UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO EM GESTÃO DA
TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

ALDOINO MENEGHELLI JR

ESTUDO DE CASO - APLICAÇÃO DE BOAS PRÁTICAS DE TECNOLOGIA DA INFORMAÇÃO (GESTÃO DE INCIDENTES) PARA UMA INSTITUIÇÃO FINANCEIRA

MONOGRAFIA

CURITIBA
2014

ALDOINO MENEGHELLI JR

ESTUDO DE CASO - APLICAÇÃO DE BOAS PRÁTICAS DE TECNOLOGIA DA INFORMAÇÃO (GESTÃO DE INCIDENTES) PARA UMA INSTITUIÇÃO FINANCEIRA

Monografia apresentada como requisito parcial à obtenção do título de Especialista em Gestão da Tecnologia da Informação e Comunicação, do Departamento Acadêmico de Eletrônica, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Alexandre J. Miziara

CURITIBA

2014

AGRADECIMENTOS

Agradeço as pessoas que de alguma maneira contribuíram com incentivos, atitudes e me apoiaram até o presente momento.

Agradeço a DEUS por tudo o que sou e por quem ELE é na minha vida!

À minha esposa, Kely, e filhos, Rafael e Maria Cecília, pela demonstração de paciência, amor, carinho, incentivo e alegria que motivam minha caminhada e alimentam minha alma e coração.

Ao Orientador Prof. Alexandre J Miziara, por colaborar na realização deste trabalho com sua experiência e dedicação.

Aos colegas de profissão que incentivaram e forneceram o devido apoio para conclusão desta mais esta etapa em minha vida.

RESUMO

MENEGHELLI, Aldoino Jr. Estudo de caso - Aplicação de boas práticas de Tecnologia da Informação (Gestão de Incidentes) para uma Instituição Financeira. 2014. XX f. Monografia (Especialização em Gestão da Tecnologia da Informação e Comunicação) – Universidade Tecnológica Federal do Paraná, Curitiba, 2014.

O estudo de caso visa investigar a relação entre a quantidade de Incidentes de Tecnologia da Informação registrados em uma instituição financeira e aplicação de boas práticas de TI relacionando disponibilidade de serviços. O estudo foi baseado em uma análise quantitativa e qualitativa considerando uma base de dados de aproximadamente 2 (dois) anos referentes à quantidade de Incidentes de Tecnologia da Informação registrados e índices de disponibilidade de serviços durante o mesmo período. O critério de escolha foi a disponibilidade dos serviços observados e o risco que estes serviços oferecem para a Instituição Financeira avaliada. O levantamento realizado procura mensurar um índice de quantidade de incidentes de Tecnologia da Informação versus a disponibilidade dos sistemas elencados para a pesquisa, bem como o reflexo destes índices na eficiência operacional de uma Instituição Financeira.

Palavras-chave: Boas práticas de TI; Gestão de Incidentes de TI; Disponibilidade de serviços; Eficiência; Instituição Financeira; Tecnologia da Informação.

ABSTRACT

MENEGHELLI, Aldoino Jr. Case Study - Application of best practices for Information Technology (Incident Management) for a Financial Institution. 2014. XX f. Monograph (Specialization Curse in Management of Information Technology and Communication) – Universidade Tecnológica Federal do Paraná, Curitiba, 2014

The case study aims to investigate the relationship between the amount of Incident Information Technology reported on a financial institution and applying best practices relating to IT service availability. The study was based on a quantitative and qualitative analysis considering a database of approximately two (2) years concerning the number of incidents recorded Information Technology and indexes of availability of services during the same period. The selection criterion was the availability of services and noted the risk that these services offer to the Financial Institution evaluated. The survey seeks to measure a quantity index Incident Information Technology versus availability listed for research systems, as well as the reflection of these indices in the operational efficiency of a Financial Institution.

Key words: Best practices of IT; Incident Management IT; Availability of services; Efficiency; Financial Institution; Information Technology.

Sumário

1 INTRODUÇÃO

Atualmente a Tecnologia da Informação está presente em praticamente todos os ramos de negócio, sejam estes direta ou indiretamente vinculados ao produto final. Empresas que anteriormente poderiam atuar com controles de produção e logística, anotações e fichários contábeis, cadastro de clientes e fornecedores dependentes apenas do conhecimento e experiência das pessoas, hoje não sobreviveriam. O crescimento em escalas variadas, a competitividade crescente, o dinamismo do mercado atual e a conexão global de comercialização de produtos podem ser apontados como alguns dos fatores influenciadores e que justificam a efetiva aplicação da Tecnologia da Informação. Para muitos ramos de negócios, a Tecnologia da Informação é considerada como ponto fundamental e estratégico para sobrevivência de uma empresa. Estar inserido no contexto tecnológico, estar conectado às necessidades do cliente e, principalmente, aperfeiçoar custos de operação e/ou produção podem acelerar e alavancar uma empresa considerando sua missão e visão estratégica. Considerando a concorrência dinâmica e o risco associado a erros vinculados ao produto, o fato de estar inserido no contexto tecnológico requer investimentos, aplicação de controles e de processos para apoio nesta caminhada. Neste cenário, encontramos um processo chamado de Gestão da Tecnologia da Informação.

A Gestão da Tecnologia da Informação atua diretamente em vários aspectos dentro de uma organização. Desde etapas consideradas simples até as mais elaboradas e complexas que demandam grandes investimentos em equipamentos e processos. Automatizar e otimizar processos dentro de uma instituição podem justificar os devidos investimentos, entretanto devem ser minuciosamente mensurados visando maximizar, tanto lucros quanto a eficiência operacional organizacional. Considerando a importância da Tecnologia da Informação e a necessidade vinculada de gestão associada, encontramos dentre os diversos processos de governança da Tecnologia da Informação, o *framework* de mercado ITIL (Information Technology Infrastructure Library), utilizado como base para o estudo apresentado.

1.1 CONSIDERAÇÕES INICIAIS

Considerando a necessidade de interação com o cliente de maneira rápida e efetiva, alta disponibilidade, conectividade e, principalmente, a tecnologia envolvida, foi definido como objeto deste estudo a aplicação de gestão e governança de Tecnologia da Informação para uma Instituição Financeira. Retomando os pontos anteriormente citados, é possível identificar imediatamente algumas necessidades vinculadas ao tipo de serviço oferecido pela Instituição Financeira. Necessidades estas podem ser resumidamente elencadas como:

- ✓ Alta disponibilidade de serviços de autoatendimento, em canais de agências e postos de atendimento bancário;
- ✓ Segurança adequada para as transações financeiras atendidas pela instituição;
- ✓ Qualidade dos serviços oferecidos para estar de acordo com o dinamismo do mercado financeiro;
- ✓ Rapidez no atendimento a problemas relacionados a indisponibilidades de sistemas, bem como, problemas relacionados aos processos das áreas de negócio envolvidas;

Em conjunto com as necessidades acima listadas, podem ser identificados pontos quando a gestão de TI é considerada essencial para uma instituição financeira, como por exemplo:

- ✓ Alinhamento e dependência de TI com as necessidades do negócio;
- ✓ Complexos ambientes de TI vinculados à disponibilidade de serviços e produtos;
- ✓ Redução de custos e riscos;
- ✓ Justificativa para investimentos em TI dentro da instituição;
- ✓ Conformidade com órgãos regulatórios e legislação da área de negócio;
- ✓ Segurança da Informação envolvida;

Considerando os pontos acima listados, além de outros que serão citados ao longo deste estudo, o foco deste documento será o processo de Gestão de

Incidentes de TI para uma Instituição Financeira. Este processo está inserido no livro de ITIL designado como Suporte a Serviços.

A Instituição Financeira em foco prevê alta disponibilidade de seus produtos e serviços. Considerando este cenário, o estudo será voltado à aplicação do processo de Gestão de Incidentes de TI e busca vincular uma associação com a disponibilidade dos serviços atendidos pela Instituição Financeira.

1.2 JUSTIFICATIVA

A implantação de um processo de Gestão de Incidentes pode gerar custos operacionais que financeiramente pode não ser possível estabelecer relação direta com índice de negociação de produtos financeiros e/ou serviços, benefícios de novos projetos e/ou campanhas, e até mesmo, no aumento ou diminuição de índices de retenção de clientes. Contudo quando ocorre um Incidente de TI, impactos e prejuízos podem ser pulverizados por diversas áreas de TI e de negócios, entretanto sem a devida caracterização do problema e/ou correção efetiva. Sem um controle e gestão deste evento, a instituição pode assumir um risco com indisponibilidades em sistemas críticos de TI que não sejam recuperados rapidamente ou em tempo hábil visando minimizar impactos, perdas financeiras ou processuais, inclusive referente a cumprimento de prazos regulatórios que podem por em risco a operação da Instituição Financeira.

Justificar a implantação e manutenção de um processo preciso de Gestão de Incidentes de TI pode representar indiretamente a manutenção de uma área interna de TI para a Instituição Financeira. Casos de terceirização de áreas de TI são comuns em diversos ramos de negócio, entretanto para o ramo financeiro há uma série de cuidados específicos que podem comprometer a confiabilidade da instituição e, há um grande risco vinculado a este ramo quando a questão é confiabilidade.

Como fator essencial, também é evidenciado a globalização dos serviços atuais no ramo financeiro, a interdependência de sistemas e a pulverização de clientes conectados em diversos países, em diferentes fusos horários e aptos a realizarem transações financeiras a qualquer momento. Deve estar claro o conceito de como esta conectividade associada ao complexo ambiente tecnológico

envolvido, afeta diretamente a operação de uma instituição financeira.

Ações rápidas e efetivas para resolução de problemas de tecnologia, integração entre equipes multidisciplinares de suporte e de múltiplos idiomas para avaliação imediata de risco, impacto e urgência fazem parte do cotidiano de instituições globais e a efetividade neste processo pode representar um grande passo neste mercado.

A competitividade do ramo financeiro associado à necessidade de estar disponível a qualquer momento, conectado aos diversos mercados e principalmente aberto às novas tecnologias significam um grande desafio para as instituições.

Embora o foco de globalização esteja presente e evidente, muitas das ações locais representam importância e principalmente apoiam na caminhada da instituição. Uma missão global com diversas ações locais deve estar alinhada internamente na instituição.

Neste estudo, manter o foco no processo de Gestão de Incidente de TI vinculando os resultados diretos nos serviços atendidos pela instituição serão base deste documento.

1.3 PROBLEMA

A utilização da tecnologia nas Instituições Financeiras vem se tornando ao longo do tempo cada vez mais presente no cotidiano dos colaboradores, bem como, dos clientes que utilizam os serviços disponibilizados pela instituição. Alguns processos e serviços podem ser listados dentre aos diversos inseridos em uma área de tecnologia de uma instituição financeira, como por exemplo:

- ✓ Processamento online, diário, semanal e mensal de transações e operações realizadas ao longo de um período considerando clientes, prestadores de serviço e colaboradores;
- ✓ Sistemas online, como por exemplo: página institucional (*Public WebPage*), serviços de internet para clientes (*Personal Internet Banking*, *Business Internet Banking*, *Mobile Banking*), Portal de Investimentos para clientes e corretoras, sistemas de Call Centers de atendimentos diversos (vendas, contratações, cobranças,

cancelamentos e reclamações diversas), ATMs (*Automatic Terminal Machines*), dentre outros;

- ✓ Sistemas online de uso interno das instituições, como por exemplo: processos de compensação de cheques; processos de transferências financeiras entre agencias e instituições distintas; processamento financeiro e contábil; reporte para órgãos regulatórios; controles internos de segurança de acesso, invasão física e virtual, processos e transações, dentre outras;

As atividades acima listadas correspondem à apenas um percentual do que uma instituição financeira atende, processa, controla e reporta. Não é uma atividade simples controlar todos os sistemas de tecnologia, bem como processos que uma instituição atende e uma dificuldade maior ainda quando um destes sistemas apresenta falhas promovendo o que é chamado de um Incidente de TI. Uma situação ainda mais crítica pode ser instaurada quando um sistema apresenta falhas e não há um controle efetivo de recuperação desta falha. Este controle remete à coordenação de atividades, engajamentos de especialistas e escalonamento necessário para recuperação rápida e efetiva do sistema que apresentou falha.

Considere um evento como a mensagem de “Sistema Temporariamente Indisponível” para um sistema de Internet Banking durante horário comercial e um dia de semana. A situação comentada requer o envolvimento de especialistas de diversas áreas de infraestrutura e suporte à aplicação de tecnologia, bem como pode surgir uma necessidade de engajamento de fornecedores externos. Considere da mesma forma apenas o envolvimento de especialistas de infraestrutura e neste cenário, deverão ser consideradas diversas áreas de suporte: servidores de infraestrutura, banco de dados, redes de telecomunicação, bem como suas instâncias de escalonamento. Caso a instituição não possua um processo para gerenciar e coordenar as ações de recuperação interagindo com as diversas equipes envolvidas, a instituição corre o risco de deixar seu sistema indisponível por minutos ou até horas, considerando um evento conhecido como Incidente de TI de severidade e prioridade crítico.

Considerando este sistema de “Internet Banking” com falha, poderão ser facilmente caracterizados alguns impactos imediatos como, por exemplo: perda de

transações financeiras, aprovação de créditos, contratação de serviços; além dos prejuízos de reputação com clientes afetando a marca da instituição, bem como divulgação negativa em mídias diversas; além de risco com ações regulatórias dos órgãos responsáveis.

Com o evento descrito acima é possível caracterizar diversos problemas que uma falha de um sistema de TI em uma instituição financeira pode acarretar.

1.4 OBJETIVOS

A seguir, serão apresentados os objetivos gerais e específicos deste estudo.

1. Objetivo geral

O objetivo geral é apresentar como o processo de Gestão de Incidentes de TI pode interagir com a visão e missão estratégica de uma Instituição Financeira, bem como com a disponibilidade dos serviços atendidos por esta instituição.

2. Objetivos específicos

Apresentar os conceitos do processo de Gestão de Incidentes de TI no cenário de uma instituição financeira.

Descrever a interação e importância do processo de Gestão de Incidentes de TI na disponibilidade dos serviços atendidos pela instituição financeira.

Apresentar a necessidade de manter processos de Gestão de TI que não podem ser mensuráveis de maneira objetiva e direta.

Apresentar resultados comparativos com a aplicação de processos de Gestão de Incidentes de TI.

1.5 METODOLOGIA

A metodologia aplicada para este estudo baseia-se em uma coleta demonstrando a quantidade de incidentes de tecnologia registrados por ferramentas padronizadas de controle interno da instituição em foco associado a um estudo destes incidentes realizando um vínculo com a disponibilidade dos serviços eleitos para a pesquisa.

A investigação aplicada foi baseada nas seguintes linhas de negócio eleitas conforme grau de importância para a instituição financeira, como segue:

- ✓ *Personal Internet Banking* – incidentes que impactaram canais de atendimento para clientes Pessoa Fisica;
- ✓ *Business Internet Banking* – incidentes que impactaram canais de atendimento para clientes Pessoa Jurídica;
- ✓ *Payments* – serviços e transações de pagamentos;
- ✓ *CallCenter Services* – incidentes que impactaram canais de atendimento via CallCenters para diversos serviços como: contratações, cancelamentos , reclamações, cobrança, etc;
- ✓ *Branches Application and Network* – incidentes que impactaram canais de atendimento em agências para clientes em geral – considerados incidentes em sistemas de tecnologia, ou seja, sem foco para incidentes de ordem natural ou devido a arrombamentos e afins;

O procedimento de pesquisa foi motivado pela necessidade de justificar a manutenção de uma área de gestão de incidentes de IT e principalmente justificar a ampliação desta área perante a instituição.

A instituição foco deste estudo foi denominada como Banco GETIC por questões de confidencialidade e a pesquisa dos dados contempla os anos de 2012 e 2013 para coleta em bases de controle internas da instituição.

A relação entre a efetividade do processo de gestão de incidentes com a disponibilidade dos serviços atendidos pela instituição é a informação alvo deste estudo.

2 FUNDAMENTAÇÃO TEÓRICA

Contemplar os diversos documentos existentes que explicam as definições de gestão de serviços de TI, o ciclo de vida de um incidente de TI e cada uma das suas etapas.

2.1 *FRAMEWORK* ITIL (*Information Technology Infrastructure Library*)

Em função da necessidade de apoio na governança de serviços de TI considerando um padrão mínimo de atendimento para prestadores de serviços desta área, a ITIL (*Information Technology Infrastructure Library*) foi criada no final da década de 1980 pela CCTA (*Central Communication and Telecom Agency*), atual OGC (*Office of Government Commerce*) principalmente para prover um padrão mínimo de atendimento destes prestadores para o governo britânico em função da crescente demanda de terceirização de serviços de IT.

Segundo informado em Project Management & Software Engineering (April 2013), as boas práticas ITIL descrevem processos, procedimentos, tarefas e listas de verificação que não são específicas para uma instituição, mas são usadas por estas para estabelecer integração com a estratégia da instituição, entregando valor e mantendo um nível mínimo de competência. Permite da mesma forma, que a instituição possa estabelecer uma base a partir da qual ela pode planejar estratégias, programar alterações e medir desempenho do ambiente. ITIL é usado também para demonstrar a conformidade e para medir melhorias implantadas.

Desde então, esta biblioteca de boas práticas de gerenciamento de serviços vem sendo usado por diversas instituições que prestam serviços e/ou que contratam serviços de TI visando a otimização dos processos internos de gerenciamento de TI.

Durante a década de 1990, o ITIL passou a ser usado por diversas instituições privadas em grande escala visando garantir a utilização de boas práticas de TI. Desde a sua formação, passou por algumas atualizações e atualmente a “biblioteca ITIL” – como é conhecida é composta de 5 (cinco) livros, como segue:

- ✓ *Service Strategy* (Estratégia do serviço);
- ✓ *Service Design* (Projeto de serviço ou Desenho de serviço);
- ✓ *Service Transition* (Transição do serviço);
- ✓ *Service Operation* (Operação do serviço);
- ✓ *Continual Service Improvement* (Melhoria contínua do serviço);

Estes cinco livros relacionam e se completam em diversas etapas. Fases como definições de estratégia, design de um serviço, fases de piloto de implantação, bem como de transição, operação e posteriormente, mas não menos importante, a fase de melhoria continua fecham o ciclo de vida de um serviço de TI.

O foco deste estudo foi definido baseando-se no quarto livro “Operação de Serviço”. Segundo publicação em *ITIL – OGC – Service Operation* - Operação de Serviço é a fase no ciclo de vida de um serviço de IT que é responsável pelas atividades de conhecidas como *as-usual-business.* A Operação de Serviço pode ser visto como a "fábrica" de TI. Isto implica um foco mais atento sobre as atividades do dia-a-dia e infraestrutura que são utilizados para prestar serviços. No entanto, esta publicação é baseada na compreensão que o objetivo principal da Operação de Serviço é entregar e servir de apoio.

Gestão das atividades de infraestrutura e do funcionamento adequado do serviço deve sempre apoiar esta finalidade. Processos bem planejados e implantados não tem efeito algum se a operação do dia-a-dia desses processos não é bem conduzida, controlada e gerenciada. Muito menos melhorias nos serviços serão possíveis se as atividades do dia-a-dia, como por exemplo, monitorar desempenho, avaliar métricas e coletar dados não são sistematicamente realizados durante Operação de Serviço. Conforme retratado em *ITIL – OGC – Service Operation*, um dos conflitos existentes em todas as fases do ciclo de vida de um serviço de TI é relação entre a visão de TI, como um conjunto de serviços de TI, que é a visão das áreas de negócio e a visão pura de TI, como um conjunto de componentes de tecnologia, que reflete a visão interna de TI.

O ponto de vista externo de TI é a forma como os serviços são experimentados por seus usuários e clientes. Para esta visão, não são considerados entendimentos específicos, bem como detalhes de que tecnologia é usada para gerenciar os serviços. Para esta visão, a preocupação maior é que os

serviços sejam entregues conforme necessário e acordado.

O ponto de vista interno de TI é a maneira em que TI com seus componentes e sistemas são administrados para entregar os serviços. Como os sistemas de TI são complexos e muitas vezes, isto significa que a tecnologia é gerida por diversas equipes ou departamentos diferentes e cada um destes, com seu foco em alcançar um bom desempenho e disponibilidade de "seus" sistemas.

Ambas as visões são necessárias quando a prestação de serviços de TI ocorre em uma instituição. A instituição que se concentra apenas em requisitos de negócios, sem mensurar como estes são entregues, acabam fazendo promessas que não podem ser mantidas. A instituição que se concentra apenas em sistemas internos, sem pensar sobre o que seus serviços suportam e entregam, corre o risco de fornecer serviços caros e que oferecem pouco valor.

Este potencial conflito entre o papel externo e visão interna é o resultado de muitas variáveis, incluindo a maturidade da instituição, a sua cultura de gestão, sua história e estratégia de mercado. Este conflito faz com que um equilíbrio entre as visões seja difícil de conseguir, e a maioria das instituições tendem mais para uma visão do que a outra. Naturalmente, nenhuma instituição será totalmente focada interna ou externamente, mas vai encontrar-se em uma posição ao longo de um range entre as duas visões.

Segundo a publicação de *Project Management & Software Engineering – ITIL,* a Operação de Serviço tem como objetivo proporcionar as melhores práticas para alcançar a entrega de níveis acordados de serviços tanto para os usuários finais quanto para clientes. Neste cenário, clientes referem-se aos responsáveis que pagam pelo serviço e negociam os níveis de acordo de serviço - SLAs.

Operação do serviço, conforme descrito no volume *ITIL Service Operation*, é a parte do ciclo de vida em que os serviços são entregues diretamente. Nesta etapa, é considerada a monitoração de problemas e equilíbrio entre a confiabilidade do serviço e o custo. As funções incluem a gestão técnica, gestão de aplicações, gestão de operações e de *Service Desk*, bem como, as responsabilidades para os times envolvidos na Operação do Serviço.

Nesta biblioteca de Operação de serviços, são contemplados os seguintes processos:

- ✓ Event management (gestão de eventos);
- ✓ Incident management (gestão de incidentes);

- ✓ Change management (gestão de mudanças);
- ✓ Problem management (gestão de problemas);
- ✓ Access management (gestão e controle de acesso);
- ✓ IT Operations Control
- ✓ Facilities Management
- ✓ Application Management
- ✓ Technical Management

Deste livro, Operação de Serviços, será aprofundada especificamente dois processos:

- ✓ Gestão de Incidentes de IT;
- ✓ Gestão de Problemas de IT;

.

2.2 GESTÃO DE INCIDENTES DE TI

De acordo com a publicação de *Project Management & Software Engineering – ITIL,* gestão de Incidentes tem como objetivo restaurar a operação normal de serviço o mais rápido possível e reduzir impactos sobre as operações de negócios, garantindo assim que os melhores níveis de qualidade e disponibilidade de serviço sejam entregues e mantidos.

Considerando todas as atividades de gestão de serviços em IT, torna-se coerente ter o entendimento claro das interações entre diversos processos que se enquadram no livro “Operação do Serviço”.

Assim como a Gestão de Incidentes, podemos citar: Gestão de Problemas (*Problem Management*), Gestão de Mudanças (*Change Management*), bem como a integração com áreas de Gestão de registro de chamados e atendimento de primeiro nível (*Service Desk- access management*).

A interação entre estes processos podem afetar diretamente o processo de Gestão de Incidentes, conforme exemplo:

Uma mudança sem o devido controle pode gerar um incidente. Este incidente caso não seja registrado adequadamente pelo *Service Desk* pode não ter o tratamento adequado, conforme urgência, criticidade e impacto e, por fim, caso um incidente não tenha o devido tratamento posterior pelo processo de gestão de

problemas, podem ocorrem novamente, o que é chamado de reincidente.

Diversas são as maneiras de registro e tratamento adequado de um incidente, desde o reporte imediato na ocorrência, o devido e correto grau de escalonamento, assim como o tratamento pós-incidente para definição efetiva da causa e definição de planos efetivos para correção desta causa.

A terminologia usada em ITIL define um incidente como: *uma interrupção não planejada em um serviço de IT ou uma redução da qualidade de um serviço de IT. Falha de item de configuração que não impacta diretamente um serviço pode ser classificada como um incidente.* Conforme citado em *Project Management & Software Engineering – ITIL,* um evento que não faz parte da operação padrão de um serviço e que causa ou pode causar interrupção ou redução na qualidade dos serviços e produtividade do cliente também pode ser classificado como um Incidente.

O processo de gestão de incidentes tem como missão essencial recuperar um serviço à sua operação normal o mais rápido possível e minimizar impactos para a operação das áreas de negocio envolvidas e desta forma garantir a manutenção do melhor nível de acordo de serviço e qualidade do mesmo.

Como há uma necessidade clara de manter níveis de serviço contratados entre IT e áreas de negócios (*business*), é possível relacionar diversos valores agregados à gestão adequada de Incidentes, como por exemplo:

- ✓ Habilidade de resolver incidentes reduzindo o tempo de indisponibilidade dos serviços;
- ✓ Habilidade de alinhar atividades em IT em tempo imediato de acordo com as prioridades previamente definidas pelas áreas de negócio;
- ✓ Habilidade para identificar melhorias nos sistemas afetados, assim como, prover a informação adequada sobre o evento para os diversos níveis gerenciais da instituição.

Para que o processo de gestão de incidentes seja efetivo, o registro adequado do evento tem importância significativa, pois pode definir as etapas necessárias bem como, o esforço demandado para resolução do problema. Seguem alguns itens importantes para o registro adequado do incidente:

- ✓ Código/protocolo para este incidente – apoio para as diversas áreas de controle;

- ✓ Categoria do Incidente – por exemplo: hardware, software, telecom, etc;
- ✓ Urgência, impacto e priorização do incidente;
- ✓ Datas e horários do inicio do incidente;
- ✓ Contatos que devem ser designados como responsáveis pelo incidente – não deve ser confundido com causador do incidente;
- ✓ Notificação – comunicação do Incident – via telefone, via email, etc
- ✓ Descrição dos sintomas;
- ✓ Descrição dos componentes de IT relacionados;
- ✓ Descrição das atividades conduzidas durante o incidente;
- ✓ Datas e horários da resolução do incidente;
- ✓ Categoria, impacto e registro final do incidente;

Durante um incidente em andamento e gerenciamento de uma conferencia telefônica de crise, também conhecida como *crisiscall*, níveis diferentes de escalonamento são acionados pelo gestor da conferencia. O escalonamento técnico com os especialistas adequados para a resolução do problema, assim como o escalonamento hierárquico e funcional assim que identificado na conferencia que o tratamento em andamento não está sendo efetivo. Escalonamentos gerenciais e com as áreas de negócio também podem ser utilizados visando informar adequadamente às áreas executivas da instituição sobre crises em andamento.

Dentre as atividades do processo de gestão de incidentes, podem ser citados:

- ✓ Avaliação do evento;
- ✓ Triagem e suporte inicial;
- ✓ Registro do evento;
- ✓ Coordenação de ações para recuperação;
- ✓ Garantir a recuperação do evento – registro;
- ✓ Apoio nas atividades de identificação da causa do incidente – gerenciamento de problemas;

Avaliação do Evento

Durante este processo são realizados diversos questionamentos referentes ao evento/incidente de TI, considerando fatos que podem confirmar ou não o atendimento pelo processo de incidentes.

Perguntas comuns durante este processo:

- ✓ Identificar qual área usuária apresenta reclamações do serviço;
- ✓ Identificar o impacto – o mais preciso possível;
- ✓ Quais são os motivos que demandam uma solução imediata;
- ✓ Quando iniciou o incidente e onde está a área negocial e serviço afetado;
- ✓ Como o processo de incidentes pode ajudar e se possível quantificar o incidente;
- ✓ Avaliar o tipo de registro do incidente e como deverão ser conduzidas as ações de recuperação;

Triagem e suporte inicial

Nesta etapa podem ser utilizadas bases de conhecimentos de eventos/incidentes previamente cadastrados e com suas respectivas soluções aplicadas, bem como iniciar o engajamento inicial das áreas envolvidas. Nesta etapa já é possível identificar a condução adequada para este incidente, ou seja, se poderá ser tratado apenas através de um protocolo de incidente, com tratamento assistido de um time de suporte ou assistido pela área de gestão de incidentes.

Registro do evento

Definido a necessidade de condução da atividade pelo processo de gestão de incidentes, alguns pontos são importantes, como por exemplo:

- ✓ Registro adequado da ocorrência;
- ✓ Avaliação e ajustes nas informações levantadas – visando o reporte

adequado para níveis gerenciais e definir o tipo de publicação, por exemplo, caso seja necessário caracterizar uma situação critica que demanda engajamento imediato de todos os times.

Coordenação de ações para recuperação

Dentre as atribuições de um coordenador que faz a gestão do incidente, conhecido como *Incident Manager*, podem ser listadas como principais as seguintes:

- ✓ Estabelecer e gerenciar uma conferencia de crise – *CrisisCall*;
- ✓ Coordenar e facilitar as ações de recuperação do serviço afetado;
- ✓ Compartilhar o senso de urgência, severidade e impacto com o público da conferencia e através do reporte adequado;
- ✓ Garantir o engajamento adequado de todas as equipes de suporte necessárias para a resolução do problema;
- ✓ Garantir o escalonamento adequado para os diversos níveis;
- ✓ Garantir que a conferência transcorra de forma tranquila, embora esteja sob a pressão para recuperação rápida e efetiva do serviço;

Acima foram listadas algumas das responsabilidades do coordenador da conferencia para recuperar os serviços de tecnologia de acordo com o nível de serviço acordado com as áreas negociais.

Garantir a recuperação do evento – registro

Tão logo recuperado o serviço afetado, esta informação deverá ser confirmada com os usuários e áreas que iniciaram o registro do evento e assim que confirmada a regularização, deverá ser enviado um comunicado informando sobre a recuperação do serviço. A classificação de severidade e impacto do incidente pode, neste momento, ser revisada considerando evidencias e informações de usuários.

Apoio nas atividades de identificação da causa do incidente – gestão de problemas

Depois de concluídas atividades de recuperação do serviço, é iniciado o processo de avaliação do incidente, suas causas e ações que podem ser introduzidas no sistema visando a não recorrência do evento.

2.3 CICLO DE VIDA DE UM INCIDENTE DE TI

Conforme descrito no capítulo anterior, as distintas fases da gestão de Incidentes apoiam na composição do ciclo de vida de um incidente de TI.

Por ser um processo intermediário do conhecido livro *Service Operation*, o processo de incidentes possui algumas etapas conhecidas como entradas e saídas que podem ser classificados até como interfaces do processo.

Entradas do processo de gestão de Incidentes

Dentre as entradas ou interfaces que alimentam ao processo de incidentes podem ser listados processos e serviços de *Service Desk*, áreas de operação, monitoração, suporte de aplicação e infraestrutura, processos de mudanças e processos que independem do controle da instituição, como por exemplo: incidentes naturais (aspectos climáticos ou de características geográficas) e incidentes de ordem física. Estas entradas iniciais somadas às entradas pertinentes ao processo, como por exemplo, consulta à uma base de conhecimento (*Knowledge Base*), experiência e conhecimento do corpo técnico compõe o gatilho inicial para o processo de gestão de um incidente de IT. Tais entradas tem papel fundamental durante o ciclo de vida do incidente, pois auxiliar no direcionamento das ações de recuperação do serviço contemplado.

Considerando uma Instituição Financeira, a interdependência de serviços, aplicativos e infraestrutura pode representar um considerável risco para a operação, entretanto, como o devido controle destas entradas pode da mesma

forma, representar efetividade na resolução de problemas, bem como na redução de impactos para as áreas de negócio. Neste ponto é possível mensurar, por exemplo, uma aplicação bancária que é executada em determinado país, entretanto depende de informações que são processadas em outro país e em caso de falhas, os times de gestão de incidentes devem interagir entre si visando à rápida recuperação dos serviços envolvidos. Interações estas que podem ser transparentes aos olhos das áreas de negócio, entretanto representam papel fundamental na recuperação do serviço.

Saídas do processo de gestão de Incidentes

Depois de finalizadas as etapas de condução de um incidente de IT, ou seja, depois de recuperados todos os serviços afetados, podem ser observadas diversas saídas do processo de incidentes. As saídas podem ser listadas inicialmente como as mesmas que realimentam o processo e listadas como entradas do processo, ou seja, ao encerrar um incidente, todas as informações pertinentes e importantes ao assunto são armazenadas na base de conhecimento para uso futuro em novos atendimentos do processo de incidentes.

Outra saída característica do processo são as conhecidas requisições de mudanças, ou seja, alterações no sistema que deverão ser comandadas e que foram identificadas durante o incidente e outra saída característica do processo de incidentes é alimentar o processo de gestão de Problemas que visa identificar a causa efetiva de um incidente, quando não está evidenciada durante o incidente e visa da mesma forma, viabilizar ações de melhorias no sistema ou infraestrutura envolvida visando evitar novas ocorrências. Este processo de gestão de problemas será abordado com mais detalhamento nos próximos capítulos.

Considerando as entradas e saídas do processo de gerenciamento de Incidentes citados acima, o ciclo de vida de um incidente é encerrado, ou seja:

- ✓ Incidente evidenciado;
- ✓ Incidente registrado e reportado adequadamente;
- ✓ Condução de ações de recuperação;
- ✓ O incidente é finalizado e resolvido;
- ✓ Bases de conhecimento são atualizadas;

- ✓ O processo de gerenciamento de problemas identifica adequadamente as causas do evento, assim como, viabiliza ações de melhorias para o sistema envolvido.

Vale frisar que o ciclo de vida de um incidente não deve ser confundido com o ciclo de vida de um serviço que abrange outras atividades e processos, entretanto pode ser considerado que o ciclo de vida de um incidente de IT está inserido no ciclo de vida de um serviço de IT.

2.4 GESTÃO DE PROBLEMAS

Este processo de gestão de Problemas (Problem Management) é da mesma forma tão importante quanto o processo de gestão de Incidentes, pois reflete uma segunda etapa de investigação, correção e adoção de melhorias para os sistemas afetados.

Segundo publicação em *ITIL – OGC – Service Operation,* gestão de Problemas é o processo responsável pelo acompanhamento e gestão do ciclo de vida de todos os problemas e incidentes de TI. Dentre sua missão, está identificar a causa raiz e prevenir problemas para que incidentes não ocorram e principalmente, eliminar incidentes recorrentes e minimizar o impacto de incidentes que não podem ser evitados. De acordo com esta mesma publicação e conforme comentado, inclui atividades necessárias para diagnosticar a causa raiz de incidentes e determinar a resolução de tais problemas. É da mesma forma, responsável por garantir que a resolução aplicada através de procedimentos através de controles adequados, especialmente.

A gestão de Problemas apoia da mesma forma nas alterações necessárias, bem como suas liberações. Mantem informações sobre os problemas e as soluções apropriadas, bem como resoluções, de modo que a instituição pode ser capaz de reduzir o número e impacto dos incidentes ao longo do tempo.

Quando se mantem informações sobre problemas, pode ser estabelecido uma forte relação com Gestão do Conhecimento, e ferramentas de gestão de base de dados de conhecimento. Esta base de dados de erro será utilizada para ambos os processos – gestão de incidentes e de problemas.

Apesar de Incidentes e Gestão de Problemas serem processos separados, eles estão intimamente relacionados e usam as mesmas ferramentas, e ainda, podem usar categorização semelhante, ou seja, impacto e prioridade de sistemas de TI referentes aos impactos, urgência e prioridade de atendimento.

Este fato assegura efetivamente a comunicação ao lidar com incidentes relacionados e problemas.

Depois de finalizado um Incidente, é providenciado o relatório pela área de gestão de Incidentes evidenciando todas as etapas deste evento e visa subsidiar informações ao processo de gestão de Problemas. Nesta etapa, podem ser realizadas reuniões (presenciais ou via conferencia) entre os responsáveis pelos serviços afetados e responsáveis pela infraestrutura e aplicação envolvida.

Nestas reuniões são discutidas as razões de ocorrência do evento, quais foram os impactos evidenciados durante e posteriormente ao incidente registrado e se há ações de melhoria para correção definitiva ou visando uma não recorrência do mesmo incidente.

Conforme a dimensão da instituição e periodicidade de ocorrência de incidentes, estas reuniões podem ter datas específicas durante a semana ou conforme demanda – de acordo com a quantidade de incidentes registrados. Um cuidado extra com este processo e deve ser registrado, é que não haja uma diferença de tempo muito grande entre a ocorrência do incidente com a reunião de gerenciamento de problema, evitando que o assunto possa cair no esquecimento, não do registro, mas das informações mais relevantes e que devem ser discutidas logo após a ocorrência do incidente.

De acordo com a necessidade das áreas de negócio, este processo pode ser invocado para apoio na identificação de situações que oferecem risco para a operação e que demandam de um esforço comum de diversas equipes, sejam estas de infraestrutura, aplicação e ou prestadores de serviços. Estas atividades são conhecidas como melhorias de serviços em operação e concentram seu foco em evitar incidentes através de atividades e/ou mudanças devidamente controladas, registradas e reportadas.

Considerando a interdependência dos processos de Gestão de incidentes e de problemas, podem ser elencados, da mesma forma, valores para as áreas de negocio, como:

- ✓ Aumento na disponibilidade e qualidade de serviço;

- ✓ Informações gravadas de incidentes resolvidos podem acelerar o tempo de resolução e identificar soluções permanentes;
- ✓ Reduz o número e tempo de resolução de incidentes e com este fato, reduz para a área de negocio, tempo de inatividade e de interrupção de negócios para sistemas críticos;
- ✓ Redução das despesas em soluções ou correções;
- ✓ Redução no custo de esforço no combate a incêndios ou para resolver incidentes repetidos.

Na ocorrência de incidentes que caracterizam uma criticidade e/ou severidade considerada de grande impacto, o processo de gestão de problemas deve ser convocado para formação de um comitê especifico para análise deste incidente. Trata-se do mesmo foco, entretanto com duração que depende da complexidade do sistema envolvido e pode variar entre semanas e meses, de acordo com as atividades que são elencadas para o evento.

Considerando sistemas e instituições globais, este processo desempenha função essencial de controle na atividade de pós-incidente, pois sistemas que interagem entre diversos países e regiões podem apresentar barreiras no momento em que é necessário um comitê de esforço comum para implantar e definir etapas de melhoria nos sistemas e, sem a coordenação de uma equipe específica, a tendência de fracasso nestas atividades aumenta e consequentemente, aumentam as chances da ocorrência de incidentes nos sistemas envolvidos.

A interação entre o processo de gestão de incidentes e de problemas é essencial para a disponibilidade e qualidade de um serviço de TI e visa principalmente manter o nível de acordo de serviço previamente definido entre TI e uma área de negócio.

O reflexo da interação entre os processos de gestão incidente e de problemas pode ser mensurado ao longo do tempo evidenciando a diminuição de incidentes ou a não recorrência dos mesmos incidentes em uma instituição.

O processo de Gestão de Problemas pode ser apresentado de forma reativa e proativa:

- ✓ Reativa - provém de problemas que são originados durante a operação de serviço;

- ✓ Proativo – provém de problemas que se iniciou na Operação de Serviço, mas geralmente conduzida como parte de Melhoria de Serviço Continuada (que não será foco deste estudo).

Assim como o processo de gestão de incidentes, o processo de gestão de problemas possui diversas etapas e podem ser relacionadas da seguinte maneira:

- ✓ Detecção do Problema – problemas podem ser levantados por diversas fontes, como: incidentes, registros excessivos no Service Desk de problemas que não foram categorizados no processo de incidentes, eventos em alertas de monitoração que podem afetar sistemas críticos, etc;
- ✓ Registro do Problema – para informar a ocorrência, impactos, usuários e sistemas afetados, contatos necessários, detalhes técnicos do incidente e descrição detalhada do incidente, assim como as ações conduzidas para recuperação do mesmo;
- ✓ Categorização do Problema – de acordo com uma matriz de impactos ajustada conforme necessidades da instituição, áreas de TI e áreas de negocio, os problemas podem ser classificados conforme categoria de atuação, como por exemplo, erros de aplicação, problemas de infraestrutura, problemas de design ou de implantação de projetos, dentre outros;
- ✓ Priorização do Problema – caracterizar a prioridade que as equipes devem atuar para correção dos problemas de acordo com as necessidades das áreas de negócio, esforços de TI e custos associados;
- ✓ Investigação e Diagnóstico do Problema – efetivamente a fase de trabalho e reuniões para analise da causa raiz e possíveis correções e melhorias cabíveis para o problema evidenciado.

Diversas causas podem ser relacionadas para os incidentes e/ou eventos durante a gestão de problemas e cada uma poderá resultar em um trabalho especifico de atuação que contempla obrigatoriamente a relação custo beneficio para a instituição e, consequentemente, assim como o processo de gestão de incidentes pode ser medido através de métricas especificas para cada processo.

2.5 RISCO, URGÊNCIA E IMPACTO DE INCIDENTES PARA SERVIÇOS DE TI

Os incidentes de TI podem ser classificados inicialmente de acordo com risco, urgência e impacto que oferecem para as áreas de negócio e diretamente associados ao nível de acordo de serviço contratado entre TI e área de negócio.

Risco

O risco é mensurado de acordo com a importância do serviço envolvido e a infraestrutura que o atende. Considerando uma instituição financeira, por exemplo, é possível evidenciar um risco relacionado a algum processo de execução programada durante a madrugada e que extrapola seu horário de execução. Caso este processo invada um horário de processamento conhecido como *online* será evidenciado o risco para transações também conhecidas como *online* devido à concorrência de processos durante o dia e neste caso, na visão do cliente, uma transação que normalmente levaria alguns segundos pode se arrastar por alguns minutos.

Considerando este mesmo exemplo e apenas transbordando para um cenário de aproximado de 1000 transações por segundo (numero comum para o ramo financeiro), podemos imaginar o efeito cascata deste evento. Outra maneira fácil de evidenciar um risco é uma situação onde a instituição possui, por exemplo, um agencia em determinada região e que á atendida por duas conexões (links) de telecomunicação. Caso ocorra falha em uma das conexões, evidenciamos um risco associado à operação desta agencia caso não sejam tomadas ações de recuperação.

Urgência

A urgência de um incidente pode ser caracterizada conforme a necessidade de recuperação de um serviço envolvido, como por exemplo, um sistema de internet banking indisponível para clientes. Pode ser evidenciado que o conceito de risco para este exemplo ficaria muito subjetivo, pois não há controle de que tipo de transação o cliente gostaria de realizar. Poderia ser desde uma consulta até uma transferência de recursos para outra conta ou pagamento de contas ou então aplicação em investimentos. Neste caso, há caracterizado a urgência em recuperar este serviço, pois efetivamente não é possível evidenciar o real impacto ou perda associada a esta falha.

Impacto

O impacto pode ser evidenciado durante o incidente ou depois de finalizado o mesmo. Evidenciar e sustentar um impacto ou perda depende de uma interação com a área de negócio envolvida, pois está associado à proposta do serviço envolvido. Por exemplo, uma área de negócio pode ter um impacto evidenciado após um mês de campanha ativa para venda de cartões de crédito no seguinte cenário:

Houve uma degradação no sistema de vendas para a operação de CallCenter, sendo caracterizado o Incidente como degradação na aplicação por uma falha de hardware prontamente resolvida com o apoio do processo de gestão de incidentes. Este tempo de resposta alto gerou atraso para determinados cliques durante o processo de venda de cartões na operação de CallCenter, sendo evidenciado perda no balanço mensal da campanha. Normalmente há uma estimativa de venda esperada e esta pode não ser atingida de acordo com a expectativa e, em uma investigação mais apurada, com o apoio do processo de gerenciamento de problemas, foi possível chegar à conclusão que a cada “clique” atrasado na operação gerou impacto no final da operação. Um operador efetivou, por exemplo, venda de 50 cartões durante um dia, mas que poderia ter vendido um volume próximo a 70 cartões neste mesmo período. Ou seja, o impacto foi evidenciado um mês depois que o incidente de IT ocorreu e foi solucionado.

Embora sejam três fatores que possuem definições e características distintas, estes têm forte dependência e relacionamento durante e depois de concluído o processo de gestão de incidentes de IT.

Ao caracterizar risco, urgência e impacto, outro fator importante é avaliar o nível de acordo de serviço contratado entre TI e a respectiva área de negocio. Estes níveis de acordo têm nomenclaturas distintas e podem ser utilizadas em conjunto ou separadas:

- ✓ PLA (*Performance Level Agreement*) – acordo de nível de serviços entre area de TI e área de negócio;;
- ✓ OLA (*Operational Level Agreement*) – acordo de nível de serviços entre áreas internas de TI para entregar um serviço para uma área de negócio;

As definições e parametrização para estes níveis de serviço são definidos em conjunto com as áreas de negocio e focais de TI. Estes documentos são utilizados como base para definição de severidade, criticidade, impacto e urgência durante e depois de finalizado um incidente de TI.

Pode ser considerado para uma instituição financeira para o seguinte exemplo:

Um serviço de CallCenter – atendimento à reclamações de cartão de crédito deve ter o seu OLA considerado de 24horas por 7 dias (7x24), entretanto seu PLA próximo à 100%. Normalmente o PLA é ajustado próximo deste valor (por exemplo 99,95%) considerando períodos de manutenção e ajustes ou alterações em ambiente de produção devidamente programados.

2.6 CONSIDERAÇÕES PARA SERVIÇOS DE TI - INSTITUIÇÃO FINANCEIRA

Considerando a interatividade e complexidade dos sistemas de TI para uma instituição financeira, vale citar alguns pontos de atenção com relação aos diversos processos que interagem, bem como a preocupação com cada sistema considerando a disponibilidade e qualidade oferecida para a área de negócio e

consequentemente para o cliente final.

Alguns critérios para avaliação da qualidade foram descritos por Parasuraman et al. (1985), que identificou um modelo conceitual para esta avaliação. Dentre seus estudos, foram comentados produtos como banco de varejo, cartão de crédito, corretoras de seguros e outros. Foram relacionados abaixo alguns dos contemplados e com o foco deste estudo:

- ✓ Confiabilidade - habilidade da instituição em entregar o serviço acordado com exatidão, confiança e entregue no prazo;
- ✓ Receptividade – disponibilidade dos colaboradores para prover o serviço – pronto atendimento;
- ✓ Credibilidade – Honestidade e seriedade, sendo importante a marca da instituição;
- ✓ Conhecimento do cliente – entendimento para as necessidades do cliente;
- ✓ Competência – habilidade e conhecimento associados para entrega do serviço;
- ✓ Comunicação – cliente informado de maneira clara, obrjetiva e com canal aberto – diretamente conectado ao cliente;
- ✓ Segurança - refere-se à ausência de riscos ou dúvidas para os serviços que a instituição atende e entrega;

Neste contexto e através destes critérios, a conclusão dos autores é que a qualidade do serviço percebida pelo consumidor é formada pela comparação entre as expectativas do serviço e o resultado percebido do serviço fornecido baseados e classificados nos critérios acima demonstrados, entre outros.

Disponibilidade

Serviços bancários estão cada vez mais inseridos em nosso dia a dia e da mesma forma estão sujeitos a alterações conforme a evolução e complexidade tecnológica apresentada no cenário atual. Um cuidado que deve ser observado é diferenciar disponibilidade de serviços de TI com alta disponibilidade de serviços para as áreas de negócio e consequentemente para clientes.

Trata-se de situações distintas e que podem gerar entendimento incorreto caso não estejam devidamente esclarecidas nos acordos de serviço.

Disponibilidade de serviços em TI pode contemplar situações de contingencia ou procedimentos para ativação de contingencia que podem não atender aos requisitos das áreas de negocio. De acordo com a característica de cada serviço atendido, deve haver níveis de acordo de serviços diferenciados visando atender às necessidades das áreas de negocio.

Considerando situações de contingencia, por exemplo, com data centers, departamentos, agências de atendimento, postos avançados de atendimento e ATMs são casos que exemplificam uma interrupção de serviços devido aos procedimentos de contingência e características dos serviços implantados, contudo devem estar em comum acordo com as áreas de negocio. Por exemplo, considerando uma agencia que esteja operando normalmente por um link de comunicação principal, no momento em que houver a transição para um link de contingencia devido a alguma falha, haverá uma interrupção momentânea para os procedimentos e transição para contingencia, mesmo que seja considerado como procedimentos automatizados.

Para uma avaliação mais detalhada, pode ser considerado um serviço de Internet Banking. Considerando uma falha no sistema de IT (aplicação, infraestrutura) que atende a aplicação bancária do Internet Banking e neste caso, não há justificativas da falha para o cliente, ou seja, independente se houve 5 minutos ou 5 horas de falha, houve a interrupção para o cliente. Considerando este cenário, deve haver uma preocupação acentuada com relação à recuperação rápida e efetiva deste tipo de serviço, pois independente da falha e de qualquer perda financeira ou operacional, há uma preocupação de reputação referente à marca e da mesma forma relacionado a órgãos regulatórios. E quando é mencionado a marca associada, está relacionada a confiabilidade e a história associada que no ramo financeiro tem um peso considerável.

Quando considerados sistemas de TI em uma instituição financeira, não pode ser desconsiderado o fator custo. Considera-se que o produto final de uma instituição financeira não é tecnologia da informação, entretanto tem relação e dependência direta com TI para sua existência. Não há operação de uma instituição financeira sem a TI, entretanto, há custos associados e devem ser mensurados adequadamente e principalmente justificados para as áreas de

negócio.

Considerando uma missão, visão e estratégia adotada pela instituição financeira, não podem ser desconsiderados pontos como, por exemplo:

- ✓ Estar conectado à globalização de sistemas e tecnologias;
- ✓ Estar aberto às novas necessidades do mercado e clientes;
- ✓ Estar disponível em qualquer tempo e lugar;

Embora sejam pontos subjetivos, não há como manter uma posição no mercado atual sem a devida preocupação com os pontos anteriormente citados. Contudo, o uso adequado de recursos e benefícios disponíveis da Tecnologia da Informação, considerando a convergência dos sistemas, produtos e da mesma forma, prevendo sistemas com alta disponibilidade e contingencia representam um grande desafio para os gestores de TI.

Qualidade

Um serviço de tecnologia da informação de qualidade no mundo financeiro significa estar disponível a qualquer momento, ser rápido, ágil e de fácil utilização do ponto de vista do cliente, sendo este interno ou externo.

O cliente interno requer a facilidade e rapidez para que as áreas de negocio e áreas de atendimento possam executar suas atividades otimizando processos e entregas.

O cliente externo mensura a qualidade de um serviço financeiro de acordo com o seu custo associado ao beneficio. Benefícios nestes casos podem significar desde valores de juros associados a produtos financeiros até o potencial tecnológico oferecido pela instituição, ou seja, produtos e serviços com preços que atendam às necessidades do cliente associados às características tecnológicas que o cliente espera.

Com estes cenários disponíveis, dinâmicos e principalmente, com maneiras distintas para identificar a qualidade de um serviço de IT no ramo financeiro, pode ser identificado a necessidade clara de otimizar recursos, processos, sistemas e principalmente, entregar um produto alinhado com a expectativa do cliente.

3 ESTUDO DE CASO

3.1 A EMPRESA

A instituição financeira considerada para este estudo de caso será nominada como **Banco GETIC**, por questões de confidencialidade.

O Banco GETIC atua globalmente no mercado financeiro e desde 1997, no mercado nacional. Desde então diversas atividades de restruturação foram implantadas envolvendo equipes da Tecnologia da Informação. Seus sistemas de tecnologia passaram por diversos processos de centralização e descentralização durante estes anos. Diversos produtos financeiros lançados, assim como muito deles foram extintos devido à característica do mercado financeiro nacional.

Conforme comentado, desde 1997, atua no mercado nacional e conta hoje com mais de 20.000 funcionários dentre os diversos sites administrativos, departamentos e agencias espalhados pelo Brasil.

Destes 20.000 funcionários, aproximadamente 3.000 são de times diretamente vinculados à tecnologia da informação.

Devido a características da marca, trata-se de uma instituição global e com fortes características desta globalização e padronização em seus produtos ofertados. Muitos destes permitem ao cliente realizar transações financeiras em diversos países, bem como, contar com o suporte e facilidades que, apenas quem atua em diversos países podem oferecer.

Características globais remetem responsabilidades extras para a instituição e para os colaboradores. Por tratar-se de uma marca global, está sujeita a diversos processos de controle, assim como, diversos órgãos regulatórios aos quais deve reportar-se.

Processos locais e globais interagem entre si através de padrões que podem ser definidos por um grupo específico ou por um fórum multidisciplinar designado para esta atividade. Processos e padrões locais requerem um esforço extra de colaboradores de TI, pois sistemas de TI devem interagir em perfeito sincronismo, exatidão e principalmente transparência aos olhos do cliente. Contudo, devem apresentar-se totalmente seguros garantindo a confidencialidade e segurança da informação necessária para o ramo financeiro.

Assim como sistemas globais de TI interagem entre si em perfeita sincronia, processos de gerenciamento de serviços de TI devem da mesma forma andam neste sincronismo.

O Banco GETIC, assim como as demais instituições financeiras, possui uma missão e visão estratégica bem definida e atualmente frisa alguns pontos essenciais que interagem entre si, ou seja, estar conectado ao seu cliente onde quer que esteja, estar aberto aos avanços tecnológicos a alterações do mercado financeiro, atuando com dinamismo e precisão, bem como estar disponível em todo o lugar e a qualquer momento. Ser um banco global com atendimento local e da mesma forma oferecer vantagens globais em todos os locais.

3.2 ESTUDO DE CASO

O estudo de caso foi baseado na avaliação dos incidentes de tecnologia registrados entre os anos de 2012 e 2013. Considerando que a instituição possui um grande leque de serviços de TI, foram retirados da base para pesquisa, apenas alguns dos serviços considerados como essenciais para a instituição financeira como:

- ✓ *Personal Internet Banking* – incidentes que impactaram canais de atendimento para clientes Pessoa Fisica;
- ✓ *Business Internet Banking* – incidentes que impactaram canais de atendimento para clientes Pessoa Jurídica;
- ✓ *Payments* – serviços e transações de pagamentos;
- ✓ *CallCenter Services* – incidentes que impactaram canais de atendimento via CallCenters para diversos serviços como: contratações, cancelamentos , reclamações, cobrança, etc;
- ✓ *Branches Application and Network* – incidentes que impactaram canais de atendimento em agências para clientes em geral – considerados incidentes em sistemas de tecnologia, ou seja, sem foco para incidentes de ordem natural ou devido a arrombamentos e afins;

O procedimento de pesquisa foi motivado pela necessidade de justificar a manutenção de uma área de gestão de incidentes de IT e principalmente justificar

a ampliação desta área perante a instituição.

3.3 ANÁLISE DOS DADOS

Dos incidentes registrados ao longo de 2012 e 2013 referente aos serviços listados no item anterior, foi possível identificar alguns pontos:

Em 2012 foram registrados 324 incidentes de tecnologia e dos serviços eleitos foram registrados um total de **97** incidentes. Em 2013 foram registrados 391 incidentes e destes, **129** incidentes foram dos serviços escolhidos. Pode ser observado um acréscimo de aproximadamente 21% na quantidade de incidentes registrados entre 2012 e 2013. Com relação aos serviços escolhidos, seguem considerações individuais:

- ✓ *Personal Internet Banking* – a quantidade de incidentes registrados entre os anos de 2012 e 2013 foram mantidos (**17** ao total por ano). Uma particularidade observada foi que embora a quantidade tenha sido mantida, os incidentes caracterizados em 2012 não se repetiram em 2013, ou seja, os 17 incidentes registrados em 2012 foram 100% resolvidos através dos processos de gerenciamento de incidentes e gerenciamento de problemas. Os incidentes registrados em 2013 tiveram como identificadas outras causas raízes comparadas à 2012.

- ✓ *Business Internet Banking* – a quantidade de incidentes registrados entre os anos de 2012 e 2013 aumentou em torno de 80%. Em 2012 foram registrados **10** incidentes e em 2013, foram registrados **18** incidentes afetando serviços de Business Internet Banking. Para estes casos, foi possível notar que 100% dos incidentes de 2012 foram totalmente solucionados devido à não repetição das mesmas causas em 2013, entretanto, os incidentes registrados em 2013 apresentaram, além do aumento na quantidade, uma diferenciação nos sintomas e características destes incidentes. Durante a pesquisa foi possível observar que muitos dos incidentes registrados

em 2013 não tiveram ainda suas causas raízes diagnosticadas – em torno de 50% - e seguem em avaliação pelos processos de gerenciamento de problemas. Este fato indica uma grande possibilidade de recorrências destes incidentes devido à não mitigação efetiva da causa raiz.

- ✓ *Payments* – com relação aos incidentes que impactaram os serviços de pagamentos foi possível observar uma manutenção na quantidade de incidentes registrados entre os anos de 2012 (**11**) e 2013 (**12**). Há uma particularidade referente à estes serviços que é o registro mínimo de mudanças, ou seja, sistemas que não sofreram alterações sistêmicas consideráveis entre 2012 e 2013. Outro fato relevante é que não houve recorrência de incidentes, ou seja, da mesma forma que para os serviços de Internet Banking, houve um trabalho efetivo entre as áreas de gerenciamento de incidente e gerenciamento de problemas neste ambiente.

- ✓ *CallCenter Services* – com relação aos incidentes registrados em 2012 (**37**), houve um aumento de praticamente 100% da sua quantidade em 2013 (**61**). Este resultado demonstrou certa preocupação durante a pesquisa e consequentemente, uma avaliação mais detalhada destes serviços. Para este caso específico, foi possível notar que houve uma alteração significativa nos processos e sistemas que atendem aos serviços de CallCenter. Houve alteração de tecnologia utilizada, alterando totalmente o fluxo de dependência e interfaces do sistema para o operador de callcenter. Identificado da mesma forma a alteração do prestador de serviço responsável pela manutenção e suporte da tecnologia implantada. Para este cenário foi possível notar que devido à necessidade de padronizar tecnologias associado à necessidade de substituição de fornecedor sem o tempo necessário para maturação do sistema no ambiente da instituição causou um aumento significativo em incidentes de tecnologia deste sistema.

- ✓ *Branches Application and Network* – para o caso de incidentes que afetaram ambiente de agencias, houve uma manutenção na quantidade de incidentes. Foram registrados **22** incidentes em 2012 contra **21** em 2013. Para este caso, foi possível notar outra característica de ofensores em incidentes de TI. Embora 100% dos incidentes tenham sido resolvidos em 2012, 50% dos incidentes registrados em 2013 foram caracterizados por alterações em regras negociais e não por alterações em sistemas de TI.

4 CONSIDERAÇÕES FINAIS

Com relação ao estudo realizado, podem ser observados pontos importantes que devem ser considerados ao implantar um processo de gestão de incidentes e gestão de problemas.

A relação entre quantidade de incidentes registradas e efetividade do processo de gestão de incidentes e problemas não pôde ser demonstrada neste estudo, pois houve um acréscimo na quantidade de incidentes mesmo com a manutenção do processo de incidentes. Contudo outros fatores devem ser considerados como conclusivos neste trabalho, como por exemplo:

- ✓ Interação direta entre os processos de gestão de incidentes e gestão de problemas como pôde ser observado em pelo menos 4 casos dos 5 citados acima.
- ✓ Alterações em sistemas e processos sem o controle devido são diretamente relacionados ao aumento de incidentes de Ti em seus sistemas.
- ✓ Sistemas que não possuem o devido conhecimento por suas áreas de suporte e manutenção oferece risco alto para a operação do ambiente em questão.

Outras conclusões puderam ser observadas durante o estudo, como por exemplo, sistemas que realizam muitas alterações em seus ambientes oferecem maior risco à operação, pois não há tempo suficiente de maturação e adaptação dos sistemas. Ambientes que estão sujeitos à suporte e manutenção de terceiros oferece da mesma forma um risco maior associado à sua operação, pois nem sempre há o mesmo engajamento e comprometimento esperado nestes atendimentos.

Efetivamente, foi possível observar a relação direta e importância em implantar e manter um processo de gestão de incidentes e problemas para uma instituição financeira, entretanto, estes processos não atuam sozinhos. Quando sistemas de TI oferecem uma interação complexa e de dimensões consideradas, obrigatoriamente há necessidade de interação de outros processos de

gerenciamento de serviços, como: gestão de testes, gestão de mudanças, gestão de conhecimento e de melhoria continua de serviços.

Considerando o foco para a instituição financeira, foi possível observar que embora muitos dos números apresentados sejam de caráter subjetivo, houve um crescimento considerável na aceitação e respeito pelos processos de gestão de incidentes e problemas. Durante as pesquisas foi possível notar a unanimidade de opiniões favoráveis ao processo de gestão de incidentes, considerando essencial para a operação do Banco GETIC. Conceitos como a convergência dos serviços de TI considerando a globalização dos serviços do Banco GETIC, foi possível notar que, embora sejam complexos os ambientes de tecnologia, a interação do processo de gestão de incidentes pode apoiar efetivamente quebrando as barreiras existentes entre áreas de suporte, aplicação e usuária, sejam estas locais ou globais, visando a atuação local com a devida visão global.

REFERÊNCIAS

ITIL – OGC – Service Operation, acesso em Novembro de 2014 e disponível em http://www.yessoft.ru/ITIL/04%20ITIL3%20Service%20Operation.pdf

Project Management & Software Engineering – ITIL, acesso em Novembro de 2014 e disponível em http://pmsware.wordpress.com/2013/04/15/21/

Incident Management: Human factors and minimising mean time to restore service http://dlibrary.acu.edu.au/digitaltheses/public/adt-acuvp272.01032011/index.html - O`Callaghan, Katherine Mary

Parasuraman, A.; Zeithaml, V. A.; Berry, L. A conceptual model of service quality and its implications for future research. Journal of Marketing, v. 49 (fall), p. 41-50, 1985. Disponível em http://www.scielo.br/scielo.php?script=sci_nlinks&ref=000175&pid=S0103-65132006000200012000021&lng=en

ITSM na Pratica, acesso em Novembro de 2014 e disponível em http://www.itsmnapratica.com.br/a-eterna-e-incendiaria-briga-entre-a-gestao-de-incidentes-e-de-problemas/

Tecnologia e Gestão, acesso em Novembro de 2014 e disponível em https://tecnologiaegestao.wordpress.com/tag/itil-v3/

Governança de TI, acesso em Novembro de 2014 e disponível em http://www.governancadeti.com/2010/09/itil-gerenciamento-de-incidentes-x-gerenciamento-de-problemas/

Gestão em Tecnologia, acesso em Novembro de 2014 e disponível em http://www.itsmnapratica.com.br/a-eterna-e-incendiaria-briga-entre-a-gestao-de-incidentes-e-de-problemas/