscos e aprofundar nas técnicas utilizadas para realizar a análise de riscos.

1.3 Gestão de Mudanças

De acordo com Freitas (2010) uma mudança é “A adição, modificação ou remoção de um serviço autorizado, planejado e suportado e/ou de seus componentes e documentação associada”.

A dependência que o negocio tem dos sistemas de informações e tecnologia faz com que um gerenciamento de mudanças gaste um tempo precioso:

- Analisando e estimando o impacto da mudança de TI no negócio da empresa;

- Identificando os problemas que continuam a aparecer e que requerem mais mudanças;
- Introduzindo novas ideias e dispositivos que causem ainda mais mudanças;

Se mudanças podem ser gerenciadas para otimizar a exposição ao risco, severidade de impacto e transtorno, e claro serem bem sucedidas numa primeira tentativa, o resultado final para o negócio está na realização antecipada de benefícios, com uma economia de dinheiro e tempo.

Mudanças aparecem como resultados de problemas, mas muitas mudanças podem vir de busca proativa de benefícios, tais como, redução de custos ou melhoria nos serviços.

O objetivo do gerenciamento de mudanças é garantir que métodos e procedimentos padronizados sejam utilizados de maneira eficiente, para minimizar os impactos no negócio causados por mudanças nos aplicativos bancários sem o devido planejamento, aumentando a disponibilidade do serviço e consequentemente melhorando a qualidade de maneira geral.

O gerenciamento de mudanças assegura que alterações no ambiente produtivo passem por avaliações de potenciais riscos, antes de sua implantação, evitando danos ou ameaças à estabilidade dos serviços em operação.

Todas as mudanças em TI devem ser justificadas, avaliadas, autorizadas, planejadas e gerenciadas para garantir que a sua implementação não cause impactos nos serviços de TI que suportam o negócio. Isso permite que os riscos sejam minimizados através do planejamento da implantação das mudanças e que estas, uma vez aprovada, sejam executadas dentro dos seguintes requisitos: custo, prazo e qualidade.

Uma premissa básica para fazer uma gestão de mudança, de acordo com o Guia ITIL *Service Transition* (2008) é que: “Nada muda no ambiente de produção de TI sem antes ser avaliado, planejado e aprovado”.

2 GESTÃO DE RISCOS DE SEGURANCA DA INFORMAÇÃO

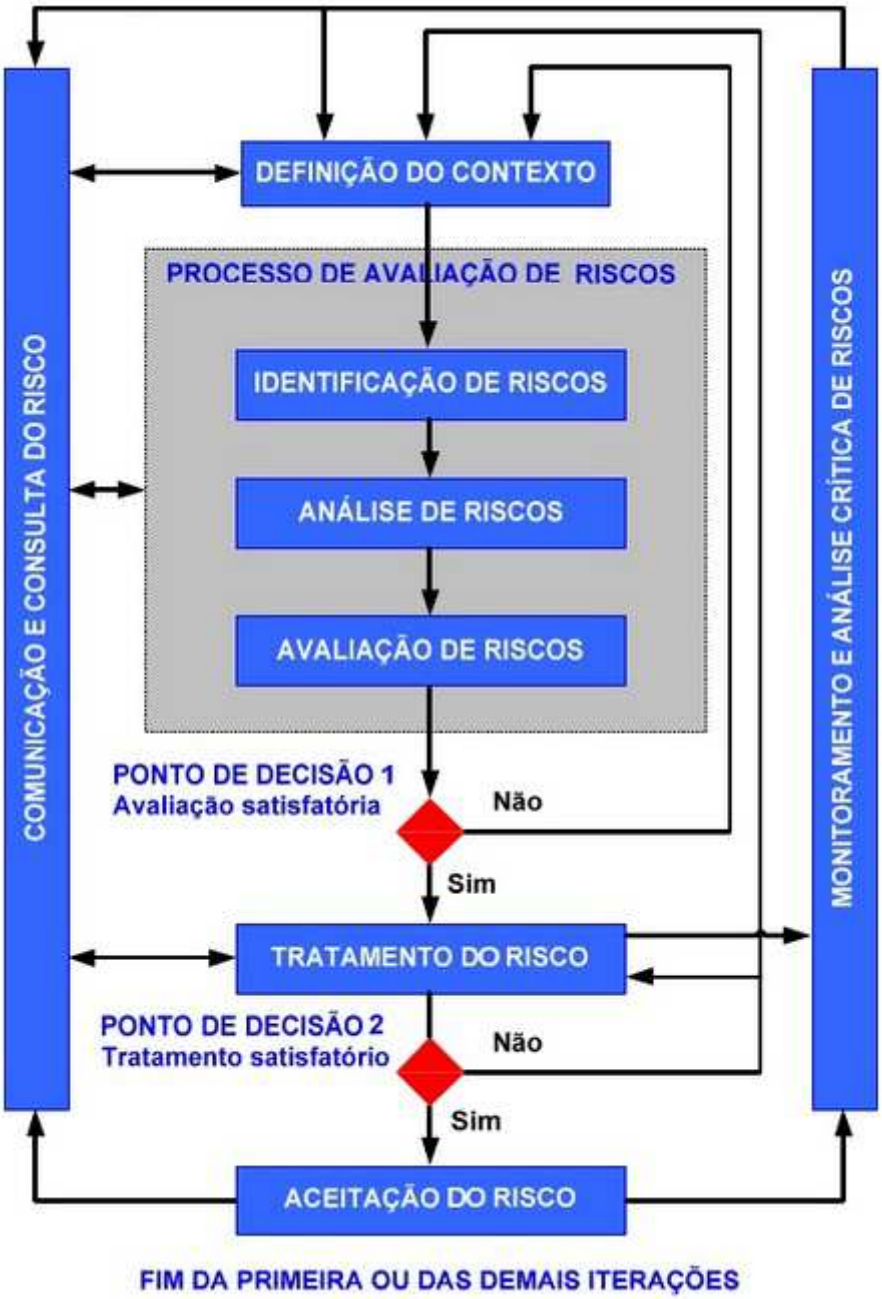
De acordo com o guia MPS.BR (2013) o propósito do processo de gestão de riscos é identificar, analisar, tratar, monitorar e reduzir continuamente os riscos em um nível organizacional e de trabalho.

Já no guia PMBOK (2013), os objetivos do processo de gestão de riscos são aumentar a probabilidade e o impacto de eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos.

A norma ISO 27005 (2011) diz que o processo de gestão de riscos pode ser aplicado a organização como um todo, a uma área específica da organização (por exemplo, departamento, local físico, serviço), a qualquer sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (por exemplo: o plano de continuidade de negócios).

A norma ISO 27005 (2011) também traz uma visão de alto nível do processo de gestão de riscos, conforme apresentado na figura 1. E esta será utilizada como base, neste trabalho, para descrever o funcionamento do processo de gestão de riscos.

Figura 1 – Processo de Gestão de riscos



Fonte - ABNT NBR ISO/IEC 27005 (2011, p.14)

O processo de gestão de riscos começa com a definição do contexto. Em seguida é feita a análise/avaliação de riscos, em que os riscos são identificados, estimados, avaliados segundo critérios definidos no momento do estabelecimento do contexto. No fim dessa fase, há o primeiro ponto de decisão. Caso as informações sejam suficientes para tratar o risco, ou seja, reduzi-lo a um nível aceitável, então a

tarefa está completa e o tratamento do risco pode suceder. Caso contrário, deverá ser realizada a revisão do contexto.

A etapa de tratamento de riscos é onde os riscos podem ser reduzidos, retidos, evitados ou transferidos. É possível que o tratamento do risco não resulte em um nível de risco residual que seja aceitável. Nessa situação, pode ser necessária outra iteração do processo de avaliação de riscos (ponto de decisão 2).

A atividade de aceitação do risco tem de assegurar que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. A comunicação do risco deve ser feita durante todo o processo, pois as informações sobre os riscos e o modo como serão tratados, podem ser úteis para os gestores e para as áreas operacionais no gerenciamento de algum incidente.

Já o monitoramento cotidiano e a análise crítica são necessários para assegurar que o contexto, o resultado da análise de riscos e do tratamento do risco, assim como os planos de gestão, permaneçam relevantes e adequados às circunstâncias.

A seguir serão descritas cada uma das atividades apresentadas acima.

2.1 Definição do Contexto

Nessa etapa do processo é quando ocorre a definição dos critérios básicos necessários para a segurança da informação, do escopo, dos limites e do responsável por conduzir o processo de gestão de riscos.

De acordo com a norma ISO 27005 (2011), os critérios básicos devem ser definidos e especificados. Pois são importantes para conduzir o processo de gestão de riscos e para garantir a segurança da informação. A norma recomenda levar em conta três critérios durante o desenvolvimento do processo, são eles:

- Critérios para a avaliação de riscos: utilizado para avaliar os riscos de segurança da informação na organização, levando em consideração: o valor estratégico do processo que trata as informações de negócio, a criticidade dos ativos envolvidos, os requisitos legais e regulatórios, bem como as obrigações

contratuais, a importância, pelo ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade e as consequências negativas para a organização (valores tangíveis e intangíveis).

- Critérios de impacto: utilizado para verificar danos ou custos a organização, levando em consideração: o nível de classificação do ativo de informação afetado, a ocorrências de violação da segurança da informação, as operações comprometidas, as perdas de oportunidades e valor financeiro, o não cumprimento de prazos, o dano à reputação e a violação de requisitos legais, regulatórios e contratuais.
- Critérios para a aceitação do risco: utilizado para definir os níveis de aceitação do risco, levando em consideração as políticas, metas e objetivos da organização, assim como dos interesses das partes interessadas.

Já o escopo precisa ser definido para assegurar que todos os ativos relevantes sejam considerados no processo de avaliação de riscos e os limites aceitáveis identificados, para ajudar o reconhecimento dos riscos e propor respostas específicas.

Tendo essa base, será possível incluir ou excluir ativos para análise e também saber em qual escala de gravidade determinado risco identificado está enquadrado (baixo, médio, alto ou fora dos limites definidos).

Outro ponto importante, recomendado em várias metodologias, melhores práticas e normas, é a definição de papeis e responsabilidades dentro do processo. Ou seja, pessoas ou equipes responsáveis por estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o processo de gestão de riscos.

2.2 Processo de Avaliação de Riscos

O propósito dessa etapa do processo é identificar os riscos, analisá-los quantitativamente ou qualitativamente e priorizá-los em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

O processo de avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades existentes (ou que poderiam existir), identifica os controles existentes e seus efeitos no risco identificado, determina as consequências possíveis e, finalmente, prioriza os riscos derivados e ordena-os de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto.

A norma ISO 27005 (2011) traz o processo de avaliação de riscos dividido em três atividades, que serão descritas a seguir.

2.2.1 Identificação de Riscos

De acordo com a norma ISO 27005 (2011) o propósito da identificação de riscos é determinar os eventos que possam causar uma perda potencial. E as atividades desenvolvidas na identificação são as seguintes:

I. Identificação de ativos: Esta atividade consiste em identificar os ativos que estejam dentro do escopo estabelecido e que requerem proteção. Há dois tipos de ativos: os ativos primários, que consistem dos principais processos e informações das atividades incluídas no escopo, por exemplo: processos cuja interrupção, mesmo que parcial, torna impossível cumprir a missão da organização; e ativos de suporte e infraestrutura sobre os quais os elementos primários do escopo se apoiam, podendo ser dos tipos: *hardware*, *software*, aplicações de negócio, rede, recursos humanos, instalações físicas etc, por exemplo: um sistema crítico para organização cuja indisponibilidade, evitará o cumprimento dos seus objetivos.

II. Identificação de ameaças: Esta atividade consiste em identificar as ameaças e suas fontes. Como a ameaça tem o potencial de

comprometer os ativos, elas podem ser intencionais, acidentais ou de origem natural e podem resultar, por exemplo, no comprometimento ou paralisação de serviços essenciais. As informações para identificação das ameaças podem ser obtidas, por exemplo, com o responsável pelo ativo e seus usuários.

III. Identificação dos controles existentes: Esta atividade consiste em identificar os controles existentes e planejados. Isso é importante, pois evitará custos e trabalho desnecessário, por exemplo, na duplicação de controles. Além disso, enquanto os controles existentes estão sendo identificados, é feita uma verificação para assegurar que eles estão funcionando corretamente. Esses controles são necessários para tratar efetivamente o risco identificado. As informações para identificação dos controles existentes podem ser obtidas, por exemplo, com as pessoas responsáveis pela segurança da informação, com os resultados de auditorias etc.

IV. Identificação das vulnerabilidades: Esta atividade consiste em identificar as vulnerabilidades que podem ser exploradas por ameaças para comprometer ativos ou a organização. Para vulnerabilidade causar um prejuízo é preciso ter uma ameaça presente para explorá-la. Uma vulnerabilidade que não tenha uma ameaça correspondente, não requer a implementação de controles no presente momento, mas convém que ela seja reconhecida e monitorada, no caso de haver mudanças. As informações para identificação das vulnerabilidades podem ser obtidas, por exemplo, utilizando métodos de testes, como avaliação e testes de segurança, teste de invasão, análise crítica de um código etc.

V. Identificação das consequências: Esta atividade consiste em identificar as consequências que a perda de confidencialidade, integridade e disponibilidade podem ter sobre os ativos, na ocorrência de um incidente. Uma consequência pode ser, por exemplo, a perda de eficácia, condições adversas de operação, prejuízos etc.

2.2.2 Análise de Riscos

A análise de risco é realizada utilizando diferentes graus de detalhamento, dependendo da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores.

A norma ISO/IEC 13335-3 (1998), que trata de técnicas para a gestão de segurança de TI, apresenta quatro tipos de análise de riscos, que diferenciam pelo nível de detalhamento, são elas:

- Método Básico: Selecionam as correções padrões, as similares adotadas por muitos sistemas que estão rodando na organização. Esse método é recomendado para sistemas que tem um nível baixo de requisitos de segurança. Ele também requer um mínimo de recurso e pouco tempo de esforce de TI para implementação.
- Método Informal: Exploram o conhecimento e a experiência das pessoas. Porém, sem um processo formal, os detalhes importantes são perdidos em uma próxima análise ou pode ser um problema se a pessoa que fez a análise de risco deixar a organização. Este método também não requer muito recurso e tempo.
- Método de análise de risco detalhada: Conduz uma análise de risco detalhada para todos os sistemas de TI na organização. Esse processo envolve em detalhes a identificação e avaliação dos ativos, determinação das ameaças e vulnerabilidades. Os resultados da análise são usados para estimar os riscos, além de identificar e justificar correções de segurança.
- Método combinado: conduz uma análise inicial de alto nível para todos os sistemas de TI, concentrando os valores do negócio que tais sistemas possuem, bem como os riscos a que estes sistemas estão expostos. Esse método é rápido e simples, os recursos e investimentos podem ser aplicados aonde houver maior benefício,

> e sistemas que tenham maior necessidade de proteção devem ser priorizados.

Os métodos de análise citados acima utilizam dois tipos de metodologia, a análise qualitativa e a quantitativa.

A análise qualitativa é utilizada para obter uma indicação geral do nível de risco e para revelar os grandes riscos. Ela utiliza uma escala de atributos qualificadores que descrevem a grandeza das consequências potenciais, podendo ser baixo, médio ou alto, e a probabilidade dessas consequências ocorrerem.

Já a análise quantitativa é utilizada para obter informações mais detalhadas e específicas dos grandes riscos. Ela utiliza uma escala de valores numéricos, tanto para consequências, quanto para a probabilidade, usando dados de diversas fontes. A qualidade da análise depende da exatidão e da integridade dos valores numéricos.

A etapa do processo que realiza a análise de riscos envolve três atividades essenciais, que serão apresentadas a seguir: Avaliação das consequências, avaliação da probabilidade dos incidentes e determinação do nível de riscos.

2.2.2.1 Avaliação das consequências

Para iniciar esta atividade, é necessário ter uma lista de cenários de incidentes identificados como relevantes, incluindo a identificação das ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos de negócio. Isso irá facilitar a valorização dos ativos e avaliação dos impactos.

Primeiramente, devem ser atribuídos valores aos ativos relevantes. Esses valores podem ser expressos de forma qualitativa, quantitativa ou uma combinação de ambos.

A valorização dos ativos começa com a classificação, levando em conta a criticidade do ativo, em função da sua importância para a realização dos objetivos de negócio da organização. Essa valorização é determinada de duas maneiras:

- Pelo custo da recuperação e reposição da informação e
- Pelas consequências ao negócio, relacionadas à perda ou ao comprometimento do ativo.

Na valorização dos ativos é importante lembrar que quanto mais relevantes e numerosos os processos de negócio apoiados por um ativo, maior é o seu valor.

A valoração dos ativos representa um dos aspectos mais importantes na avaliação do impacto de um cenário de incidente, pois o incidente pode afetar mais de um ativo (por exemplo: os ativos dependentes) ou somente parte de um ativo. Diferentes ameaças e vulnerabilidades causarão diferentes impactos sobre os ativos, tais como perda da confidencialidade, da integridade ou da disponibilidade.

Portanto a avaliação das consequências está relacionada à valoração dos ativos baseada na análise de impacto no negócio.

2.2.2.2 Avaliação da probabilidade dos incidentes

Para iniciar essa atividade, também será necessário ter uma lista de cenários de incidentes, incluindo a identificação das ameaças, vulnerabilidades, ativos que foram afetados e as consequências para os ativos e processos de negócio.

Nessa etapa do processo também poderá ser utilizada tanto a técnica de análise qualitativa, como a técnica de análise quantitativa para avaliar a probabilidade de ocorrência de algum cenário de incidente.

Tendo os cenários de incidentes identificados, para realizar a análise da probabilidade, será necessário combinar a frequência da ocorrência das ameaças, com a facilidade de exploração das vulnerabilidades, e uma das formas para colher esses dados, é considerar as experiências passadas.

2.2.2.3 Determinação do nível de riscos

Já nessa etapa do processo de análise dos riscos, uma lista de cenários de incidentes, com suas consequências associadas aos ativos, processos de negócio e suas probabilidades, geradas nas atividades anteriores, será necessária.

Com os valores atribuídos para a probabilidade e para a consequência de um risco, será possível, por meio de uma combinação da probabilidade de um cenário de incidente e suas consequências, determinar o nível do risco.

A saída dessa última atividade do processo de análise de riscos será uma lista contento os riscos e seus respectivos níveis de valores, que deverá ser utilizada na atividade seguinte, a avaliação dos riscos.

2.2.3 Avaliação dos riscos

Utilizando os critérios de avaliação e impacto dos riscos, decididos durante a etapa de definição do contexto, juntamente com o levantamento dos riscos estimados na etapa de análise, será possível realizar a avaliação dos riscos.

A norma ISO 27005 (2011) recomenda que as decisões tomadas durante a atividade de avaliação de riscos sejam baseadas, principalmente, no nível de risco aceitável. No entanto, convém que as consequências, a probabilidade e o grau de confiança na identificação e análise de riscos também sejam considerados.

Outro ponto importante, que deve ser observado durante a etapa de avaliação de riscos, é considerar os requisitos contratuais, legais e regulatórios que a organização deve cumprir.

No final dessa etapa, uma lista com os riscos priorizados deve ser disponibilizada para etapa seguinte, que é a de tratamento dos riscos.

2.3 Tratamento do Risco

Nessa etapa do processo, o objetivo é reduzir o risco a um nível aceitável, criando um plano de tratamento de riscos, baseado em controles para modificar, aceitar, evitar ou compartilhar os riscos.

A norma ISO 27005 (2011) descreve quatro opções para tratamento de riscos, são eles: modificação do risco; aceitação do risco; ação de evitar o risco; e o compartilhamento do risco.

Convém que as opções do tratamento do risco sejam selecionadas com base no resultado do processo de avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos.

Uma vez que o plano de tratamento do risco tenha sido definido, os riscos residuais precisam ser determinados. Isso envolve uma atualização ou uma repetição do processo de avaliação de riscos, considerando-se os efeitos previstos do tratamento do risco que foi proposto. Caso o risco residual ainda não satisfaça os critérios para a aceitação da organização, uma nova iteração do tratamento do risco pode ser necessária antes de se prosseguir à aceitação do risco.

No final dessa etapa, um plano de tratamento de riscos, com as ações e controles necessários para reduzir os riscos para um nível aceitável é gerado, juntamente com os riscos residuais. Estes deverão ser disponibilizados para a próxima etapa do processo, a aceitação do risco.

2.4 Aceitação do Risco

Nessa etapa do processo as decisões de aceitar os riscos são tomadas e formalmente registradas, juntamente com as responsabilidades pela decisão.

Essas decisões são tomadas pelos gestores responsáveis, que fazem uma análise crítica dos planos propostos de tratamento do risco e dos riscos residuais, em seguida aprovam, se for o caso, registram as condições associadas a essa aprovação.

Com a lista de riscos aceitos, incluído as justificativas para aqueles que não satisfaçam os critérios normais para aceitação do risco, já será possível realizar a implementação dos controles para mitigar os riscos.

2.5 Comunicação e Consulta do Risco

A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, compartilhando as informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos.

A comunicação eficaz entre as partes interessadas é importante, uma vez que isso pode ter um impacto significativo sobre as decisões que devem ser tomadas.

Convém que a organização desenvolva planos de comunicação dos riscos tanto para as operações rotineiras como também para situações emergenciais. Portanto, convém que a atividade de comunicação do risco seja realizada continuamente.

2.6 Monitoramento e Análise Crítica de Riscos

Esta última fase do processo é feito dois tipos de monitoramento, um nos riscos e seus fatores e o outro no processo de gestão de riscos.

Convém que o monitoramento e a análise crítica dos fatores de riscos sejam feitos a fim de identificar, o mais rápido possível, eventuais mudanças no contexto da organização e manter uma visão geral dos ricos.

Como os riscos não são estáticos, as ameaças, as vulnerabilidades, a probabilidade ou consequências podem mudar de repente, sem qualquer indicação. Portanto, o monitoramento constante é necessário para que se detectem essas mudanças.

A norma ISO 27005 (2011) recomenda que alguns itens devam ser monitorados continuamente:

- Novos ativos que tenham sido incluídos no escopo da gestão de riscos;
- Modificações necessárias dos valores dos ativos;
- Novas ameaças ativas, tanto fora, quanto dentro da organização;
- As vulnerabilidades novas ou ampliadas;
- As vulnerabilidades já identificadas;
- As consequências ou o impacto ampliado de ameaças, vulnerabilidades e riscos avaliados;
- Incidentes relacionados a segurança da informação.

Quanto ao processo de gestão de riscos, convém que seja continuamente monitorado, analisado criticamente e melhorado, quando necessário e apropriado.

O monitoramento cotidiano e a análise crítica são necessários para assegurar que o contexto, o resultado do processo de avaliação de riscos e do tratamento do risco, assim como os planos de gestão, permaneçam relevantes e adequados.

As melhorias no processo devem ser comunicadas aos gestores apropriados, para que possam ter certeza que, nenhum risco seja ignorado ou subestimado, que as ações necessárias sejam executadas e as decisões corretas sejam tomadas.

A atividade de monitoramento do processo de gestão de riscos deverá lidar com:

- Contexto legal e ambiental;
- Contexto da concorrência;
- Abordagem do processo de avaliação de riscos;
- Valor e as categorias dos ativos;
- Critérios de Impacto;

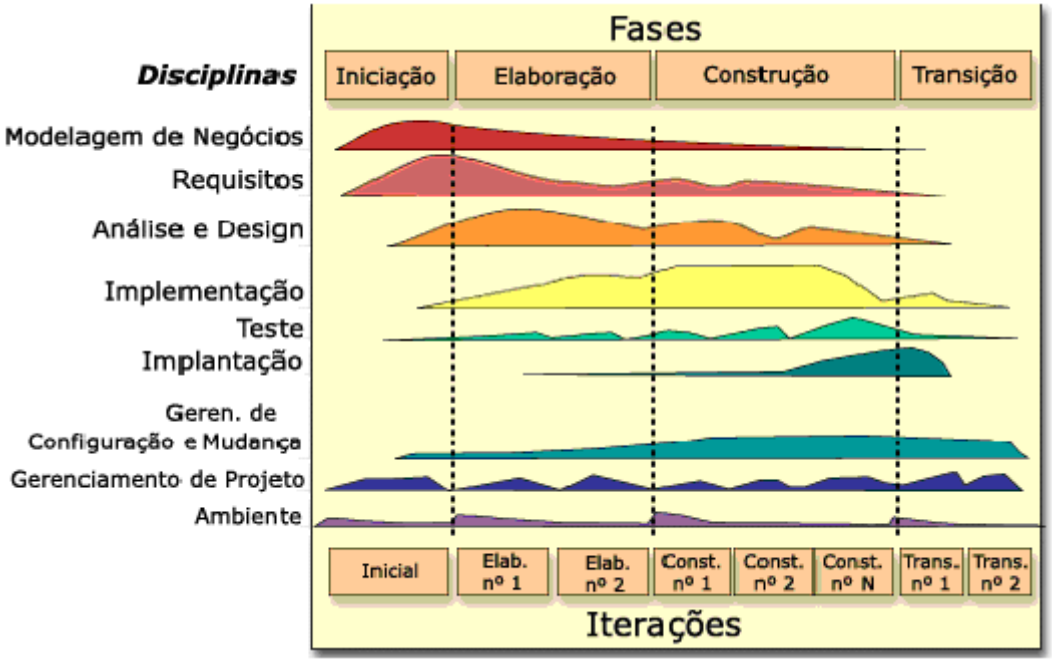
- Critérios para avaliação de riscos;
- Critérios para aceitação de riscos;
- Custo total de propriedade;
- Recursos humanos.

3 AMBIENTE DE DESENVOLVIMENTO DE SISTEMAS

Este capítulo tem o objetivo de apresentar os principais processos encontrados no ambiente de desenvolvimento de sistemas das instituições financeiras bancárias e envolvidos no atendimento de demandas do tipo: manutenção evolutiva[5] e manutenção corretiva[6].

A metodologia de desenvolvimento de sistema utilizada como exemplo, para extrair os processos e apresentar as atividades envolvidas no atendimento das demandas, será o processo unificado.

Figura 2 – Processo Unificado



Fonte – http://pt.wikipedia.org (2014)

A figura 2 mostra o ciclo de vida de desenvolvimento de *software* na visão do processo unificado. Este método é dividido em quatro fases sequenciais, onde cada fase é concluída por um marco principal. No final de cada fase, uma avaliação

[5] Manutenção Evolutiva: Pode ser do tipo: Adaptativa, quando há adequação do software para acomodar mudanças em seu ambiente externo; Perfectiva, quando o cliente exige acréscimos funcionais; e Preventiva, quando é necessário melhorar a confiabilidade e manutenibilidade futura.

[6] Manutenção Corretiva: Quando há necessidade de diagnósticos e correções de erros;

é executada para determinar se os objetivos da fase foram alcançados. Uma avaliação satisfatória permite que a demanda passe para próxima fase.

Para atingir o objetivo do trabalho, o processo de gerenciamento de mudanças será o responsável por aplicar a análise de riscos no ambiente de desenvolvimento de *softwares*, com o propósito de extrair as informações necessárias para serem utilizadas no seu processo.

A seguir serão apresentados os principais processos envolvidos no desenvolvimento das aplicações bancárias e os fluxos de atendimento das demandas, dando destaque ao processo de gerenciamento de mudanças.

3.1 Processos de Atendimento de Demandas

No ambiente de desenvolvimento de sistemas das instituições bancárias, podemos encontrar diversos processos de atendimento de demanda, que irão depender do caráter e da natureza da mudança solicitada. Neste trabalho será tratado somente as demandas de manutenção de *software*, que é um processo de melhoria e otimização do *software* já desenvolvido, ou seja, com uma versão em produção, como também o reparo de defeitos.

As demandas de manutenção de *software* podem ser de natureza, evolutiva, corretiva ou eventual. O seu enquadramento vai depender do que foi solicitado. As de natureza evolutiva, consideradas como melhorias, são as mudanças provocadas pela evolução do aplicativo, por exemplo, a criação de novas funcionalidades para melhorar a aplicabilidade e usabilidade do *software*. Já as corretivas, consideradas como defeitos, são as mudanças provocadas por ocorrências de erros, visando a sua respectiva solução. Enquanto que as eventuais, consideradas como serviços, são as mudanças que visam realizar pesquisas para detecção de erros ou subsidiar análise gerencial ou geração de relatório e que não se enquadra nas demais naturezas existentes.

Outra natureza de manutenção das aplicações, bastante comum nas instituições bancárias, são as do tipo manutenções legais. Estas mudanças são introduzidas para atender uma determinação legal, ou seja, provocada por uma nova legislação. Elas têm como características possuir uma data de implantação vinculada à data na qual a nova legislação entrará em vigor.

Quanto ao caráter da mudança, existem dois: a emergencial, que são as mudanças provocadas pela ocorrência de incidentes ou por situações que causem prejuízo financeiro ou de imagem a instituição, exigindo um atendimento tempestivo da demanda, e a normal, que não se enquadra no caráter emergencial.

A seguir serão apresentados dois exemplos de atendimento de demandas, um para manutenção evolutiva e outro para manutenção corretiva.

Baseado na metodologia de desenvolvimento de sistemas adotada nesse trabalho, os fluxos a seguir, mostram os principais processos envolvidos no atendimento de demandas evolutivas e corretivas.

Esses fluxos exemplificam, de forma macro, o caminho percorrido por uma demanda, durante o seu ciclo de desenvolvimento, até ser implantada em produção.

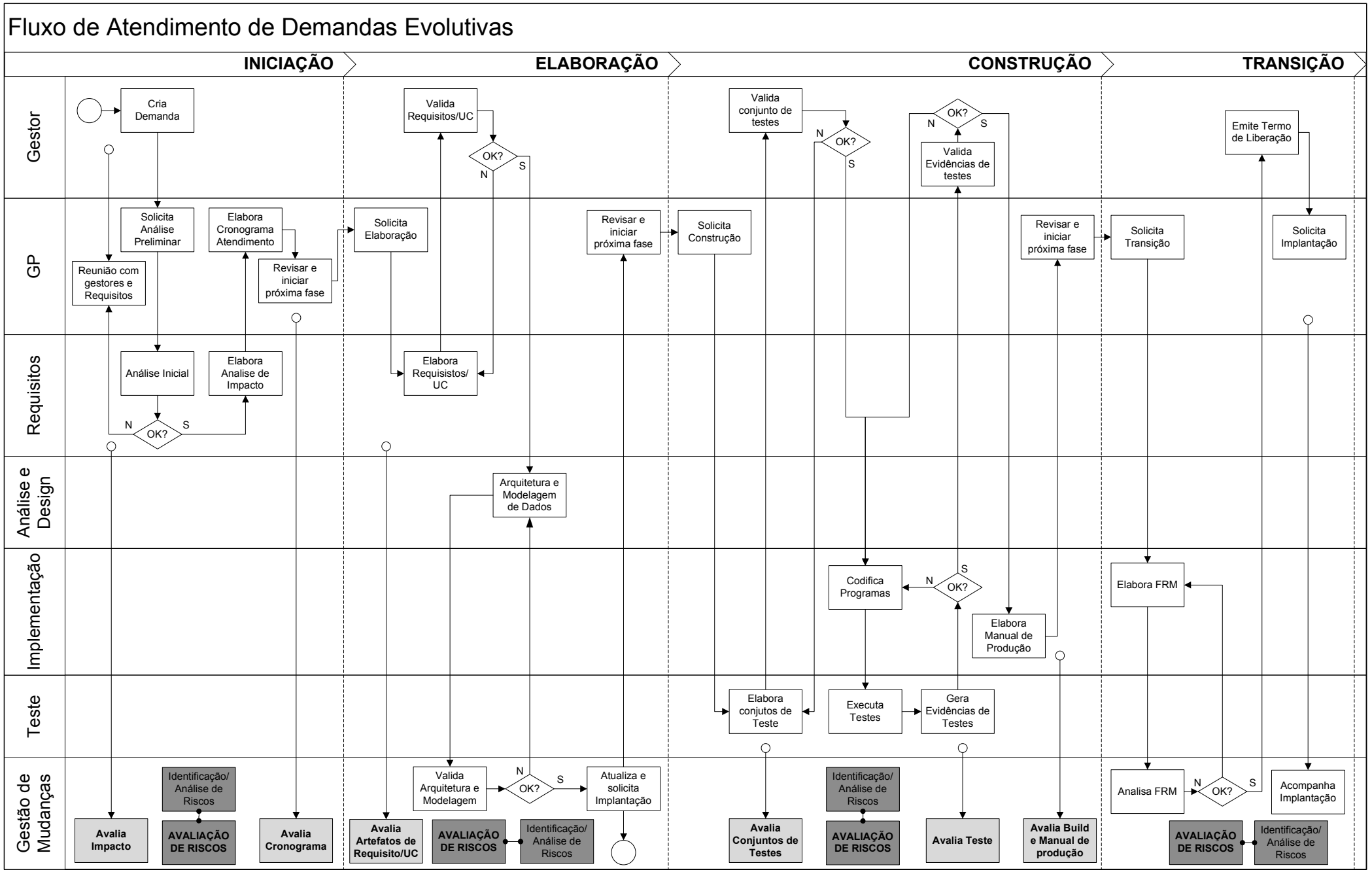
Nota-se que no final de cada fase, há um marco, o qual orienta o responsável pelo processo de Gestão de Projetos (GP) a fazer revisões nas atividades e nos produtos entregues da fase atual e para em seguida autorizar a iniciação da próxima fase. Esse modelo de desenvolvimento permite que a qualquer momento, caso uma falha seja encontrada, seja possível voltar às atividades das fases anteriores.

As atividades referenciadas nos marcos podem minimizar a ocorrência de algumas falhas, porém, a maior parte são falhas relacionadas ao escopo, custo e prazos planejados. Já as falhas de desenvolvimento de sistemas, ou seja, aquelas relacionadas à qualidade, desempenho, usabilidade, confiabilidade, satisfação do cliente, entre outros, não são detectadas por essas atividades.

Então, conforme destacado nos fluxos, surgiu uma proposta de aplicar a técnica de análise de riscos no processo de gerenciamento de mudanças, o qual faz

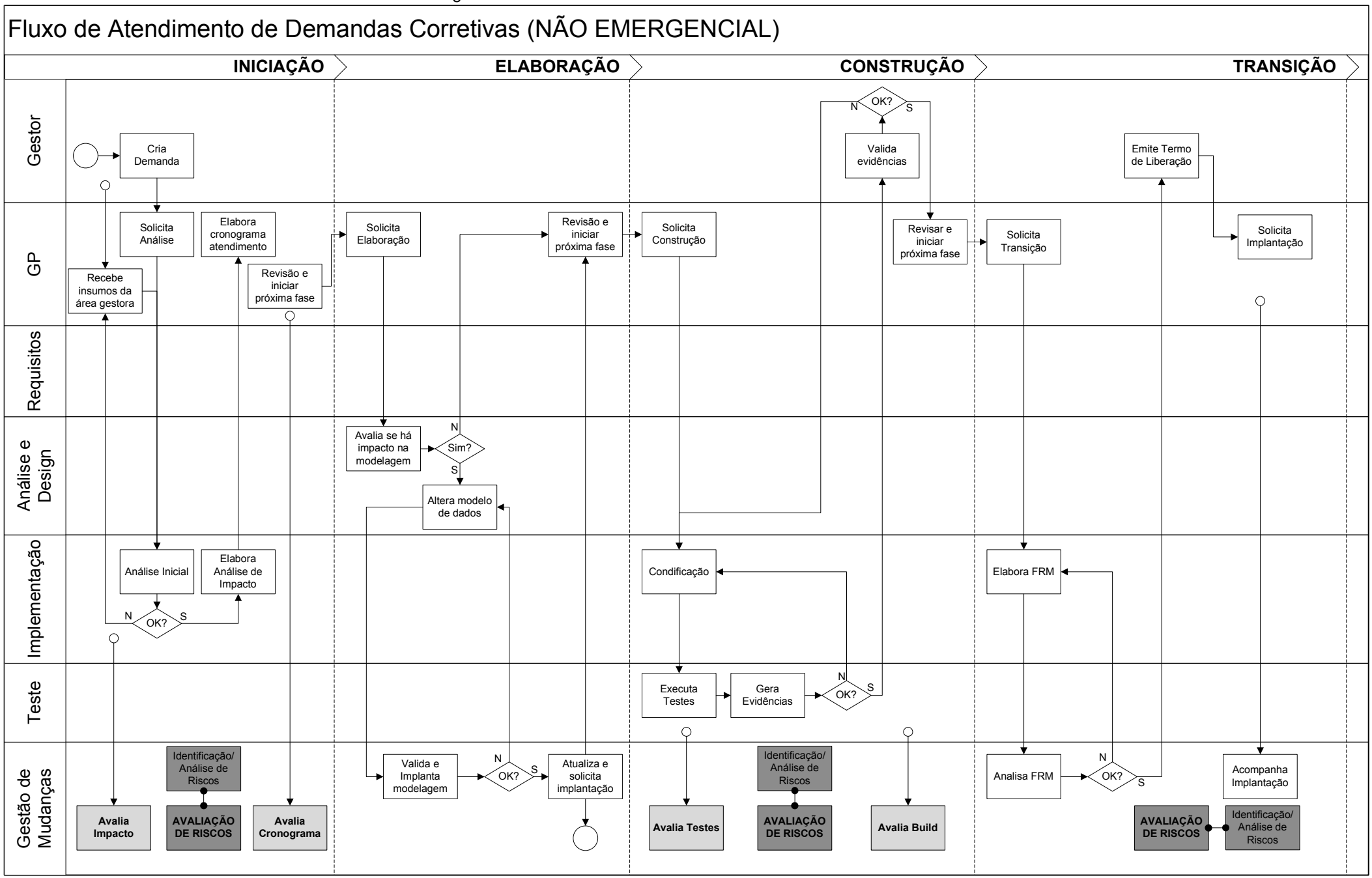
uma análise mais crítica em cada fase do ciclo de vida de desenvolvimento, e detecta falhas e erros antes de implantar a mudança em produção. Além de melhorar o processo de gerenciamento de mudanças, a análise de riscos servirá também para conscientizar os gestores do negócio sobre os riscos envolvidos em determinadas mudanças.

Fluxo 1 – Atendimento de Demandas Evolutivas.



Fonte – Elaborado pelo autor.

Fluxo 2 – Atendimento de Demandas Corretivas não Emergenciais.



Fonte – Elaborado pelo autor.

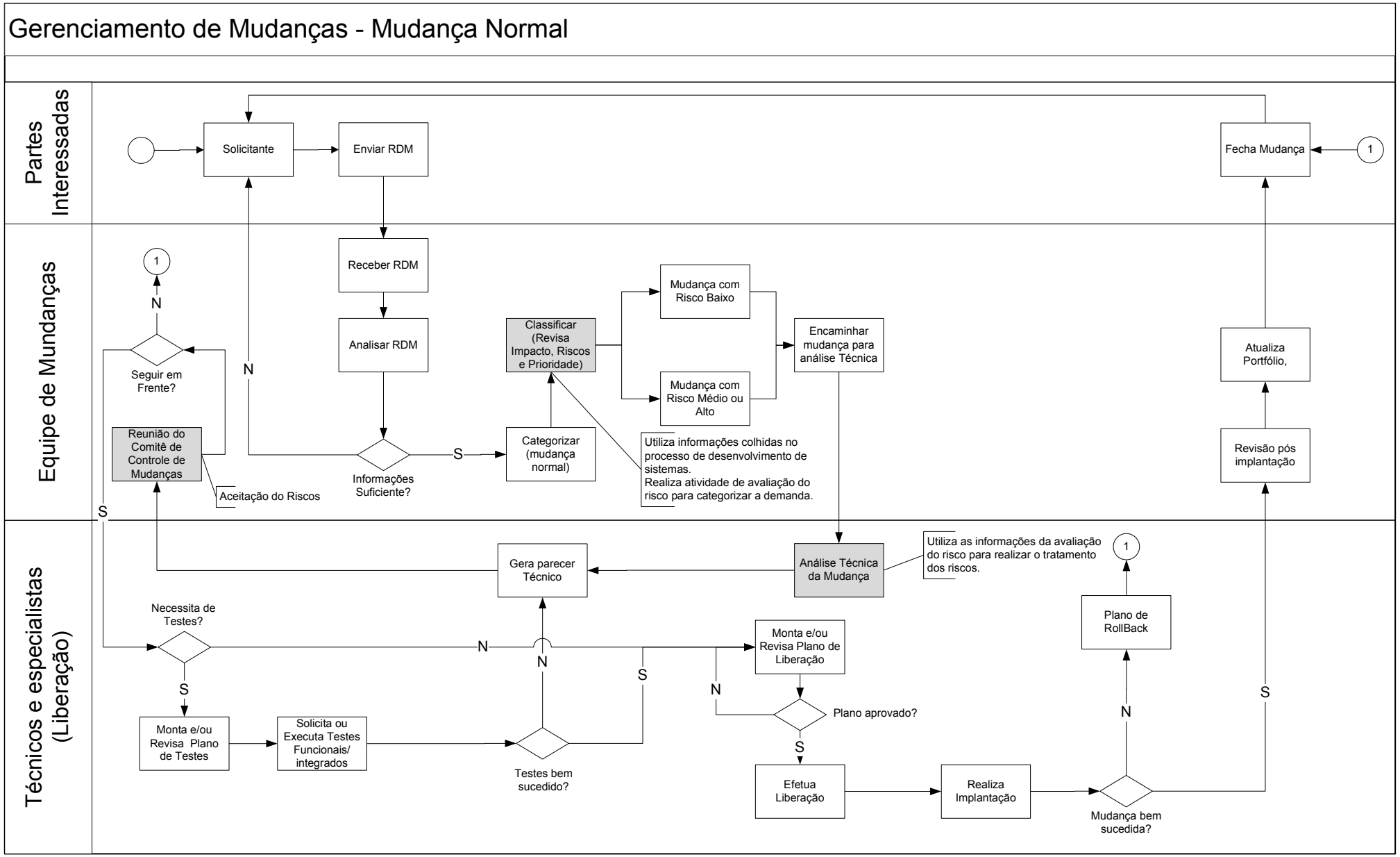
3.2 Processo de Gerenciamento de Mudanças

Nesse trabalho foram tratados duas categorias de mudanças, a normal e a emergencial. A mudança normal é aquela que tem uma programação para implantação planejada antecipadamente, a qual é submetida para avaliação, aprovação e agendamento de execução. Já a mudança emergencial, trata-se de um tipo de mudança que deve ser introduzida para a resolução de incidentes que estejam impactando gravemente os negócios das instituições financeiras bancárias. Neste último caso, algumas atividades essenciais do processo normal não são executadas, com o objetivo de implantar a demanda em tempo hábil, evitando maiores prejuízos para instituição.

A seguir serão apresentados, de forma macro, dois fluxos de atendimento de mudanças, um para as mudanças normais e outro para as mudanças emergenciais. Estes dois fluxos contêm algumas das principais atividades realizadas pelo processo de gerenciamento de mudanças e algumas delas foram incluídas para utilizar os resultados das análises de riscos, que irá auxiliar a equipe de mudanças a categorizar, classificar e gerar parecer técnico das mudanças.

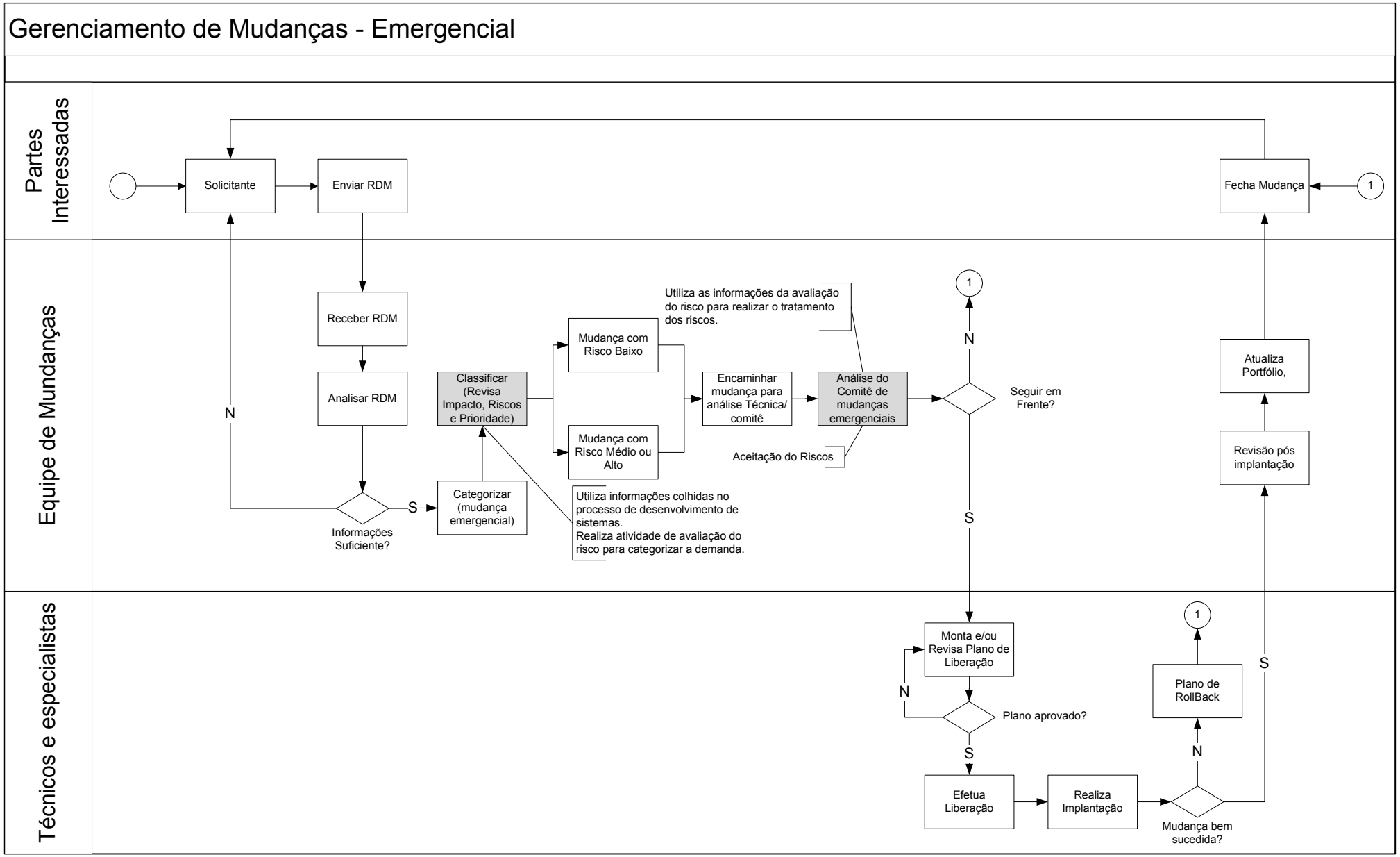
Outro ponto importante que também precisa ser destacado é que o processo de gerenciamento de mudanças será conduzido do início ao término do atendimento de uma demanda. Ele estará presente em todas as fases de atendimento, com o objetivo de garantir uma mudança de qualidade e de obter um maior aproveitamento do tempo, possibilitando uma análise mais precisa, evitando que esta seja feita somente após a solicitação de mudança, via RDM (ANEXO A).

Fluxo 3 – Gerenciamento de Mudanças Normais.



Fonte – Elaborado pelo autor.

Fluxo 4 – Gerenciamento de Mudanças Emergenciais.



Fonte – Elaborado pelo autor.

Os fluxos 3 e 4 demonstram as atividades que as mudanças normal e emergencial deverão percorrer até a sua implantação.

A mudança normal percorre um caminho mais longo, com o objetivo de mitigar todos os riscos, realizando analises mais completas, que irá exigir o envolvimento de equipes técnicas e gestores do negócio relacionados à mudança, além de testes dos sistemas, interfaces e itens de configuração impactados.

Já a mudança emergencial percorre um caminho mais curto, com um objetivo de restabelecer o funcionamento normal do sistema o mais breve possível. Isso exige que o processo execute menos atividades, principalmente a de análise técnica e testes funcionais. Porém é importante que os riscos sejam mitigados.

A seguir, são apresentados os principais papeis e responsabilidades que estão presentes no processo de gerenciamento de mudanças, da área de TI das instituições financeiras bancárias.

3.2.1 Proprietário do Processo de Gerenciamento de Mudanças;

É a autoridade máxima do processo, ele deve garantir a efetividade do processo e a melhoria contínua.

Como dono do processo, ele deverá cumprir as seguintes responsabilidades:

- Garantir o cumprimento dos requisitos do processo;
- Assegurar o ciclo de melhoria contínua do processo;
- Assegurar a integração com os processos correlatos;
- Garantir a aderência do processo com os requerimentos de negócio da instituição bancária;
- Coordenar o comitê de revisão do processo;
- Desenhar e manter o processo, incluído suas métricas e indicadores;

- Avaliar periodicamente os relatórios gerenciais e adotar as ações corretivas necessárias;
- Realizar auditorias periódicas no processo;
- Trazer para o processo os ajustes estratégicos decorrentes de novos requerimentos de negócio, bem como avaliar periodicamente o atendimento aos requerimentos em vigor;
- Aprovar modificações para o processo.

3.2.2 Gerente de Mudanças

Possui autoridade, participa tanto do desenho, quanto da execução do processo sob a direção do proprietário. É ele quem faz cumprir as regras estabelecidas para o processo.

Como gerente do processo, ele deverá cumprir as seguintes responsabilidades:

- Conduzir o processo de gerenciamento de mudanças;
- Assegurar o registro adequado de todos os RDMs;
- Garantir a classificação e priorização de todas as mudanças registradas;
- Assegurar a realização do CCM quando necessário;
- Garantir o efetivo envolvimento das áreas participantes e impactadas;
- Certificar-se da existência de Planos de Retorno;
- Garantir a base de dados de mudanças devidamente atualizada;
- Interagir com os processos de gerenciamento de problemas e incidentes para avaliação dos incidentes ocasionados por mudanças;
- Garantir o uso do processo de gerenciamento de mudanças;

- Receber, registrar e alocar prioridade para todas as mudanças, conforme escopo do processo;
- Submeter as mudanças de riscos elevados ao CCM;
- Providenciar as condições de agenda para a realização do CCM;
- Definir o fórum do CCM e convocar os participantes, de acordo com o envolvimento nas mudanças e conduzir o CCM;
- Revisar todas as mudanças implementadas;
- Submeter as mudanças emergenciais ao CCME;
- Monitorar os indicadores de desempenho do processo;
- Prover informações gerenciais para o proprietário do processo;

3.2.3 Responsável pela Mudança

Atua como auxiliar do gerente de mudanças na operacionalização do processo.

Como responsável pela mudança, ele deve cumprir as seguintes responsabilidades:

- Avaliar a consistência e a pendência dos RDMs submetidos ao processo;
- Verificar se as mudanças solicitadas afetam os serviços bancários;
- Avaliar a conformidade das mudanças em relação as determinações de órgãos regulatórios;
- Revisar e atualizar registros de mudanças;
- Rejeitar mudanças que se apresentarem impraticáveis;
- Envolver áreas específicas dentro do ciclo de mudanças;
- Solicitar parecer das áreas envolvidas nas mudanças;
- Avaliar os pareceres recebidos das áreas envolvidas nas mudanças;

- Revisar, avaliar e atualizar o risco das mudanças solicitadas;
- Notificar as áreas envolvidas no momento da execução das mudanças;
- Garantir que mudanças emergenciais sejam vinculadas a incidentes;

3.2.4 Grupo técnico e especialista

São os especialistas e executores técnicos da mudança, que respondem diretamente ao responsável pela mudança. São eles que fazem a análise técnica e executam os planos especificados no contexto da mudança.

Como técnico e especialista da mudança, eles devem cumprir as seguintes responsabilidades:

- Avaliar a viabilidade técnica de execução da mudança;
- Auxiliar a negociação de datas para execução das mudanças;
- Alterar a data de execução da mudança, quando necessário;
- Solicitar e acompanhar a disponibilização de recursos para execução das mudanças, quando necessário;
- Realizar a análise técnica dos riscos envolvidos na mudança;
- Elaborar e disponibilizar relatório técnico para o CCM;
- Montar e executar testes, quando necessário;

3.2.5 Comitê Consultivo de Mudanças;

É um grupo de pessoas com autoridade e poder de decisão para deliberar sobre as mudanças. São eles que avaliam, aprovam, autorizam ou rejeitam mudanças.

O CCM deve cumprir as seguintes responsabilidades:

- Garantir o cumprimento dos requerimentos de aprovação para mudanças, sob uma perspectiva integrada.
- Avaliar os requerimentos definidos para as mudanças;
- Avaliar os riscos e impactos para o negócio;
- Realizar avaliações integradas das mudanças;
- Aprovar ou rejeitar as mudanças;

3.2.6 Comitê Consultivo de Mudanças Emergenciais;

É um subgrupo do comitê consultivo de mudanças, focado em deliberar sobre as mudanças emergenciais. São eles quem avalia, aprovam, autorizam ou rejeitam mudanças.

O CCME deve cumprir as seguintes responsabilidades:

- Avaliar a real urgência da mudança;
- Aprovar ou rejeitar as mudanças emergenciais;
- Responsabilizar-se pelos resultados da implantação;

4 ANÁLISE DE RISCOS NO PROCESSO DE GESTÃO DE MUDANÇAS

Este capítulo tem o objetivo de mostrar a viabilidade de utilizar a atividade de análise de riscos no processo de gerenciamento de mudanças, como tentativa de melhorar o processo e mitigar os riscos envolvidos em mudanças críticas nos serviços bancários.

Para atingir o objetivo, primeiramente, é proposto utilizar a técnica de análise de riscos, com enfoque de alto nível, na atividade de Classificação de Mudanças do processo de gerenciamento de mudanças.

Essa atividade é responsável por revisar e/ou identificar os impactos, os riscos e por classificar a mudança, de acordo com o nível do risco (baixo, médio ou alto). O objetivo dessa atividade é conhecer os impactos e riscos envolvidos em uma mudança e dar maior atenção e prioridade para aquelas que têm um nível de risco mais elevado, alocando, quando necessário, um pessoal melhor qualificado para realizar a análise técnica e a mudança.

Partindo dessa primeira análise de riscos, é sugerido também que seja feita uma segunda, quando necessário, porém com enfoque de mais baixo nível, que irá analisar, de forma detalhada, as funcionalidades que sofreram impacto com a mudança. Essa segunda análise será feita somente quando a mudança impactar funcionalidades de nível de risco elevado, identificadas na análise anterior. Ela será utilizada pela atividade de Análise Técnica da Mudança, para identificar os demais sistemas e serviços afetados, os riscos e impactos para o negócio e também para elaborar o relatório técnico da mudança, utilizado pelo CCM.

A atividade de Análise Técnica da Mudança é responsável por realizar as análises técnicas, gerar relatórios para as reuniões do CCM e definir se há necessidades de refazer os testes antes da implantação.

A análise de risco também poderá ser utilizada em diversas outras atividades do processo de gerenciamento de mudanças, como: Analisar RDM, Efetuar Liberação, Criação e/ou execução do plano de contingência, entre outros. Isso poderá contribuir consideravelmente para melhoria do processo e qualidade dos serviços entregues aos clientes das instituições bancárias.

A ideia inicial é que o processo de gerenciamento de mudanças esteja presente em todas as fases de atendimento da demanda, ou seja, a análise de riscos será realizada à medida que o atendimento evoluir. Com isso, é possível obter um melhor aproveitamento do tempo, possibilitando realizar as análises de riscos com mais qualidade e evitar que riscos críticos não sejam identificados.

Outro ponto importante é ter uma base de conhecimento, que possibilite o armazenamento das análises já realizadas. Isso irá garantir agilidade no processo, quando outra mudança impactar alguma funcionalidade ou ativo de serviços já analisados, e também possibilitará gerar dados para obter indicadores, os quais poderão ser utilizados para verificar se a atividade de análise de riscos está gerando resultados positivos.

Então, partindo desses princípios, será possível utilizar a atividade de análise de riscos, no processo de gerenciamento de mudanças, com o objetivo de diminuir a ocorrência de falhas e erros atribuídos à área de tecnologia.

E para tornar a proposta passível de ser testada, será apresentando um exemplo para demonstrar a utilização da atividade de análise de riscos, no processo de gerenciamento de mudanças, baseando-se em uma instituição financeira bancária e dados fictícios.

Conforme descrito no capítulo 2, os primeiros passos para fazer uma boa análise de riscos é definir o contexto, no qual são identificados os critérios básicos, o escopo e os limites da análise. Em seguida, parte-se para o processo de avaliação de riscos. Nessa etapa, os riscos são identificados, analisados e avaliados, gerando uma lista de riscos ordenados por prioridade de acordo com os critérios de avaliação.

4.1 Análise de riscos para Classificar Mudanças

O exemplo tratado nesse item tem o propósito de utilizar a técnica de análise de riscos para identificar riscos, impactos, e por classificar as mudanças de acordo com o nível de risco atribuído na análise.

A análise de riscos apresentada como exemplo neste trabalho, foi desenvolvida baseada na ISO/IEC 27005 (2011), com o propósito de ser a primeira iteração. Por isso foi utilizado uma estimativa qualitativa para os riscos, em que o impacto e probabilidade dos cenários de incidentes, foram mensurados a partir de escalas de atributos qualificadores.

As vantagens dessa abordagem em relação ao risco são: a facilidade de compreensão pelas pessoas envolvidas e a rapidez e simplicidade no desenvolvimento, comparada às estimativas quantitativas. Porém uma desvantagem que vale destacar é a escolha subjetiva das escalas, mas isso poderá ser minimizado com uma boa equipe de gestão de riscos.

Nos próximos itens, uma simulação da análise de risco será apresentada para a atividade de Classificação da Mudança, mas antes de prosseguir, é preciso esclarecer o exato momento que o processo de gerenciamento de mudanças e a atividade de análise de risco irão iniciar no fluxo de atendimento da demanda.

Conforme descrito no capítulo 3, o processo de gerenciamento de mudanças estará presente em todas as fases do atendimento de uma demanda. Então, assim que a fase de iniciação da demanda finalizar, o processo de gerenciamento de mudanças será sensibilizado, iniciando o planejamento preliminar da mudança e a análise inicial de riscos. À medida que o atendimento da demanda evolui, a análise de riscos para classificar a mudança também evolui. Assim, após finalizar o atendimento da demanda e a RDM for aberta, o processo de gerenciamento de mudanças já terá todos os riscos mapeados e a mudança classificada, trazendo agilidade para o processo.

4.1.1 Definição do contexto

Feita a contextualização, o próximo passo é definir o contexto, identificando os critérios de impacto e avaliação de riscos, o escopo e limites do processo, e também fazer o levantamento das informações necessárias sobre a instituição bancária. Todas essas informações serão utilizadas para subsidiar a avaliação de riscos.

Considerando uma situação hipotética, de uma instituição financeira bancária XPTO fictícia, que está entre os quatro maiores bancos do Brasil, foram feitos levantamentos para identificar todos os sistemas que a instituição possui para sustentar as operações bancárias, e os seguintes sistemas foram encontrados:

Quadro 1 – Sistemas bancários e seus objetivos.

Sigla	Descrição	Objetivo
SI001	Sistema de Administração de Recursos de Terceiros	Sistema responsável por manter as operações em fundos de investimento. Disponibilizando aos clientes as opções de aplicação e resgate por meio do internet banking e pontos de atendimento. Esse sistema também é responsável por calcular todos os rendimentos das aplicações.
SI002	Sistema de Microfilmagem	Sistema responsável por gerar e emitir microfichar para armazenado dados por um longo período.
SI003	Sistema de Deposito e Conta Corrente	Sistema responsável pela atualização de saldo das contas dos clientes, disponibilização de créditos, cobrança de tarifas, contabilidade, autorização de transações, entre outras. Ou seja, ele é responsável por contralar todas as operações possíveis em uma conta bancária.
SI004	Sistema de Empréstimo	Sistema responsável por realizar empréstimos aos clientes da instituição bancária. Esse sistema avalia, aprova ou rejeita uma solicitação de crédito.
SI005	Sistema Demonstrativo de Movimentação Financeira	Sistema responsável por disponibilizar os extratos de movimentação financeira aos clientes e à receita federal.
SI006	Sistema de Avaliação de Riscos	Sistema responsável por avaliar os riscos envolvidos em uma solicitação de empréstimo, financiamento, cartão de crédito, entre outros.

Fonte – Elaborado pelo autor.

Em seguida, para cada sistema encontrado, foi necessário também identificar suas principais funcionalidades, ou seja, as ações que o sistema em produção é capaz de executar, como por exemplo, cadastrar cliente, consultar clientes, efetuar saques, entre outros.

Continuando com o exemplo da instituição financeira XPTO, o quadro 2 descreve as funcionalidades identificadas para cada sistema que está em produção:

Quadro 2 – Módulos e funcionalidades dos sistemas

Sigla	Módulo	Funcionalidade (Ativo)
SI001	On-Line	Aplicar em fundos de investimento
		Resgatar em fundos de investimento
		Consultar aplicação em fundos de investimento
		Cadastrar perfil do investidor
		Consultar fundos de investimento disponível
	Batch	Atualizar saldo de fundo de investimento
		Autorizar aplicação em fundo de investimento
		Autorizar resgate em fundo de investimento
		Gerar interface SI001 x SI005
SI002	On-Line	Solicitar geração de extrato para microfilmagem
		Solicitar geração de relatório para microfilmagem
	Batch	Gerar extrato de conta corrente para microfilmagem
		Gerar extrato de fundo de investimento para microfilmagem
		Gerar relatório contábil para microfilmagem
SI003	On-Line	Autorizar transação financeira on-line
		Autorizar abertura de conta
		Consultar saldo de contas
		Solicitar remanejamento de conta
	Batch	Atualizar Saldo de Conta
		Estornar Débito
		Estornar Crédito
		Debitar em conta corrente
		Creditar em conta corrente
		Manter Serviço de Conta Poupança
		Gerar interface SI003 x SI005
		Encerrar automaticamente as contas
SI004	On-Line	Consultar Cliente
		Cadastrar Informações
		Consultar Linha de Crédito do Cliente
		Simular Empréstimo
		Solicitar Empréstimo
	Batch	Gerar Interface SI004 x SI006
		Aprovar Solicitação de Crédito
		Atualizar Taxa de Juros
SI005	On-Line	Consultar informativo de fundos de investimento
		Consultar extrato de conta corrente
		Consultar informe de Rendimento
		Consulta Declaração de Imposto de Renda Retido na Fonte
	Batch	Emitir mala direta de conta em encerramento
		Gera interface SI005 x SI003
		Emitir Declaração de Imposto de Renda Retido na Fonte
		Gera extrato mensal de conta corrente
		Gera informativo mensal de fundo de investimento
SI006	On-Line	Consultar Riscos
		Cadastrar Riscos
		Cadastrar Empréstimo
	Batch	Avaliar Risco de Empréstimo
		Gerar Relatório de avaliação do risco
		Armazenar histórico de avaliação

Fonte – Elaborado pelo autor.

Com todas as informações sobre a instituição bancária, principalmente os sistemas e as funcionalidades identificadas, é possível dar início a atividade de análise de riscos.

Baseado no propósito e nos objetivos do trabalho, o escopo dessa atividade estará restrito ao processo de gerenciamento de mudanças, que é acionando quando ocorrem manutenções nas aplicações bancárias, e limitado à atividade de Classificar Mudanças, de acordo com o sistema e funcionalidades afetadas.

Já os critérios de avaliação de riscos, que serão utilizados para avaliar os riscos, são os seguintes:

- Os riscos que envolvam perda de confidencialidade, disponibilidade e integridade das informações dos clientes, são considerados graves;
- Riscos em mudanças que afetam requisitos legais e regulatórios terão prioridades e são considerados graves;
- Riscos que causam dano a imagem e reputação do Banco são considerados graves;
- Riscos que afetam mudanças que tem um prazo legal terão prioridades e são considerados graves;
- Riscos que atingem ativos e processos críticos, impactando a implantação da mudança, são considerados graves;

Além disso, é necessário definir também os critérios de impacto. Esses critérios foram especificados em função dos danos e custos, causados por um evento relacionado à segurança da informação à instituição, à instituição. E os seguintes critérios devem ser considerados na avaliação do impacto:

Quadro 3 – Critérios de Impacto;

Critérios	**Alto**	**Médio**	**Baixo**
Valor do ativo;	- Ativos apoiam atividades essenciais do negocio e mantém o seu funcionamento. Em caso de paralisação, haverá prejuízos à imagem e reputação do banco, além de grandes prejuízos financeiros; - Ativos que envolvem prazo legal para entrar em produção, devido a alteração de legislação e/ou regulamentação	- Ativos que apoiam processos internos e que em caso de paralisação não haverá grandes perdas; - Ativos que apoiam atividades do negocio, porém não mantém o seu funcionamento. Em caso de paralisação, haverá redução de desempenho do negócio.	- Ativos que não prejudicam as atividades do negocio em caso de paralisação; - Ativos que apoiam processos internos e em caso de paralisação as perdas serão pequenas.
Consequências para o negócio/instituição bancária	- Interrupção das atividades do negócio; - Interrupção dos serviços; - Efeitos negativos sobre a imagem e reputação; - Violação da legislação e/ou regulamentação; - Grandes prejuízos financeiros; - Perdas consideráveis da segurança da informação.	- Redução de desempenho do negócio; - Perda de vantagens competitivas; - Perda de segurança da informação; - Perda de confiança dos clientes; - Significantes perdas financeiras;	- Pequenas perdas financeiras e operacionais. - Efeitos mínimos para o negócio e para a instituição;

Fonte – Elaborado pelo autor.

E por último, é necessário definir os critérios de aceitação do risco. E os seguintes devem ser respeitados:

Quadro 4 – Critério para aceitação do risco

Nível do Risco (1 a 25)	Descrição	Aceitabilidade	Exceções	Observações
Alto (15 a 25)	A maioria dos objetivos não podem ser atingidos; Paralisação dos serviços bancários; Danos graves a imagem e reputação do banco;	Inaceitável, requer ação imediata para mitigar o risco;		
Médio (4 a 12)	Alguns objetivos não podem ser atingidos; Alguns ativos podem afetados e estes não comprometem o negócio;	Não pode ser aceito, requer ação para mitigar o risco;	Autorizado pelo gestor do produto	O NR igual a 4 formado por NI 1 e NP 4 e vice versa são considerados riscos médio
Baixo (1 a 4)	Efeitos menores que são facilmente remediados e não comprometem o negocio e os serviços	Risco aceitável.		O NR igual a 4, formado por NI 2 e NP2 é considerado risco baixo; Os riscos devem ser monitorados durante o processo de implantação.

Fonte – Elaborado pelo autor.

Após a definição do contexto, inicia-se a atividade de avaliação de riscos. Nessa etapa do processo os responsáveis irão utilizar as informações levantadas e, inicialmente, a análise de impacto e cronograma de atendimento da demanda. À medida que o atendimento da demanda evoluir, os demais artefatos poderão ser utilizados pela avaliação de riscos, como as especificações, os casos de uso, os planos de testes, evidencias de testes etc.

Considerando que uma demanda de negocio, aberta pela área gestora, solicita a mudança da regra de rendimento da poupança, a área estratégica da instituição identificou que duas demandas de manutenção evolutiva deveriam ser abertas, uma para o sistema SI003 e outra para o sistema SI005. Estes deverão realizar os ajustes necessários nas funcionalidades, para atender a nova regra que foi imposta um por uma determinação do Banco Central.

Partindo desse princípio, a análise de risco envolvendo o sistema SI003 será apresentada a seguir.

4.1.2 Estimativa de riscos no atendimento das mudanças

Para dar inicio a esta etapa do processo, é recomendado que os ativos, as ameaças, as vulnerabilidades e as consequências já tenham sido identificados. Então, para evitar a repetição de informações, esses itens identificados serão apresentados no quadro 9 (no próximo subitem), o qual irá tratar da avaliação dos riscos.

Conforme apresentado no capítulo 2, a estimativa de riscos compreende três atividades: avaliação das consequências, avaliação da probabilidade dos incidentes e determinação do nível de riscos.

O quadro 5 a seguir apresenta uma matriz com valores pré-definidos, e duas variáveis para definir o nível de risco (NI): o valor do ativo e as consequências para o negócio. Para cada uma dessas variáveis são estipulados três níveis (baixo, médio ou alto) e a combinação de ambos, define o nível de impacto do cenário de incidente.

Os critérios de impacto, conforme definido anteriormente no quadro 3, mostram as descrições dos níveis de cada uma das variáveis. Vale lembra também que quanto mais relevantes e numerosos os processos de negócio apoiados por um ativo, maior é o seu valor.

Quadro 5 – Determinação do nível de impacto

Valor do ativo	Baixa			Média			Alta		
Consequências para o negócio e para a instituição bancária	B	M	A	B	M	A	B	M	A
Nível de Impacto (NI)	1	2	3	2	3	4	3	4	5

Fonte – Elaborado pelo autor.

No quadro 6 são apresentados os dois critérios fundamentais para avaliar a probabilidade de ocorrência de um cenário de incidente: a probabilidade de ocorrência da ameaça e a facilidade de exploração da vulnerabilidade. Nesse quadro, cada critério possui três níveis de gravidade (baixo, médio ou alto) e cada nível de gravidade possui condições para o enquadramento, estas, definidas por meio de análise do processo e do ambiente de mudanças.

Quadro 6 – Avaliação da probabilidade do incidente

Critério	**Alto**	**Médio**	**Baixo**
Probabilidade da ameaça	Ameaças comuns que ocorrem rotineiramente no cotidiano na área de tecnologia do banco. Sistemas com altos índices de defeitos	Ameaças com uma frequência variável, mas que não ultrapassa três ocorrências por ano.	Ameaças raras, sua frequência é de uma ocorrência a cada um ano.
Facilidade de exploração da vulnerabilidade	Vulnerabilidades facilmente exploradas devido à ausência de controles de verificação e procedimentos de análise	Vulnerabilidades exploradas devido a falhas de execução nos procedimentos e controles implementados;	Vulnerabilidades de difícil exploração devido ao amplo conhecimento técnico e as auditorias regulares nos controles e procedimentos.

Fonte – Elaborado pelo autor.

Em seguida, o quadro 7 irá definir o nível de probabilidade do incidente. Este quadro apresenta uma matriz com valores pré-definidos e dois critérios de avaliação: a probabilidade de ameaça e a facilidade de exploração da vulnerabilidade. Para cada um desses critérios há três níveis de gravidade (baixo, médio ou alto), conforme definido no quadro 6. E o nível de probabilidade é calculado utilizando a combinação dos valores dos dois critérios de avaliação.

Quadro 7 – Determinação do nível de probabilidade

Probabilidade da ameaça	Baixa			Média			Alta		
Facilidade de exploração da vulnerabilidade	B	M	A	B	M	A	B	M	A
Nível de Probabilidade (NP)	1	2	3	2	3	4	3	4	5

Fonte – Elaborado pelo autor.

E por último, o quadro 8 apresenta uma matriz para determinar o nível de risco, que será calculado pela multiplicação do nível de impacto, extraído do quadro 5, pelo nível de probabilidade, extraído do quadro 7 (NR = NI x NP).

Quadro 8 – Matriz do nível de risco

	Probabilidade (NP)	Muito Baixo (1)	Baixo (2)	Médio (3)	Alta (4)	Muito alta (5)
Impacto (NI)	Muito alto (5)	5	10	15	20	25
	Alto (4)	4	8	12	16	20
	Médio (3)	3	6	9	12	15
	Baixo (2)	2	4	6	8	10
	Muito Baixo (1)	1	2	3	4	5
Legenda:						
	Risco Baixo					
	Risco Médio					
	Risco Alto					

Fonte – Elaborado pelo autor.

No próximo item, serão apresentados os ativos, as ameaças, as vulnerabilidades e as consequências identificadas no atendimento, que juntamente com as estimativas definidas e apresentadas até o momento, será possível calcular o nível dos riscos e avaliar os cenários de incidentes, gerando uma lista de riscos com nível de prioridade.

4.1.3 Identificação e Análise/Avaliação de riscos no atendimento das mudanças

A partir desse ponto, é onde realmente ocorre a avaliação dos riscos, pois até o momento foi feito uma breve análise, o levantamento das informações necessárias para realizar a avaliação, e definido o método para avaliar os riscos.

O quadro 9 a seguir, representa uma matriz que será utilizada para sistematizar a análise de riscos. Essa matriz contém todos os ativos identificados e suas respectivas ameaças, vulnerabilidades e consequências. Além disso, há também as informações de estimativas de riscos, que são calculadas com auxilio dos critérios e das matrizes, com valores pré-definidos, que foram apresentadas no tópico anterior.

Quadro 9 - Análise de riscos 01.

Análise de riscos – DEMANDA N°00001 (SI003)							
Identificação de riscos					**Estimativa de riscos**		
N°	**Ativo**	**Ameaça**	**Vulnerabilidade**	**Consequência**	**NI**	**NP**	**Nível de risco**
1	Prazo Legal	Indisponibilidade de recursos humanos	Ausência de recursos humanos;	- Violação da legislação e/ou das regulamentações - Prejuízo financeiro devido a multas aplicadas pelo Banco Central; - Perda de Oportunidades de Negócio;	5	2	10
2	Categoria da Mudança	Erro durante categorização da mudança	Inexistência de revisão na abertura de demanda	- Tempo de trabalho perdido; - Retrabalho;	1	4	4
3	Recursos Humanos	Indisponibilidade de técnico especializado para realizar a mudança	Treinamento insuficiente	- Interrupção dos serviços; - Violação de segurança da informação, no caso de haver erros não identificados na demanda;	3	1	3
4	Demanda Evolutiva	Erro na entrega dos artefatos	Inexistência de controle para verificar a entrega de todos os artefatos	- Interrupção de operações internas; - Custo financeiro e operacional para elaboração e/ou reposição	1	5	5
5	Demanda Evolutiva	Abuso de direitos	Procedimento de testes de *softwares* insuficientes ou inexistentes	- Interrupção de operações internas; - Custo operacional e financeiro para elaboração;	1	5	5
6	Demanda Evolutiva	Defeito de *software*	Especificações confusas ou incompletas para analistas e desenvolvedores	- Tempo de trabalho perdido - Perda de confiabilidade - Retrabalho;	1	5	5
7	Serviço de Conta Poupança	Implantação de aplicativo com defeito.	Inexistência de uma análise técnica das alterações nas aplicações	- Comprometimento dos serviços de Conta Poupança; - Prejuízos à imagem e reputação do banco; - Interrupção de atividades do negócio; - Perda de confiança dos clientes; - Tempo de reparo; - Perda de segurança da informação	5	3	15
8	Serviço de Geração de Interfaces com outros sistemas	Dados incompletos ou inconsistentes	Inexistência de validação dos layouts das interfaces e dos dados.	- Tempo de reparo; - Interrupção de operações internas; - Perda de integridade dos dados	3	3	9

Fonte – Elaborado pelo autor.

Quadro 9 – Análise de riscos 02

Análise de riscos – DEMANDA N°00001 (SI003)							
Identificação de riscos					Estimativa de riscos		
N°	**Ativo**	**Ameaça**	**Vulnerabilidade**	**Consequência**	**NI**	**NP**	**Nível de risco**
9	Serviço de Geração de Interfaces com outros sistemas	Abuso de direitos	Insuficiência de execução e validação de testes integrados.	- Comprometimento dos serviços de geração de interfaces; - Comprometimento dos serviços do sistema que utiliza a interface (geração de extratos mensais);	3	4	12
10	Elaboração	Abuso de direitos	Ausência ou insuficiência de auditoria periódica nos artefatos de caso de uso para verificar se foram alterados de acordo com o especificado.	- Perda de integridade dos dados; - Perda de eficiência/confiança	2	4	8
11	Codificação	Defeito de software	Inexistência de controle eficaz para verificação e validação do código	- Perda de reputação técnica; - Tempo de reparo; - Custo financeiro e operacional;	4	4	16
12	Codificação	Defeito de software	Inexistência de controle eficaz para verificar o atendimento de todo o escopo da demanda.	- Perda de reputação técnica; - Tempo de reparo; - Custo financeiro e operacional; - Interrupção dos serviços; - Redução do desempenho do negócio	4	3	12
13	Testes	Abuso de direitos	Ausência ou insuficiência de evidência de testes	- Perda de reputação técnica; - Retrabalho; - Custo financeiro e operacional;	5	2	10
14	Testes	Erro durante os testes	Inexistência de controle eficaz para verificação e validação das evidências de testes.	- Perda de reputação técnica; - Retrabalho; - Custo financeiro e operacional; - Interrupção dos serviços;	5	1	5
15	Versão do Programa	Erro durante o versionamento	Inexistência de controle de versão, que evita que outra demanda, que impacta os mesmos programas, suba para produção antes do programado.	- Perigo ocasionado à segurança dos dados; - Interrupção de atividades do negócio; - Interrupção dos serviços; - Perda do ativo;	5	1	5

Fonte – Elaborado pelo autor.

Para facilitar o entendimento, a seguir será apresentada uma simulação de como calcular o valor de um risco, utilizando o ativo de N°1, do quadro 9, como exemplo.

O primeiro passo é determinar o nível de impacto (NI) utilizando o quadro 5, mas antes, é necessário atribuir um valor para o ativo e para as consequências do impacto no negócio, utilizando o quadro 3. Percebe-se que o ativo N°1 (quadro 9), é referente a prazos legais para estar em produção, e que caso a ameaça se concretize, as consequências são severas, pois viola a legislação e gera grandes prejuízos financeiros a instituição. Então, enquadrando esses itens na matriz descrita no quadro 5, verificamos que ela retornará um valor de impacto igual a 5, pois o ativo e as consequências possuem um nível alto.

O próximo passo é determinar o nível de probabilidade (NP), utilizando o quadro 7. Nessa etapa é necessário atribuir valores à probabilidade da ameaça e à facilidade de exploração da vulnerabilidade. E, para isso, utiliza-se o quadro 6, que irá servir para enquadrar a ameaça com os critérios de probabilidade, e a vulnerabilidade com os critérios de facilidade de exploração. Então, com auxilio do quadro 6 e do conhecimento da equipe de gerenciamento de mudanças, foi atribuído um valor de nível médio para a probabilidade, e um valor de nível baixo para facilidade de exploração, que enquadrados na matriz do quadro 7, gera-se um valor de nível de probabilidade igual a 2.

E por fim, é calculado o nível de risco (NR), utilizando o quadro 8, onde é aplicada a seguinte fórmula: NR = NI x NP, que resolvida ficaria: NR = 5 x 2 → NR = 10 (Risco Médio).

Finalizada a atividade de identificação e mensuração dos riscos, é hora de iniciar a etapa final, que irá avaliar e priorizar os riscos, levando em consideração o nível do risco (NR) e os critérios de avaliação e aceitação dos riscos.

O quadro 10 a seguir, representa uma forma de avaliar os riscos e priorizá-los. O primeiro elemento do quadro é o cenário de incidentes, isto é, a descrição da ameaça explorando a vulnerabilidade de um ativo. Em seguida há o nível de risco (NR), que é a referencia da combinação da probabilidade com o impacto da ocorrência do cenário de incidentes. E por último, os quesitos que irão ajudar a definir a ordem de prioridade dos riscos, ou seja, aqueles riscos que

merecem mais atenção por parte dos envolvidos no Comitê Consultivo de Mudanças (CCM) e aqueles que necessitam de uma segunda iteração, para analisar os riscos em um nível mais baixo.

Quadro 10 – Critérios para avaliação de riscos 01.

Demanda N°00001 (SI003)			Atinge algum processo estratégico?	Atinge algum ativo crítico?	Viola algum requisito legal?	Causa dano a imagem e reputação?	Viola qual atributo da segurança da informação?	Priorização do risco.
N°	**Cenário de risco**	**NR**						
1	Indisponibilidade de recursos para atender uma demanda com prazo legal, devido a ausência de recursos humanos especializados	10	Sim	Sim	Sim	Não	Não	1
2	Erro durante a categorização da mudança devido a inexistência de revisão na abertura de demanda	4	Não	Não	Não	Não	Não	15
3	Indisponibilidade de técnico especializado para realizar a mudança, devido a insuficiência de treinamento.	3	Sim	Não	Não	Não	Não	13
4	Erro na entrega dos artefatos devido inexistência de controle para verificar a entrega de todos os artefatos.	5	Não	Não	Não	Não	Não	14
5	Abuso de direitos no fluxo de atendimento de demandas evolutivas, devido a insuficiência ou inexistência de procedimento de testes de *softwares*.	5	Sim	Sim	Não	Não	Não	12
6	Defeito no *software* devido a especificações confusas ou incompletas para analistas e desenvolvedores	5	Sim	Sim	Não	Sim	C	9
7	Implantação de aplicativo que disponibiliza serviços de conta poupança com defeito devido inexistência de uma análise técnica das alterações nas aplicações	15	Sim	Sim	Não	Sim	C/D/I	2
8	Dados incompletos ou inconsistentes no serviço de geração de interfaces para outros sistemas, devido inexistência de validação dos layouts das interfaces e dos dados.	9	Sim	Sim	Não	Sim	Não	3

Fonte – Elaborado pelo autor.

Quadro 10 – Critérios para avaliação de riscos 02.

Demanda N°00001 (SI003)			Atinge algum processo estratégico?	Atinge algum ativo crítico?	Viola algum requisito legal?	Causa dano a imagem e reputação?	Viola qual atributo da segurança da informação?	Priorização do risco.
N°	**Cenário de risco**	**NR**						
9	Abuso de direito na validação dos serviços de geração de interfaces, devido a insuficiência de execução e validação dos testes integrados.	12	Não	Sim	Não	Não	I	5
10	Abuso de direitos na fase de Elaboração, devido ausência ou insuficiência de auditoria periódica nos artefatos de caso de uso para verificar se foram alterados de acordo com o especificado.	8	Não	Não	Não	Não	I	10
11	Defeito de *software* devido a inexistência de controle eficaz para verificação e validação do código	16	Não	Sim	Não	Não	C/D/I	4
12	Defeito de *software* devido a inexistência de controle eficaz para verificar o atendimento de todo o escopo da demanda.	12	Não	Sim	Não	Não	Não	8
13	Abuso de direitos na fase de testes, devido a ausência ou insuficiência de evidência de testes.	10	Sim	Sim	Não	Não	Não	6
14	Erro durante os testes, devido a inexistência de controle eficaz para verificação e validação das evidências de testes.	5	Sim	Sim	Não	Não	Não	7
15	Erro durante o versionamento dos programas, devido a inexistência de controle de versão, que evita que outra demanda, que impacta os mesmos programas, suba para produção antes do programado.	5	Não	Sim	Não	Não	Não	11

Fonte – Elaborado pelo autor.

Após a identificação dos elementos construtivos do risco (ativo, ameaça, vulnerabilidade e consequência) e após a estimativa do impacto e da probabilidade dos cenários de incidentes, os riscos foram avaliados segundo os critérios elencados no quadro 10. O resultado desse percurso é uma lista de riscos ordenados por prioridade de tratamento, conforme o quadro 11 a seguir. Desse modo, os riscos encontrados por meio de uma análise/avaliação de riscos com enfoque de alto nível apontam para os principais problemas de segurança da informação do escopo considerado.

Quadro 11 – Riscos ordenados por prioridade.

Prioridade	**Cenário de Risco**
1	Indisponibilidade de recursos para atender uma demanda com prazo legal, devido a ausência de recursos humanos especializados.
2	Implantação de aplicativo que disponibiliza serviços de conta poupança com defeito devido inexistência de uma análise técnica das alterações nas aplicações.
3	Dados incompletos ou inconsistentes no serviço de geração de interfaces para outros sistemas, devido inexistência de validação dos layouts das interfaces e dos dados.
4	Defeito de *software* devido a inexistência de controle eficaz para verificação e validação do código.
5	Abuso de direito na validação dos serviços de geração de interfaces, devido a insuficiência de execução e validação dos testes integrados.
6	Abuso de direitos na fase de testes, devido a ausência ou insuficiência de evidência de testes.
7	Erro durante os testes, devido a inexistência de controle eficaz para verificação e validação das evidências de testes.
8	Defeito de *software* devido a inexistência de controle eficaz para verificar o atendimento de todo o escopo da demanda.
9	Defeito no *software* devido a especificações confusas ou incompletas para analistas e desenvolvedores
10	Abuso de direitos na fase de Elaboração, devido ausência ou insuficiência de auditoria periódica nos artefatos de caso de uso para verificar se foram alterados de acordo com o especificado.
11	Erro durante o versionamento dos programas, devido a inexistência de controle de versão, que evita que outra demanda, que impacta os mesmos programas, suba para produção antes do programado.
12	Abuso de direitos no fluxo de atendimento de demandas evolutivas, devido a insuficiência ou inexistência de procedimento de testes de *softwares*.
13	Indisponibilidade de técnico especializado para realizar a mudança, devido a insuficiência de treinamento.
14	Erro na entrega dos artefatos devido inexistência de controle para verificar a entrega de todos os artefatos.
15	Erro durante a categorização da mudança devido a inexistência de revisão na abertura de demanda

Fonte – Elaborado pelo autor.

Todo esse processo de análise e avaliação de riscos feitos até o momento é usado para classificar a mudança, atribuindo-lhe um nível de risco (baixo, médio ou alto) para implantação. E para realizar o enquadramento, o dono do processo poderá definir uma escala com valores pré-definidos, que irá conter uma faixa de valores para cada nível, por exemplo: baixo – 0 a 99; médio - 100 a 299; e alto – acima de 300. Os valores são obtidos por meio da soma de todos os NR identificados.

Além da classificação da mudança, as análises e avaliações de riscos são usadas para identificar os principais cenários de incidentes, ou seja, aqueles que podem causar sérios prejuízos a instituição e, principalmente, identificar os riscos

que devem passar por uma segunda iteração, o qual possibilitará analisar o risco mais a fundo e identificar possíveis falhas no desenvolvimento, antes de realizar a implantação da mudança. Além de também mostrar para o gestor quais os riscos necessitam de tratamento, com o objetivo de mitigá-los a um nível aceitável.

A segunda iteração da análise e avaliação de risco é feita nos ativos que envolvem análises técnicas, ou seja, os que impactam as funcionalidades do sistema. Estes devem passar por uma segunda iteração, com o objetivo de identificar e eliminar qualquer risco de incidente que possa causar impactos negativos a instituição.

4.2. Resultados Obtidos

Com o exemplo apresentando nesse estudo de caso, foi possível perceber que é viável a utilização da análise de risco para identificar os riscos inerentes às etapas de desenvolvimento e gerenciamento de mudanças, analisar o nível de exposição de cada um e classificá-los, possibilitando que os gestores tomem conhecimento dos riscos e determinem quais riscos serão eliminados, mitigados, aceitáveis e quais serão acompanhados.

Dentre os vários benefícios que a análise de risco pode trazer tanto para o ambiente de desenvolvimento de sistemas, quanto para o negócio das instituições financeiras bancárias, foram destacados os seguintes:

- Identificar os sistemas mais críticos da organização;
- Identificar as funcionalidades mais críticas de cada sistema;
- Identificar as dependências que os sistemas têm entre si;
- Identificar as falhas no desenvolvimento das melhorias de sistemas, que podem impactar o negócio e trazer prejuízo a organização;
- Identificar quais demandas tem prioridade de implantação e quais necessitam de maior atenção na implantação (classificar mudanças);

- Priorizar os cenários de incidentes que possuem maior nível de risco, possibilitando atacar os riscos mais críticos e mais prováveis de ocorrer.
- Controlar os recursos humanos necessários para implantação de mudanças;
- Alertar gestores e tomadores de decisão dos riscos envolvidos nas demandas, entre outros.

Com este estudo pode-se perceber também que a atividade de análise de riscos, quando aplicada em conjunto com as outras atividades do processo de gestão de riscos, poderá trazer mais benefícios e obter um maior desempenho da atividade de análise de riscos. Pois, como esta atividade é executada pelo próprio processo que deseja ter seus riscos identificados e analisados, é necessário que se tenha o processo de gestão de riscos para percorrer todos os processos que faz uso da atividade de análise de risco e realizar: o planejamento dos planos de mitigação, eliminação e acompanhamento do risco, o controle e monitoramento, que corresponde a execução e acompanhamento dos planos elaborados, e a melhoria das atividades de análise de riscos.

CONCLUSÃO

O estudo permitiu compreender que aplicando a técnica de análise de riscos no processo de gerenciamento de mudanças, será possível identificar os grandes riscos envolvidos na implantação de mudanças. E quando a análise é feita corretamente, ela poderá trazer vários benefícios para o negocio da empresa, como, evitar que falhas graves ocorram no ambiente produtivo, agilidade nos processos, mapeamento dos sistemas mais críticos para o negócio, entre outros.

O estudo também permitiu compreender que além da técnica de análise de riscos, as grandes instituições financeiras bancárias necessitam de processos de gerenciamento de riscos, não só no ambiente produtivo, mas também no ambiente de desenvolvimento. Este processo, quando aplicado nesses ambientes, possibilitará que os responsáveis pela área de TI planejem, executem, monitorem e melhorem todas as atividades que envolvem riscos críticos para o negócio.

Outros benefícios que a análise de risco, juntamente com as demais atividades da gestão de risco poderá trazer para o negócio e para o ambiente de TI, são as possibilidades de melhorem os resultados, através da identificação e da análise de uma gama mais ampla de questões, fornecendo uma forma sistemática de tomar decisões embasadas em informações. Além de reduzir surpresar, aproveitar oportunidades, melhorar o planejamento, desempenho e eficácia, economia e eficiência, e a reputação da empresa.

Deste modo, os objetivos do trabalho foram alcançados, já que os instrumentos propostos de análise e avaliação dos riscos contribuem na identificação e tratamento dos riscos envolvidos em uma mudança na aplicação bancária, agindo de forma proativa, evitando que estes se propagem para o ambiente produtivo.

Dentro da temática pesquisada existem ainda algumas lacunas que precisam ser preenchidas com trabalhos monográficos, foram destacadas algumas como sugestão de trabalho futuro:

- Analisar a viabilidade de realizar avaliação de risco em mudanças que envolvem ativos físicos, como: migração de servidores, de sites, de Data Center, entre outros.
- Propor uma metodologia de um processo de gerenciamento de riscos no ambiente de desenvolvimento das instituições financeiras bancárias;
- Mapear processos críticos para o negócio de uma instituição financeira bancária e propor soluções para gerenciamento e tratamento de riscos.
- Aplicar a atividade de análise de risco em um ambiente real, com objetivo de gerar indicadores.

REFERÊNCIAS

ABNT NBR ISO/IEC 17799. **Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação.** 2.ed. Rio de Janeiro: ABNT: 2005.

ABNT NBR ISO/IEC 27005. **Técnicas de segurança — Gestão de riscos de segurança da informação.** Projeto de revisão. Rio de Janeiro: ABNT: 2011.

APM Group. ITIL - **Service Transition**. V3: OGC, 2008. 399p.

BACEN. **O Acordo da Basileia.** Disponível em: <http://www.bcb.gov.br/?BASILEIA> Acesso em: 25 fev. 2014

BANCO DO BRASIL. **Novo Acordo de Capitais – Basiléia II.** Disponível em: <http://www.bb.com.br/portalbb/page51,136,3442,0,0,1,8.bb?codigoNoticia=4813&codigoMenu=413&codigoRet=4119&bread=9_1_4> Acesso em: 25 fev. 2014

CORREIO BRAZILIENSE. **Clientes do Bradesco e Caixa enfrentam filas após falha no sistema**: Transações bancárias não puderam ser realizadas na sexta-feira; no 1º dia útil depois do incidente, clientes precisam ter paciência. 2013. Disponível em:<http://www.correiobraziliense.com.br/app/noticia/economia/2013/07/08/internas_economia,375728/clientes-do-bradesco-e-caixa-enfrentam-filas-apos-falha-no-sistema.shtml> Acesso em: 11 fev. 2014

DIÓGENES, Yuri; MAUSER, Daniel. **Certificação Security +**: Da Prática para o Exame SYO-301. Rio de Janeiro: Novaterra, 2011. 390p.

DOROW, E. **Governança e a Gestão de Riscos em TI.** Disponível em: <http://www.governancadeti.com/2010/11/governanca-e-a-gestao-de-riscos-em-ti/> Acesso em: 25 fev. 2014.

ESPINHA, Rafael; SOUSA, João. **Melhorando Processos Através da Análise de Risco e Conformidade**. DevMedia Engenharia de Software magazine. Rio de Janeiro. Edição especial. 10p. a 21p. Jan. 2007.

FREITAS, M. A. dos Santos. **Fundamentos do Gerenciamento de Serviços de TI**: Preparatório para a certificação ITIL V3 Foundation. Rio de Janeiro: Brasport, 2010. 351p.

ISO/IEC 13335-3. **Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security.** 1 ed. Technical Report: 1998.

MATIAS, F. J. F. **Impacto da gestão do risco nas instituições financeiras**. 2012. 98 f. Trabalho de Conclusão de Curso (Mestrado em Contabilidade e Finanças) – Instituto Politécnico de Setúbal, Portugal, 2012. [Orientador: Prof. Dr Teresa Alves]. Disponível em: <http://comum.rcaap.pt/bitstream/123456789/3995/1/Disserta%C3%A7%C3%A3o%2

0%20Impacto%20da%20gest%C3%A3o%20do%20risco%20nas%20instui%C3%A7%C3%B5es%20finaceiras..pdf> Acesso em: 24 fev. 2014.

MPS.BR - Melhoria de Processo do Software Brasileiro. **Guia de Implementação – Parte 5: Fundamentação para Implementação do Nível C do MR-MPS-SV:2012.** Softex: 2013.

OHTOSHI, P. H. **Análise comparativa de Metodologias de Gestão e de Análise de Riscos sob a Ótica da Norma NBR-ISO/IEC 27005**. 103 f. Trabalho de Conclusão de Curso (Especialização em Gestão de Segurança da Informação Comunicações) – Universidade de Brasília – UnB, Brasília, Brasil, 2008. [Orientador: Prof. Dr. Edgard Costa Oliveira]

TERRA.COM. **Sistema do BB sai do ar e clientes ficam sem serviço.** O sistema do Banco do Brasil saiu totalmente do ar neste domingo. 2013. Disponível em: <http://economia.terra.com.br/vc-reporter-sistema-do-bb-sai-do-ar-e-clientes-ficam-sem-servico,c1dcf12e156f2410VgnVCM3000009af154d0RCRD.html> Acesso em: 11 fev. 2014.

ANEXO A – RDM - Formulário de Requisição de Mudanças


RDM.pdf

Formulário de Requisição de Mudanças

Grau de sigilo
#xx

Data	Solicitante	Aplicativo	Numero da Demanda

1. Ambiente

- ☐ Pré-Produção * (CN de Operações/BR)
- ☐ HMP
- ☐ Produção

2. Justificativa da Demanda *(Conforme natureza e caráter):*

3. Benefício da Mudança *(Visão de Negócio):*

4. Houve atualização do Manual de Produção? ☐ Sim ☒ Não

5. Haverá acompanhamento da CEDES na execução da solicitação? ☐ Sim Nome: Tel.: ☐ Não

6. Haverá alteração de regra de negócio? ☐ Sim ☐ Não

7. Haverá interrupção do serviço prestado ou algum outro impacto em produção decorrente do atendimento desta mudança? ☐ Sim Descrição: _____ ☐ Não

7.1. Existem transações que deverão ser desabilitadas durante a execução da mudança? ☐ Sim Quais? _____ ☐ Não

8. Período do atendimento *(marcar mais de um se necessário)*:

- ☐ Antes do on-line;
- ☐ Depois do on-line;
- ☐ Concorrente ao on-line;
- ☐ Antes da diária;
- ☐ Depois da diária;
- ☐ Concorrente a diária;
- ☐ Outra restrição (descrever): _____

9. SOLICITAÇÃO Assinalar o(s) item(ns) a ser(em) executados(s):

9.1. Aplicações - Plataforma NT/ Linux/ VMS/ Ponta Cliente

- ☐ 9.1.1. Páginas / Pacote;
- ☐ 9.1.2. Componentes (HIS, MDAC, MJET, API/DLL, etc.);
- ☐ 9.1.3. Rotina Batch;
- ☐ 9.1.4. Outros (Staffware, Site Server, etc.);
- ☐ 9.1.5. Execução de Query: ☐ Update ☐ Insert ☐ Delete

Detalhamento das Atividades *(Ao detalhar a(s) atividade(s) segregue conforme o(s) item(ns) selecionado(s)):*

Existe interdependência com outras rotinas/atividades?

Há execução de rotina? ☐ Sim ☐ Não. Se sim, a rotina pode ser interrompida?

9.2. Aplicações - Unix/ Solaris

- ☐ 9.2.1. Pacote para Deploy - SJSAS/JBOSS;

- ☐ 9.2.2. Pacote para Deploy - Conteúdo estático (SJSWS, APACHE)
- ☐ 9.2.3. Documento de Deploy (SIT);
- ☐ 9.2.4. Bibliotecas e versões a serem utilizadas;
- ☐ 9.2.5. Rotina Batch;
- ☐ 9.2.6. Nome da url da Aplicação;
- ☐ 9.2.7. Nome do diretório para armazenamento da parte estática;
- ☐ 9.2.8. Instância Serv. de aplicação: ☐ Intra ☐ Inter ☐ Extra;
- ☐ 9.2.9. Sistemas e Módulos impactados / envolvidos;
- ☐ 9.2.10. Outros (Staffware, JVM, SJS, MQ, etc.): _____;

Detalhamento das Atividades *(Ao detalhar a(s) atividade(s) segregue conforme o(s) item(ns) selecionado(s))*:

Existe interdependência com outras rotinas/atividades?

Há execução de rotina? ☐ Sim ☐ Não. Se sim, a rotina pode ser interrompida?

9.3. Aplicações - Mainframe

- ☐ 9.3.1. Programas Batch;
- ☐ 9.3.2. Alteração de JCL, Proc e Sysin;
- ☐ 9.3.3. Programas On-line;
- ☐ 9.3.4. Aplicações, Transações e Arquivos - CICS;
- ☐ 9.3.5. Outros (Staffware, MQ, Content Manager, etc.);
- ☐ 9.3.6. Execução de Query: ☐ Update ☐ Insert ☐ Delete

Detalhamento das Atividades *(Ao detalhar a(s) atividade(s) segregue conforme o(s) item(ns) selecionado(s))*:

Existe interdependência com outras rotinas/atividades?

Há execução de rotina? ☐ Sim ☐ Não. Se sim, a rotina pode ser interrompida? _____

9.4. Banco de Dados

- ☐ DB2
- ☐ Oracle
- ☐ Sybase
- ☐ MS SQL Server
- ☐ Sybase-IQ
- ☐ PostgreSQL
- ☐ Caché
- ☐ IDMS Normal
- ☐ IDMS Liquidado

9.4.2. Nome do Database ou Esquema:

9.4.3. Modelo

- ☐ Cool:Gen
- ☐ Power Designer

9.4.3.1. Nome do Modelo

- ☐ DES:
- ☐ TQS:
- ☐ HMP:
- ☐ PRD:

9.4.4. Dependências:

9.4.5. Em Caso de transferência de Procedure, Functions ou Packages informar:

- ☐ 9.4.5.1. De:
- ☐ DES para HMP
- ☐ DES para PRD
- ☐ TQS para HMP
- ☐ HMP para PRD
- ☐ 9.4.5.2. Origem
- ☐ 9.4.5.3. Destino:
- ☐ 9.4.5.4. Lista dos Objetos:

Detalhamento das Atividades *(Ao detalhar a(s) atividade(s) segregue conforme o(s) item(ns) selecionado(s))*:

9.5. Segurança - Definições

☐ SIASE Informar as alterações no SIASE:

	RACF	Incluir, Excluir	Grupo	Perfil	Transação

Formulário de Requisição de Mudanças

		ou Alterar?			

	SINAV - Disponibilização de aplicações para o SINAV/HMP:

	LDAP	Incluir, Excluir ou Alterar?	Grupo	Perfil

	SISGR

Detalhamento das Atividades *(Ao detalhar a(s) atividade(s) segregue conforme o(s) item(ns) selecionado(s)):*

Existe interdependência com outras rotinas/atividades?

9.6. Segurança - Banco de Dados

☐ DB2 ☐ Oracle ☐ Sybase
☐ MS SQL Server ☐ Sybase-IQ ☐ PostgreSQL
☐ Caché ☐ IDMS Normal ☐ IDMS Liquidado

Detalhamento das Atividades *(Ao detalhar a(s) atividade(s) segregue conforme o(s) item(ns) selecionado(s)):*

9.6.1. Concessão de privilégios (para criação de contas, necessário o formulário #20 – Ficha de Identificação de criação de conta)

10. Recursos de Armazenamento de dados:
(Caso haja impacto em relação aos recursos de armazenamento em disco, preencher o quadro abaixo).

Ambiente Partição IBM / Domínio SUN / Servidor	Tipo de arquivo base de dados/arquivos gerais/ arquivos temporários	Área estimada (GB)

11. Documentos de Testes

(Os documentos listados serão encaminhados de acordo com a necessidade da demanda)

☐ 11.1. Evidência de Teste;
☐ 11.2. Estratégia de Testes da Demanda, Endereço/Anexo;
☐ 11.3. Roteiro de Testes da Demanda, Endereço/Anexo;
☐ 11.4. Roteiro de Testes de Carga/Stress, Endereço/Anexo;
☐ 11.5. Documento para Criação de Ambiente, Endereço;
☐ 11.6. Casos de Teste;
☐ 11.7. Scripts;
☐ 11.8. Massa de Testes;

Detalhamento das Atividades *(Ao detalhar a(s) atividade(s) segregue conforme o(s) item(ns) selecionado(s))*

12. Observações: