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

MARCIO ROMEU ARAUJO DE SOUSA

ANALISE DO PROCESSO DE GESTÃO DE INCIDENTES ALINHADO ÀS RECOMENDAÇÕES DE MELHORES PRÁTICAS DO ITIL - ESTUDO DE CASO DE UMA INSTITUIÇÃO PÚBLICA BANCÁRIA.

Brasília
2016

MARCIO ROMEU ARAUJO DE SOUSA

ANALISE DO PROCESSO DE GESTÃO DE INCIDENTES ALINHADO ÀS RECOMENDAÇÕES DE MELHORES PRÁTICAS DO ITIL - ESTUDO DE CASO DE UMA INSTITUIÇÃO PÚBLICA BANCÁRIA.

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 Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Mauricio Lyra.

Brasília
2016

MARCIO ROMEU ARAUJO DE SOUSA

ANALISE DO PROCESSO DE GESTÃO DE INCIDENTES ALINHADO ÀS RECOMENDAÇÕES DE MELHORES PRÁTICAS DO ITIL - ESTUDO DE CASO DE UMA INSTITUIÇÃO PÚBLICA BANCÁRIA.

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 Governança de Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra.

Brasília, 17 de Outubro de 2016.

Banca Examinadora

_____

Prof. Dr. Nome completo

_____

Prof. Dr. Nome completo

Dedico este trabalho à minha família, amigos e colegas de trabalho que me apoiaram incondicionalmente e me compreenderam em mais uma etapa da minha vida.

AGRADECIMENTOS

Primeiramente, agradeço à Deus por sempre ter me direcionado e consolado nos momentos mais difíceis, possibilitando a finalização desse trabalho mesmo com todos os obstáculos.

Ao meu Orientador Prof. Dr. Maurício Lyra que compreendeu minhas dificuldades e apoiou em todos os momentos, possibilitando-me assim um grande aprendizado.

Aos meus pais e minha irmã que sempre estiveram lá me motivando e incentivando, compreendendo assim todas minhas ausências e momentos roubados do nosso convívio, assim como desentendimentos, para realização desse projeto.

Aos meus amigos que me ajudaram e incentivaram para o alcance de mais essa etapa na minha vida, a qual possibilitará novos horizontes.

Aos meus colegas e amigos Jaqueline Mercier, Rubia Scrocaro, Sara Vieira e Higo Bandeira, que tanto me ajudaram, apoiaram e incentivaram na finalização deste trabalho.

E finalmente, a todos que me ajudaram e apoiaram de alguma forma a seguir com esse trabalho o qual me possibilitou um vasto conhecimento, não somente na área cientifica, como para vida, me ajudando assim a construir um mundo com qualidade e ética.

“Você pode encarar um erro como uma besteira a ser esquecida, ou como um resultado que aponta uma nova direção."

Steve Jobs

RESUMO

Este trabalho de conclusão de curso foi desenvolvido com o objetivo de avaliar a aderência do processo Gerenciamento de Incidentes de uma Instituição Pública Bancária alinhado às recomendações do ITIL. Teve como escopo o estudo de uma das melhores práticas reconhecidas internacionalmente em Governança de TI, a *Information Technology Infrasctructure Library* (ITIL) e a avaliação do processo de Gerenciamento de Incidentes atualmente implantado em uma Instituição Pública Bancária quanto à aderência. O trabalho utilizou o método estudo de caso único, onde foram realizadas pesquisas bibliográficas e documentais. Obteve-se como resultado a análise da aderência nas recomendações de melhores práticas pelo *framework* ITIL. Os resultados obtidos com o estudo mostraram que o processo de Gerenciamento de Incidentes possuía lacunas que podem ser reformuladas pelas recomendações do ITIL e que serão necessárias readequações; assegurando assim que a infraestrutura e os serviços de TI atendam aos requisitos do negócio da Instituição.

Palavras-chave: Governança de TI. ITIL. Gerenciamento de Incidentes.

ABSTRACT

This paper concluded the course was developed with the aim to evaluate the adherence to Incident Management process from a bank aligned to ITIL recommendations. Was to study the scope of an internationally recognized best practices in IT Governance, Information Technology Infrasctructure Library (ITIL) and evaluation of the Incident Management process currently deployed in a bank for adhesion . The study used a single case study method, which bibliographic and documentary surveys were conducted. Obtained as a result of the analysis of the adherence of the Incident Management process in use at the bank aligned to best practice recommendations advocated by ITIL framework. The results obtained from the study showed that the process of change management had deficiencies relating to compliance with the recommendations of ITIL and adjustment will be required to process maturity; ensuring that the infrastructure and IT services are aligned with business requirements.

Key words: IT Governance. ITIL. Incident Management.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

BABOK	*The Guide to the Business Analysis Body of Knowledge*
BIS	*Bank for International Settlements* ou Banco de Compensações Internacionais
BPM CBOK	*Business Process Management Body of Knowledge*
BSC	*Balanced Scorecard*
CCTA	*Central Computer and Telecommunications Agency* ou Agência Central de Computadores e Telecomunicações
CIO	*Chief Information Officer*
CMMI	*Capability Maturity Model Integration*
COBIT	*Control Objectives for Information and Related Technology*
eSCM-SP	*Service Provider Capability Maturity Model*
GTI	Governança de TI
IC	Item de Configuração
IEC	*International Engineering Consortium*
ISO	*International Standartization Organization*
IT	*Information Technology*
ITIL	*Information Technology Infraestructure Library*
LCR	*Liquidity Coverage Ratio* ou Índice de Liquidez de Curto Prazo
MPS.br	Melhoria de Processos do Software Brasileiro
NSFR	*Net Stable Funding Ratio* ou Índice de Liquidez de Longo Prazo
OGC	*Office of Government Commerce* ou Câmara de Comércio do Governo
OPM3	*Organizational Project Management Maturity Model*
PDCA	*PLAN - DO - CHECK - ACT* ou Planejar - Executar - Verificar - Agir
PMBOK	*Project Management Body of Knowledge*
PRINCE2	*Project in controlled environment*
Risk IT	*Enterprise Risk: Identify, Govern and Manage IT Risks*
SAS 70	*Statement on Auditing Standards for services organizations*
SGC	Sistema de Gerenciamento de Configuração
SOX	*Sarbanes-Oxley Act*
TI	Tecnologia da Informação
TOGAF	*The Open Group Architecture Framework*
Val IT	*Enterprise Value: Governance of IT Investments*

SUMÁRIO

INTRODUÇÃO

Contextualização

Mais do que nunca a TI deve estar alinhada às áreas de negócio de forma a contribuir no alcance dos objetivos estratégicos das empresas. A tecnologia deve ajudar na continuidade do negócio, eliminando as barreiras que impossibilitam as operações ou mesmo afetem os negócios da corporação. Melo (2008) afirma que a TI vem impactando os negócios de uma maneira jamais vista e está, cada vez mais, no domínio do negócio. Assim, a TI está adquirindo uma função de agente de desenvolvimento e de definição de estratégias em diferentes níveis (corporativo, de negócio e até mesmo funcional). Para atender a essas necessidades, o modelo de sistemas de informação das organizações contemporâneas deve ser o mais abrangente e completo possível.

Todos estão sujeitos a barreiras como interrupções frequentes e inesperadas nos serviços de TI. A ITIL (2011) define incidente como “uma interrupção inesperada de um Serviço de TI ou diminuição da sua qualidade”. Nesse mercado de trabalho de muita competitividade, as organizações que estiverem mais preparadas com flexibilidade e agilidade na resolução de incidentes se destacarão.

A ocorrência de paradas e falhas nos ambientes de operações de TI das empresas é algo que acontece com certa frequência e de forma inesperada. As organizações normalmente já possuem algum processo de gerenciamento de incidentes, formalizado ou não, para resolução desses problemas. Todavia, a recorrência desses incidentes e a não formalização desse processo é algo que pode acarretar prejuízos às empresas, mostrando o quanto o gerenciamento de incidentes se não aplicado de forma a seguir as melhores práticas aprovadas, pode ser falho e afetar assim a imagem da empresa.

Este estudo de caso teve como alvo uma Instituição Pública Bancária, onde as operações de TI, sendo cruciais para realização das estratégias de negócio, são afetadas por incidentes graves e recorrentes ocasionando sérios impactos para o cliente. Dessa forma, verificaremos se processo de gerenciamento de incidentes aplicado na Instituição está em acordo com as recomendações das melhores práticas de mercado.

Problema da Pesquisa

Para imagem Instituição estudada, incidentes recorrentes tem um impacto bastante negativo, visto que, de acordo com o nível da ocorrência, o impacto pode chegar aos pontos de venda (agências) da Instituição Pública Bancária estudada, influenciando assim no atendimento aos clientes da empresa e, consequentemente, numa visão negativa da organização.

Nesse contexto, o Gerenciamento de Incidentes, processo pertencente à biblioteca de infraestrutura ITIL, entra como agente primordial para disponibilidade de serviços de uma empresa, tendo como principal objetivo garantir que todos os incidentes sejam resolvidos no menor tempo possível e os serviços sejam restaurados à sua normalidade, sempre considerando os tempos acordados, com as prioridades pré-definidas e com o mínimo de impacto no negócio da empresa. Esse processo é de grande importância para uma organização, visto que ele visa reduzir o impacto de paradas nos serviços do negócio, garantindo assim a disponibilidade.

Mesmo com todos os distintos procedimentos aplicados na Instituição Pública Bancária em questão, a recorrência de incidentes é comumente percebida e pontuada pelas salas de monitorações, devendo ser desprendido tempo e mão de obra para rápida resolução, não sendo devidamente tratados.

Haja vista o problema apresentado, entende-se necessária a revisão do processo de Gerenciamento de Incidentes atualmente implantado nesta Instituição Pública Bancária, alinhado às melhores práticas do ITIL, evitando assim a recorrência de problemas e diminuindo o impacto no negócio.

Justificativa

De acordo com uma Pesquisa Nacional de Segurança da Informação (DARYUS, 2014), apenas 36,36% das empresas entrevistadas possuem processo formal para gestão de incidentes de Segurança da Informação. Esse número revela a baixa adesão a um processo de gerenciamento de incidentes por parte das empresas (Governamentais, Industriais e de Serviços), principalmente àqueles incidentes que impactam na Segurança da Informação.

Este estudo de caso ajudará substancialmente no entendimento da aplicação eficaz das recomendações do Gerenciamento de Incidentes, processo pertencente à metodologia ITIL, e atenderá os questionamentos relativos à capacidade deste processo, quando implantado e seguido de acordo com as melhores práticas, influenciar na qualidade dos serviços oferecidos e satisfação do cliente, com consequentes benefícios para estratégia da organização.

Esse estudo contribuirá, para Instituição Pública Bancária, na compreensão de como metodologias e melhores práticas como o ITIL, possui função essencial na execução do plano estratégico da empresa, utilizando práticas de gestão e de operação adequadas apara atender aos objetivos de negócio. Já para o mundo acadêmico, essa pesquisa mostra que o gerenciamento de incidente bem aplicado e seguido de acordo as melhores práticas, diminui consideravelmente o número de incidentes tecnológicos, que trazem prejuízos para o negócio da Instituição. E para o pesquisador o interesse desperta a partir do quanto esse tipo de ocorrência acontece nos ambientes tecnológicos e não são devidamente tratadas, e da importância do uso de metodologias de melhores práticas nos processos para o alcance dos objetivos estratégicos de uma organização.

Objetivos de Pesquisa

O objetivo principal deste trabalho é avaliar a aderência do processo de gerenciamento de incidentes utilizado na Instituição Pública Bancária¸ ao descrito nas melhores práticas do ITIL, assim como apontar as diferenças identificadas e sugerir adequação ao processo da Instituição de acordo com o recomendado ITIL.

A partir do objetivo geral, foram levantados os seguintes objetivos específicos para esta pesquisa:

- Descrever a importância da Governança de TI;
- Descrever o modelo de melhores práticas ITIL com o processo de Gerenciamento de Incidentes;
- Apresentar o Estudo de Caso da Instituição Pública Bancária;
- Analisar e compor o cenário da Instituição Pública Bancária com o modelo de melhores práticas ITIL e a Governança de TI.

- Propor alterações no processo de Gerenciamento de Incidentes da Instituição Pública Bancária de acordo com as melhores práticas recomendadas do ITIL.

Metodologia

Para alcançar os objetivos acima e realização deste estudo de caso foram utilizados os conceitos de pesquisa bibliográfica e documental, de natureza qualitativa e descritiva. Em relação aos procedimentos técnicos, a pesquisa foi classificada como Bibliográfica, Documental e Estudo de Caso, de acordo com o especificado por Reis (2012, p.55) em relação à classificação:

> **Pesquisa bibliográfica:** é a mais simples técnica de pesquisa acadêmica. Explica um problema fundamentando-se apenas nas contribuições secundárias, ou seja, nas informações e dados extraídos de leitura corrente e de referências, de revistas impressas e virtuais, material audiovisual, entrevistas, documentos etc. que foram produzidos por outros autores e que versam sobre o tema selecionado para o estudo. Fornece os elementos teóricos para o item denominado referencial teórico.
>
> **Pesquisa documental:** é a técnica de pesquisa que objetiva investigar e explicar um problema a partir de informações, dados e fatos históricos relatados em documentos pessoais como cartas, diários, fotos, vídeos, ofícios, informativos e em documentos institucionais como relatórios de pesquisa que incluem dados estatísticos, gráficos e tabelas, boletins, periódicos, jornais.
>
> **Estudo de caso:** é a técnica de pesquisa com base empírica que consiste em selecionar um objeto de pesquisa, que pode ser um fato ou um fenômeno, um determinado caso estudado nos seus vários aspectos. Neste tipo de pesquisa o pesquisador e o participante representante da situação-problema cooperam mutuamente com o estudo.

Em relação aos objetivos, é uma pesquisa definida como Descritiva, já que descreve um objeto de estudo determinado, estabelece uma relação entre fenômenos e população (grupo social, usando dados para procurar descobrir a frequência com que os fatos acontecem no cenário pesquisado, técnica essa utilizada para desenvolver uma pesquisa bibliográfica documental.

Já em relação à análise das informações e dados, é uma pesquisa definida como Qualitativa, por interpretar e dar significados aos fenômenos analisados sem adotar métodos e técnicas estatísticas como base do processo de análise de um problema. Assim, a pesquisa desse estilo não tem seus resultados apresentados em números, unidades de medidas ou categorias homogêneas de um problem.

Estrutura do trabalho

Este estudo de caso foi elaborado de acordo com as etapas a seguir:

Na primeira etapa foi feita a pesquisa bibliográfica dos conceitos teóricos em artigos científicos, dissertações e teses, livros, *web-sites* e revistas cientificas entre os anos de 2001 a 2016. Essa pesquisa subsidia a construção a construção do trabalho, embasando o estudo de verificação dos processos utilizados na Instituição Pública Bancária frente às melhores práticas de Governança de TI e do processo Gerenciamento de Incidentes, dentro da biblioteca ITIL.

Na segunda etapa foram consolidados os conceitos pesquisados dos elementos teóricos que embasam o estudo de caso apresentado.

Já na terceira etapa, é iniciado o estudo de caso, com a apresentação da Instituição Pública Bancária estudada, assim como o processo de Gerenciamento de Incidentes executado na empresa, a partir de informações documentais como manuais, processos documentados e normativos.

Na quarta etapa foi feita a comparação entre o processo de Gerenciamento de Incidentes utilizado na Instituição Pública Bancária com as recomendações de melhores práticas do ITIL para verificação da aderência, apontando assim os gaps identificados no processo da organização. Essa comparação foi feita num quadro, listando cada elemento verificado da teoria com o processo da Instituição.

Na quinta etapa foram feitas propostas de adaptações no processo de Gerenciamento de Incidentes da empresa, a partir do resultado da comparação, em atendimento às recomendações de melhores práticas do ITIL.

Na sexta etapa foi apresentado o resultado da avaliação feita no estudo de caso, assim como pontos críticos e pontos a serem considerados para sugestão de alteração do processo da Instituição Pública Bancária.

Através desse estudo de caso pretende-se demonstrar a importância de se aderir às melhores práticas do ITIL na formulação de um processo de Gerenciamento de Incidentes, com o objetivo de minimizar os impactos de ocorrência na realização do negócio.

1 A GOVERNANÇA DE TI

1.1 Motivação para Governança de TI

A Governança de TI tem sua motivação em diversos fatores de acordo com Fernandes e Abreu (2012, p. 7), como ter a TI como prestadora de serviços, a possibilidade de uma maior integração tecnológica, a dependência do negócio na TI, a existência de marcos de regulação, e um dos principais fatores é propiciar uma maior transparência da administração de uma organização.

Destrinchando esses fatores, temos a possibilidade de uma maior integração tecnológica de processos através da TI, a qual percebe-se uma grande visibilidade no risco que a TI figura para continuidade do negócio, o qual, de certo, deve ser mitigado e contingenciado.

Fernandes e Abreu (2012, p. 10) também descrevem sobre a dependência do negócio em relação à TI: “quanto mais as operações diárias e as estratégias corporativas chaves dependem da TI, maior é o papel estratégico da TI para empresa. ”. Baseado nessa constatação, a TI poderá ter vários contextos dentro de uma organização de acordo com o impacto que ela terá nas operações chaves (presente) e nas estratégias chaves (futuro), funcionando como ou estratégica para o negócio, ou com conotação de uma Fábrica para o negócio, ou apenas executando tarefas de suporte ou exercendo um papel de mudança direcionando o futuro da organização.

Outra motivação bastante relevante para Governança de TI são os Marcos de Regulação (*compliance*) os quais apesar de representarem restrições ao negócio, devem ser implantados, visto que fornecem capacidade de atração de capital de risco, a um custo baixo e com geração de lucros (FERNANDES; ABREU, 2012). Ou seja, para TI, os sistemas que envolvem transações da empresa, como as contábeis e financeiras, devem seguir as seguintes regras:

- Estar disponível para consulta de relatórios com os resultados financeiros e contáveis;
- Armazenar dados e informações de forma adequada e com segurança;
- Disponibilizar trilhas e informações para auditoria e verificação de processos;

- Ter seus riscos mapeados e gerenciados.

Os principais marcos de regulação são:

1.1.1 Sarbanes-Oxley Act

Garante a fidedignidade dos relatórios financeiros e controles associados e responsabiliza conjuntamente diretores e o responsável pela área de finanças por atos lesivos aos acionistas e ao mercado. Teve como motivadores para sua criação os escândalos financeiros acontecidos em companhias abertas nos Estados Unidos, como a Enron e outras, que fizeram com que os investidores perdessem a confiança no mercado de capital americano.

Fernandes e Abreu (2012, p. 28) definem os objetivos principais da Sarbanes-Oxley como “proteger os investidores do mercado de capitais americano de fraudes contábeis e financeiras de companhias abertas, assim como instituir uma série de penalidades contra crimes relacionados, tendo foco nos ‘controles internos sobre relatórios financeiros’”.

1.1.2 Acordo da Basileia II

O Acordo da Basileia II estipula requisitos de capital mínimo para as instituições financeiras, em função dos seus riscos de crédito e operacionais. Esses requisitos são necessários devido o “risco operacional” de TI dos bancos ser uma questão prioritária pelo avanço em tecnologias, variedade de canais e produtos. (FERNANDES; ABREU, 2012).

Esse marco de regulação engloba todos os processos de TI e suas respectivas áreas organizacionais, tendo impacto diretamente nos seguintes pontos:

- Capacidade de armazenamento de dados granulados dos clientes com objetivo de avaliar riscos.
- Integridade das informações das transações do banco.
- Integridade das informações armazenadas sobre os clientes e operações de crédito.

- Segurança dessas informações.
- Contingências na operação.
- Planejamento de capacidade.
- Planejamento de desastre e recuperação.
- Integridade do processo de emissão de relatórios requeridos pelo BIS (*Bank for International Setlements).*

1.1.3 Acordo da Basileia III

Após a eclosão da crise em 2008, pôs-se em cheque a até então prevalecente Basiléia II. Com a fragilidade demonstrada pelas instituições financeiras o modelo regulatório adotado até o momento passou a não ser suficiente para prevenir crises de grandes proporções. E a partir da crise foi percebido que a regulação financeira não pode ser focada no individuo, e sim no sistema como um todo, reconhecendo-o maior que a soma de suas partes (Viñals 2010).

A partir de um acordo entre os países do G20 (grupo das 20 maiores economias) em Novembro de 2010 chegaram a uma conclusão sobre a reforma do sistema bancário e das suas maiores instituições de créditos, causadoras da crise financeira de 2008. Esse acordo é o Acordo de Basiléia III, considerado mais um complemento do que uma ruptura com o fracasso do modelo de regulação anteriores, e formado pelos documentos: “Basel III: *A global regulatory framework for more resilient bank sand banking system*” (Basel Committe Banking Supervision 2010a) e “Basel III: *International framework for liquidity risk measurement, standards and monitoring*” (Basel Committe on Banking Supervision 2010b) (LEITE; REIS, 2013, p. 171).

O Acordo da Basiléia III tem como principais pontos o reforço dos requisitos de capital próprio das instituições de crédito; aumento considerável da qualidade desses fundos próprios; redução do risco sistêmico e um período de transição que seja suficiente para acomodar essas exigências. E, segundo o comitê, seus principais objetivos são:

- Aumentar a qualidade do capital disponível de modo a assegurar que os bancos lidem melhor com as perdas;
- Aumentar os requerimentos mínimos de capital, incluindo um aumento no capital principal de 2% para 4,5%;
- Criar um colchão de conservação de capital e de um colchão anticíclico de capital, ambos em 2,5% cada;
- Diversificar a cobertura do risco, incorporando as atividades de trading, securitizações, exposições fora do balanço e derivativos;
- Introduzir uma taxa de alavancagem para o sistema e medidas sobre requerimentos mínimos de liquidez, tanto para o curto quanto (LCR) para o longo prazo (NSFR);
- Aumentar a importância dos pilares II e III do acordo anterior no processo de supervisão e de transparência. Para isso, o comitê propõe práticas para a gestão de liquidez, realização dos testes de estresse, governança corporativa e práticas de avaliação de ativos. Ainda, há a preocupação com a gestão e concentração de risco além da promoção de incentivos para que os bancos tenham uma melhor administração do risco e retorno orientados para o longo prazo.

Leite e Reis (2013) parafraseiam Wellink (2010): “com a introdução de tais medidas, espera-se que seja possível se obter um sistema bancário mais forte e estável, além de diminuir a alocação ineficiente de recursos que acontece em períodos de excessivo crescimento de crédito”.

1.2 Conceituando a Governança de TI

O IT Governance Institute (2007) afirma que “a governança de TI é de responsabilidade da alta administração (incluindo diretores e executivos), na liderança, nas estruturas organizacionais e nos processos que garantem que a TI da empresa sustente e estenda as estratégias e objetivos da organização”.

De acordo com Weil e Ross (2006), o conceito de Governança de TI existe nos negócios há muito tempo, porém, o interesse e a preocupação generalizados a

seu respeito são bastantes recentes (...). Eles ainda afirmam que a boa governança de TI harmoniza decisões sobre a administração e utilização da TI com resultados esperados e objetivos do negócio.

A Governança de TI é uma parte integral da Governança Corporativa, e foi criada para nomear as práticas de gestão da TI desenvolvidas para garantir o alinhamento de TI às iniciativas de Governança Corporativa (FREITAS, 2013). Consiste em liderança, estrutura organizacional e processos que garantem que a TI Corporativa sustente e estenda os objetivos e estratégias corporativas (CAMPOS; SANTOS, 2011).

Uma outra abordagem da estratégia implantada nas organizações afirma que a Governança de TI é o elemento que permite que a organização possa formular e controlar estratégia de TI e dar direção apropriada com o propósito de alcançar a vantagem competitiva para a corporação, estando focada na integração entre o negócio e a TI (VAN GREMBERGEN, 2000; VAN GREMBERGEN; DE HAES; GULDENTOPS, 2004; IBGC, 2005).

Aragon e Abreu (2012) afirmam que a Governança de TI, como disciplina, busca o direcionamento da TI para atender ao negócio e o monitoramento para verificar a conformidade com o direcionamento tomado pela administração da organização. A Governança de TI deve promover o alinhamento da TI ao negócio (suas estratégias e objetivos), promover a implantação de mecanismos que garantam a continuidade do negócio contra interrupções e falhas (manter e gerir as aplicações e infraestrutura de serviços) e promover, em parceria com as áreas de controle interno, compliance e gestão de riscos, o alinhamento da TI a marcos de regulação extremos como a Sarbanes-Oxley, Basileia II e outras normas.

E com a análise de diversas definições, Fernandes e Abreu (2006) concluem que a Governança de TI almeja compartilhar as decisões de TI com os outros dirigentes da organização, estabelecendo as regras, enquanto esta última estabelece os processos que direcionarão o uso da tecnologia da informação pelos usuários, negócios da organização, departamentos e divisões, fornecedores e clientes.

1.3 Objetivo da Governança de TI

De acordo com Aragon e Abreu (2012), o principal objetivo da Governança de TI é alinhar a TI aos requisitos do negócio, considerando soluções de apoio ao negócio, assim como a garantia da continuidade dos serviços e a minimização da exposição do negócio aos riscos de TI. A seguir, são listados alguns sub-objetivos (ARAGON; ABREU, 2012):

- Promover o posicionamento mais claro e consistente da TI em relação às demais áreas de negócio da empresa. Significa que a TI deve entender as estratégias do negócio e traduzi-las em planos para sistemas, aplicações, soluções, estruturas organizacionais, processos e infraestrutura, desenvolvimento de competências, estratégias de *sourcing* e de segurança da informação.
- Promover o alinhamento e a priorização das iniciativas de TI com as estratégias de negócio: isto significa que o que foi planejado para acontecer deve ser priorizado, visando as prioridades do negócio e as restrições de capital de investimento.
- Promover o alinhamento da arquitetura de TI, sua infraestrutura e aplicações às necessidades de negócio, em termos de presente e futuro: implantar os projetos e serviços planejados e priorizados.
- E promover a implantação de melhoria dos processos operacionais e de gestão necessários para atender aos serviços de TI, conforme padrões que atendam às necessidades do negócio.

Pode-se concluir que a Governança de TI tem dois grandes objetivos: a entrega de valor, aparada no alinhamento dos negócios e da TI, e a mitigação de riscos, direcionada pela atribuição de responsabilidades na organização (INFORMATION TECHNOLOGY, 2003b).

1.4 Fundamentos da Governança de TI

O tema Governança Corporativa veio a surgir nas organizações no final da década de 80, se intensificando nos anos 90 a partir dos escândalos financeiros conhecidos mundialmente. Esses escândalos protagonizados por grandes corporações norte-americana de capital aberto (como a companhia de energia Eron Creditors Recovery Corporation, a WorldCom, a Tyco Internacional Ltd.) motivaram o surgimento da lei Sarbanes-Oxley Act (SOX), que teve novas regras elaboradas em 2002 nos Estados Unidos, patrocinadas pelos congressistas Paul Sarbanes e Michel G.Oxley (SOUSA; FRAGA, 2004; FERNANDES; ABREU, 2006; WEILL; ROSS, 2004).

A lei SOX veio com o objetivo de recuperar a confiança dos investidores nos relatórios financeiros das organizações, institucionalizando assim a estrutura de Governança. Tinha como premissa eliminar irregularidades contábeis e a manipulação dos preços das ações das empresas, impondo regras e penalidades rígidas aos executivos, alinhando seu comportamento com os interesses dos acionistas. As responsabilidades principais dos executivos, impostas por essas leis, fizeram com que a Governança Corporativa se tornasse fonte de vantagem competitiva (WEILL; WOODHAM, 2002; MAYER, 2004).

O IBCG (2012) define Governança Corporativa como:

> [...] o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselhos de administração, diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para sua longevidade.

Após entenderem que a continuidade dos negócios das organizações engloba aspectos como confidencialidade, integridade e disponibilidade de informações, regras e normas especificas também foram impostas para o comportamento esperado dos departamentos de TI, dando responsabilidades diretas aos executivos de TI quando há exposição a riscos, malversação ou fraudes nos sistemas de informação.

Sendo assim a governança corporativa e a de TI tem um papel fundamental para continuidade do negócio, e, de acordo com Jaeger-Neto e Colaboradores (2009), elas podem influenciar significativamente no desempenho da organização, através da

geração de valor para o negócio e da gestão equilibrada do risco com o retorno do investimento.

1.5 A importância e benefícios da Governança de TI

De acordo com Weill e Ross (2006) a implementação de uma Governança de TI eficiente para sustentar estratégias é a causa de parte do sucesso de muitas empresas que se destacam pelo seu desempenho. Para eles, o alcance de resultados superiores depende necessariamente da definição de um sistema de direitos decisórios para garantir o uso e gestão apropriada da TI, definindo assim quem deve tomar as decisões e como elas devem ser tomadas e monitoradas.

Já Mendonça et al. (2013) complementa que “o bom desempenho da governança de TI traz bons resultados para organização”. Segundo Bowen e colaboradores (2007 apud MENDONÇA et al., 2013, p. 450), “a gestão de recursos de TI ajuda na obtenção de sucesso da organização e uma governança de TI eficaz gera benefícios verdadeiros para a organização, tais como: credibilidade, referência em produtos, na prestação de serviços e diminuição dos custos”. Dessa forma percebemos que a governança de TI se mostra como um mecanismo capaz de permitir o alinhamento entre as estratégias de negócio e da TI, além de fornecer um maior profissionalismo aos processos decisórios da TI.

A crescente dependência das empresas em relação à informação e a TI suscita a necessidade da implantação de uma Governança de TI. Uma boa GTI harmoniza decisões sobre a administração e a utilização de TI com os comportamentos e objetivos do negócio e, sem essas estruturas de governança cuidadosamente projetadas e implantadas, as empresas deixam essa harmonia ao acaso.

Outro ponto bastante comentado a respeito do benefício da GTI é a entrega de valor da TI produzida pela adoção desse mecanismo. Segundo Weill e Ross (2006) o valor da TI depende mais do que apenas uma boa tecnologia, e a GTI é fundamental para o aprendizado organizacional sobre esse valor. Essa entrega de valor decorre do alinhamento entre a TI e o negócio, pois ambos precisam ter clareza sobre o objetivo a ser atingido; dessa forma, o grau em que a TI entrega valor é uma

função do alinhamento entre a organização de TI para o atendimento das expectativas do negócio (INFORMATION TECHNOLOGY..., 2003b; GREMBERGEN *et al.,* 2004).

Weill e Ross (2006) concluem que uma Governança de TI eficaz é o indicador mais importante do valor que a organização aufere com a Tecnologia da Informação. Sendo essencial para garantir melhorias eficazes e eficientes nos processos das empresas, a GTI fornece uma estrutura que liga os processos de TI, os recursos de TI e as informações às estratégias e objetivos da empresa. Além disso, implantar uma Governança de TI é também garantir que as informações da empresa e a tecnologia aplicada suportam os objetivos do negócio, podendo a empresa tirar todo proveito dessas informações, maximizando os benefícios, capitalizando em oportunidades e adquirindo vantagem competitiva (ALVES; RANZI, 2006).

1.6 Boas práticas de Mercado (Modelos)

Segundo Weiss e Bernardes (2014, p. 103), "introduzir práticas de governança de TI significa promover mudança no *modus operandi* da organização". As boas práticas de governança convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade (IBGC, 2009).

Para atender as necessidades de governança de TI, modelos, metodologias, padrões e ferramentas vem sendo consolidados em framework de melhores práticas do mercado. Essas iniciativas favorecem a integração da TI com as demais funções organizacionais e tornam seus processos de trabalho mais transparentes, inteligíveis, controláveis e confiáveis.

Fernandes e Abreu (2012, p. 202) relacionam os principais modelos de melhores práticas que auxiliam a implantação da Governança de TI no quadro abaixo:

Quadro 1 - Principais Modelos de Melhores Práticas

Modelo de melhores práticas	Escopo do modelo
COBIT – ***Control Objectives for Information and related Technology***	Modelo abrangente aplicável para a auditoria e o controle de processos de TI, desde o planejamento da tecnologia até a monitoração e auditoria de todos os processos.
Val IT – ***Enterprise Value: Governance of IT Investments***	Modelo que trata da governança dos investimentos de TI e gerenciamento do portfólio desses investimentos.

Risk IT – ***Enterprise Risk: Identify, Govern and Manage IT Risks***	Modelo que trata do gerenciamento dos riscos de TI.
ISO 31000	Trata dos princípios e guias para o gerenciamento de riscos.
CMMI – ***Capability Maturity Model Integration***	Desenvolvimento de produtos e projetos de sistemas e software.
MPS.br	Modelo brasileiro para a melhoria do processo de software.
ITIL – ***Information Technology Infrastructure Library***	Serviços de TI, segurança da informação, gerenciamento da infraestrutura, gestão de ativos e aplicativos, etc.
ISO/IEC 20000	Norma abordando requisitos e melhores práticas para o gerenciamento de serviços de TI.
ISO/IEC 27001 e ISO/IEC 27002	Requisitos e código de prática para a gestão da segurança da informação.
Modelos ISO – ***International Organization for Standardisation***	Sistemas da qualidade, ciclo de vida de software, teste de software, etc.
eSCM-SP – ***Service Provider Capability Maturity Model***	Outsourcing em serviços que usam TI de forma intensiva.
PRINCE2 – ***Project in controlled environment***	Metodologia de gerenciamento de projetos.
PMBOK – ***Project Management Body of Knowledge***	Base de conhecimento em gestão de projetos.
OPM3	Modelo de maturidade para o gerenciamento de projetos.
SCRUM	Método ágil para o gerenciamento de projetos.
BSC – ***Balanced Scorecard***	Metodologia de planejamento e gestão da estratégia.
Seis Sigma	Metodologia para melhoria da qualidade de processos.
SAS 70 – ***Statement on Auditing Standards for services organizations***	Regras de auditoria para empresas de serviços.
TOGAF – ***The Open Group Architecture Framework***	Modelo que trata o desenvolvimento e a evolução de arquiteturas de TI.
BPM CBOK – ***Business Process Management Body of Knowledge***	Corpo de conhecimento para o gerenciamento de processos de negócio.
BABOK – ***The Guide to the Business Analysis Body of Knowledge***	Guia de conhecimento para a prática de análise de negócio.

Fonte: Fernandes e Abreu (2012)

Dados os modelos no quadro acima, para este trabalho foi escolhido, como base, a biblioteca ITIL. Como um *framework,* o principal objetivo do ITIL é prover um conjunto de práticas de gerenciamento de serviços de TI testadas e comprovadas no mercado, que podem servir como balizadoras para organizações que já possuem suas operações de TI em curso e pretendem otimizá-las ou para a implementação de novas operações (Fernandes e Abreu, 2012).

2 O ITIL – INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

Segundo o ITIL V3, um serviço é um “meio de entregar valor aos clientes, facilitando o alcance dos resultados que os clientes desejam, tirando deles a propriedade dos custos e riscos específicos”. Já o Gerenciamento de Serviços é definido pelo ITIL como “um conjunto de capacitações organizacionais especializadas para fornecer valor aos clientes na forma de serviços, transformando recursos em serviços valiosos”. Essas capacitações são os processos e as funções utilizados para gerenciar os serviços ao longo do seu ciclo de vida. E neste cenário, o ITIL é um dos modelos mais utilizados em todo o mundo como base para a implementação de boas práticas de Gerenciamento de Serviços de TI, sendo por esse motivo a escolha como *framework* referência desse trabalho.

2.1 O que é o ITIL

O ITIL - acrônimo de *Information Technology Infrastructure Library*, é um framework de processos de gestão de TI criado pela CCTA (*Central Communications and Telecommunications Agency*), atual OGC (*Office of Government Commerce*) do governo inglês, composto de práticas, coerentes e integradas, de gerenciamento de serviços de TI (OGC, 2007).

Freitas (2013, p. 61) descreve uma dúvida bastante comum a respeito do ITIL sobre o gênero que deve preceder a palavra ITIL:

> O conceito de “biblioteca” para denominar um conjunto de livros, no Brasil, é mais utilizado quando queremos nos referir ao local onde são armazenados os livros. Não costumamos chamar de biblioteca um conjunto de livros simplesmente. Eu particularmente classifico ITIL como “o” ITIL por estar me referindo a um “conjunto de livros”. Do contrário chamaremos de “a” ITIL por causa do termo “biblioteca”, mas quando nos referirmos a um livro específico chamaremos de “o” livro Estratégia de Serviço, por exemplo.

Por este motivo, e a título de padrão e preferencias, neste trabalho o termo ITIL será referenciado como masculino, exceto quando for utilizado um anglicismo para denominar a sigla, como por exemplo: o *framework* ITIL, a *best practice* ITIL, a biblioteca ITIL, etc.

Mansur (2007) conceitua a biblioteca ITIL como um conjunto de orientações descrevendo as melhores práticas para um processo integrado do gerenciamento de

e serviços de TI. Desenvolvido no final da década de 80 pelo CCTA (atual OGC), o ITIL compreende uma biblioteca de recomendações baseada em processos que apresenta um conjunto de melhores práticas capazes de promover a qualidade nos serviços computacionais no setor de TI.

Complementando, Magalhães e Pinheiro (2007) apresentam o ITIL como um conjunto de melhores práticas que vem ao encontro do novo estilo de vida imposto às áreas de TI, promovendo maturidade ao processo de gerenciamento de TI e propiciando a construção de valor para TI.

2.2 Benefícios na Implantação do ITIL

Segundo Fernandes e Abreu (2012) a adoção das práticas do ITIL pretende levar a organização a um grau de maturidade e qualidade que permita o uso eficaz e eficiente dos seus ativos estratégicos de TI, sempre com o foco no alinhamento e na integração com as necessidades dos clientes e usuários. “O ITIL V3, com sua abordagem de ciclo de vida, permite que se tenha uma visão do gerenciamento de serviços pela perspectiva do próprio serviço, em vez de focar em cada processo ou prática por vez”. Essa visão deixa claro a grande importância de um dos objetivos: mensurar e gerenciar o valor que os serviços de TI adicionam efetivamente ao negócio. (FERNANDES; ABREU, 2012, p. 257)

Gaspar, Gomez e Miranda (2010), que possuem a mesma abordagem que Fernandes e Abreu (2012), complementam com uma lista das principais razões para se adotar o ITIL, que são elas:

- Adotar práticas já usadas mundialmente;
- Retorno mais rápido sobre o projeto de implementação.
- Os processos serão mais eficientes e eficazes, com foco em rapidez e resultados positivos;
- Melhoria da qualidade dos serviços de TI;
- Alinhamento da TI com as necessidades do negócio;
- Aumento da satisfação do cliente;
- Obter a visão da capacidade atual;
- Manter equipe de TI focada e motivada.

O ITIL é um modelo de práticas com objetivos, entradas e saídas de processos e atividades que podem ser adotadas de acordo com a necessidade de cada organização, não sendo um modelo de regras engessadas a serem seguidas (OGC, 2000a).

Magalhães e Pinheiro (2007) afirmam que para alcançar os benefícios com a adoção das melhores práticas do ITIL, é necessário que organização tenha plena consciência de sua importância e esteja seriamente comprometida com sua implementação. A partir desse comprometimento em larga escala, os seguintes benefícios poderão ser alcançados com o gerenciamento de serviços e incidentes de TI:

- Melhoria na qualidade dos serviços de TI, tornando-os mais confiáveis para o suporte à execução da estratégia de negócio;
- Melhoria na satisfação dos clientes, pois a área de TI passa a conhecer e fornecer o que eles esperam;
- Melhoria da imagem da área de TI pelo incremento da qualidade dos serviços de Tecnologia da Informação, atraindo novos clientes e encorajando o aumento da demanda de serviços de TI por parte da clientela atual;
- Maior motivação dos integrantes da equipe de TI derivada da melhoria na satisfação no trabalho, obtida por um conhecimento melhor da capacidade disponível e mais elevada gestão das expectativas, tanto de TI quanto dos clientes e usuários;
- Diminuição nos prazos de atendimento de incidentes, solução de problemas e execução de mudanças, associadas ao aumento da taxa de sucesso em tais processos.

Observa-se então que um bom Gerenciamento de Incidentes, quando aplicado de forma robusta e engajada, pode ter efeitos direto na Governança de TI, na Estratégia da Organização e, por fim, na satisfação dos usuários e clientes dos serviços de TI da empresa.

2.3 A Estrutura do Modelo

Para Fernandes e Abreu (2012), o ITIL pode ser considerado uma fonte de boas práticas utilizadas pelas organizações para estabelecer e melhorar suas capacitações em gerenciamento de serviço, tendo um Núcleo composto por cinco publicações relacionadas a um estágio do ciclo de vida do serviço, com orientações para uma abordagem integrada de gerenciamento de serviços. Este núcleo (figura 1) e os livros do ITIL são apresentados logo a seguir.

Figura 1 - O Núcleo do ITIL

Fonte: Adaptado de OGC

A figura acima mostra o funcionamento macro do modelo com os módulos funcionando de maneira cíclica. Todo o processo é circundado pela Melhoria Contínua de Serviço, responsável por identificar e otimizar pontos de atenção no processo de gerenciamento de serviços de TI, agregando valor e qualidade aos serviços das organizações.

Fernandes e Abreu (2012) resume os cinco livros do ITIL da seguinte forma:

- **Estratégia do Serviço:** Orienta sobre como as políticas e processos de gerenciamento de serviço podem ser desenhadas, desenvolvidas e implementada como ativos estratégicos ao longo do ciclo de vida de serviço. Entre os tópicos abordados nesta publicação, estão os ativos de serviço, o catálogo de serviços, gerenciamento financeiro, gerenciamento do portfólio de serviços, desenvolvimento organizacional, riscos estratégicos etc.

- **Desenho do Serviço:** Fornece orientação para o desenho e desenvolvimento dos serviços e dos processos de gerenciamento de serviços, detalhando aspectos do gerenciamento do catálogo de serviços, do nível de serviço, da capacidade, da disponibilidade, da continuidade, da segurança da informação e dos fornecedores, além de mudanças e melhorias necessárias para manter ou agregar valor aos clientes ao longo do ciclo de vida de serviço.

- **Transição do Serviços:** Orienta sobre como efetivar a transição de serviços novos e modificados para operações implementadas, detalhando os processos de planejamento e suporte à transição, gerenciamento de mudanças, gerenciamento da configuração e dos ativos de serviço, gerenciamento da liberação e distribuição, teste e validação de serviço, avaliação e gerenciamento do conhecimento.

- **Operação do Serviço:** descreve a fase do ciclo de vida do gerenciamento de serviços que é responsável pelas atividades do dia a dia, orientando sobre como garantir a entrega e o suporte a serviços de forma eficiente e eficaz e detalhando os processos de gerenciamento de eventos, incidentes, problemas, acesso e de execução de requisições.

- **Melhoria Continua do Serviço:** Orienta, através de princípios, práticas e métodos de gerenciamento da qualidade, sobre como fazer sistematicamente melhorias incrementais e de larga escala na qualidade do serviço, nas metas de eficiência operacional, na continuidade do serviço etc., com base no modelo PDCA preconizado pela ISO/IEC 20000.

Para este trabalho, que tem seu objetivo principal baseado no processo Gerenciamento de Incidentes, somente serão abordadas os conceitos e funções deste processo em especifico, assim como detalhados, sucintamente, os outros processos

e funções considerados relevantes neste e em outros estágios do ciclo de vida do serviço. O ciclo de vida Operação de Serviço, descrito a seguir, é onde o Gerenciamento de Incidentes está inserido.

2.4 A Operação de Serviço

O ciclo Operação de Serviço contempla as atividades operacionais do dia a dia de TI que mantem os serviços tecnológicos em funcionamento com base nos níveis de serviços acordados. Para Freitas (2013), os objetivos desse ciclo são manter a satisfação e a confiança nos serviços de TI por parte dos usuários e minimizar o impacto na execução diária do negócio pela empresa, coordenando as atividades requeridas para entregar os serviços de TI nos níveis acordados pelos clientes e usuários.

Fernandes e Abreu (2012) alertam que o estágio da Operação do Serviço é bastante crítico dentro do ciclo de vida do serviço, pois erros na condução, no controle e na gestão das atividades operacionais do dia a dia poderão comprometer a disponibilidade do serviço, mesmo que ele tenha sido muito bem desenhado e que sua implementação em produção tenha sido um sucesso.

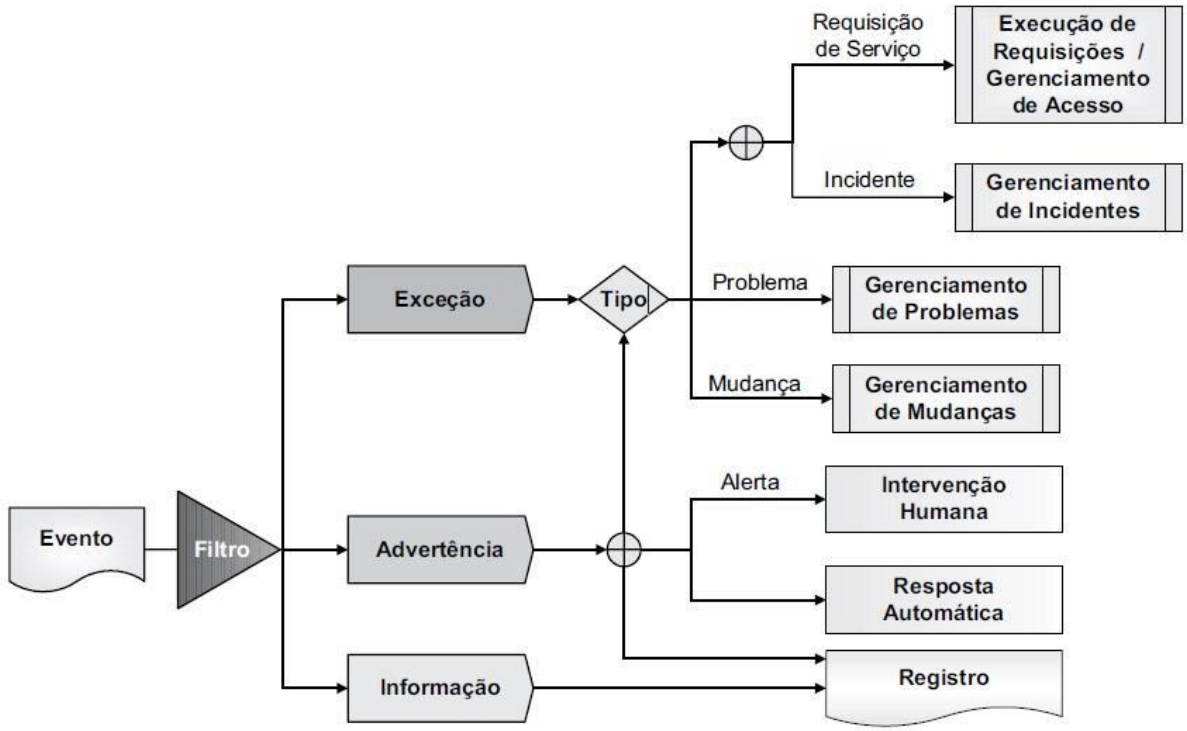
Os autores acima ainda afirmam que um dos maiores desafios deste estágio é seguir processos, funções e atividades que visam a regularidade da entrega dos serviços nos níveis preestabelecidos, num ambiente que sofre constantes mudanças de formas imprevisíveis. Dessa forma, a Operação do Serviço tem um importante papel de encontrar um ponto de equilíbrio entre conjuntos de prioridades conflitantes, minimizando assim os riscos.

As equipes desse estágio também enfrentam outro crucial desafio levantado pelos autores:

> As equipes de Operação do Serviço devem sempre estar conscientes de que são provedoras de serviços para o negócio e que uma das habilidades mais importantes a serem exercidas é a comunicação. O quanto antes a Operação de Serviço se envolver nas atividades de desenho e transição, menores serão os riscos de problemas inesperados durante a fase recorrente.
>
> (FERNANDES; ABREU, 2012, p. 277)

A figura 2 mostra o relacionamento entre os processos da Operação de Serviço:

Figura 2 - Processo Operação de Serviço



Fonte: Fernandes e Abreu (2012)

2.4.1 Os Processos e Funções da Operação de Serviço

Dentro do ciclo da Operação do Serviço existem cinco processos que sustentam o estágio:

- Gerenciamento de Eventos.
- Cumprimento de Requisição.
- Gerenciamento de Problemas.
- Gerenciamento de Acesso.
- Gerenciamento de Incidentes.

E quatro funções que permeiam a Operação do Serviço:

- Central de Serviços.
- Gerenciamento Técnico.
- Gerenciamento de Operações de TI.
- Gerenciamento de Aplicações.

A seguir será explanado cada processo e função de forma sucinta.

2.5 Gerenciamento de Eventos

De acordo com Freitas (2013), Evento é uma mudança de status significativa para o gerenciamento de um serviço de TI. É um alerta de notificação criado por qualquer serviço de TI, Item de Configuração ou ferramenta de monitoração, podendo demandar ações das equipes de Operações de TI e gerar um registro de incidente. Um evento pode indicar que algo não está de acordo com a operação normal do serviço ou descumprindo um nível de serviço acordado.

O Gerenciamento de Eventos tem como objetivos detectar eventos que façam sentido para o ciclo de vida do serviço, determinar a ação de controle adequada e coordenar o direcionamento dos eventos por outros processos e funções.

O autor também define que os eventos a serem monitorados são especificados e acordados na fase do Desenho de Serviço, durante os processos Gerenciamento de Disponibilidade, Gerenciamento da Capacidade e Gerenciamento de Segurança, e na fase Transição de Serviço durante o processo Validação e Teste do Serviço, com o desenho de mecanismos de teste das Liberações.

Um Evento pode ser classificado com base em três categorias:

- Informativo: Eventos que não requerem ações, sendo armazenados e mantidos por um determinado tempo. Geralmente utilizados para verificar o status de um IC ou confirmar se uma situação foi atendida ou executada. Servem também como insumos para monitorar o desempenho de ICs ou Serviços, como quantidade de transações em um período ou monitorar o acesso de usuários a um sistema.

- Aviso: Evento gerado quando um serviço ou IC está se aproximando de uma situação limite, como por exemplo, taxa alta de colisões na rede, uso de *swap* em disco do servidor, uso de *tablespace*do Banco de Dados, proximidade de ruptura do nível de serviço acordado.

- Exceção: quando uma determinada situação predefinida não está funcionando conforme previsto. Pode estar associado a metas de

níveis de serviços, perdas de funcionalidades ou baixa performance que impactem os serviços e possam vir a causar um incidente iminente ou quando o incidente já aconteceu.

2.6 Cumprimento de Requisição

Das solicitações feitas à Central de Serviços pelos usuários nem todas são sobre incidentes, podendo ser serviços que são previamente planejados, não causam impactos nos serviços de TI e já possuem procedimentos específicos para sua execução. Essas solicitações geralmente não precisam de testes complexos, não consomem recursos de capital alto e nem causam indisponibilidade nos serviços de TI. O processo Cumprimento de Requisição é o responsável por executar as Requisições de Serviços dos usuários que não estão relacionadas a incidentes e são previamente aprovadas, com baixo ou nenhum impacto na operação de TI, podendo ser realizado sem a necessidade de planejamento e/ou aprovação do Gerenciamento de Mudanças (FREITAS, 2013, p. 320).

Para que o Cumprimento de Requisição ocorra com sucesso, é importante que as equipes de suporte saibam diferenciar uma Solicitação de Serviço de um Registro de Incidente. Atualmente, muitas das equipes de TI trabalham em função de “apagar incêndios” operacionais da área de negócio, daí se dar sua grande dimensão. Atender a incidentes nos serviços de TI é diferente de corrigir erros operacionais nos sistemas causados por equívocos dos usuários, isso pode ocasionar acionamentos equivocados às equipes de TI, dando um custo a mais desnecessários paras empresas.

Este é um ponto crítico para as empresas que são auditadas pela lei Sarbanes-Oxley, pois pode alterar a integridade das informações financeiras, e deve ser realizado sempre com a devida aprovação das áreas de negócio envolvidas e com as devidas evidências da aprovação de sua realização. Requisições de Serviço são requisições de execução de serviços que já foram planejados, pré-aprovados e constam no Catálogo de Serviços.

A seguir alguns exemplos de Requisições de Serviços:

- Esclarecimento sobre dúvidas de uso dos sistemas.

- Solicitação de manuais.
- Instalação de softwares já pré-aprovados.
- Desbloqueio de usuário.

2.7 Gerenciamento de Problemas

Um Problema é a Causa Raiz de um ou mais incidentes. Já a Causa Raiz é a Causa desconhecida de um Incidente ou Problema. Essa Causa Raiz ainda não é conhecida no momento da abertura e registro do Problema, e sua investigação inicial é de responsabilidade do Gerenciamento de Problemas.

O processo Gerenciamento de Problemas tem como objetivo principal prevenir a ocorrência de Problemas e Incidentes associados a eles através da eliminação de Incidentes Recorrentes e da minimização do impacto de Incidentes que não puderam ser prevenidos (FREITAS, 2013, p. 326). O processo pode ter sua atuação subdivida em duas formas:

- **Gerenciamento de Problemas Reativo:** quando a resolução de problema é feita em resposta a um ou mais incidentes já ocorrido, tanto recorrente como incidente grave (o qual teve impacto significativo para o negócio).
- **Gerenciamento de Problemas Proativa:** quando problemas e falhas conhecidas são identificados e resolvidos com ações proativas planejadas, antes da ocorrência de incidentes que causem impactos no negócio. É iniciado na Operação de Serviço, mas geralmente executado como parte da Melhoria Continua dos Serviços de TI.

Magalhães e Pinheiro (2007) definem o processo de Gerenciamento de Problemas como a busca para eliminar, de forma permanente, os problemas e os incidentes repetitivos que afetam a infraestrutura de TI e, consequentemente, a prestação dos serviços de TI à organização dentro dos níveis de serviços acordados, com a finalidade de oferecer serviços de TI mais estáveis e reduzir o impacto sobre a produtividade das áreas cliente e do negócio de uma forma ampla.

O conceito do processo está ligado à prevenção de incidentes por meio da identificação e do tratamento definitivo da Causa Raiz de maneira que haja uma redução do número de incidentes. Parte da premissa que, com a eliminação das causas, haverá uma diminuição da quantidade de incidentes e o consequente aumento do índice de disponibilidade dos ativos de serviços entregues aos usuários (MELENDEZ FILHO, 2011).

2.7.1 Diferença de Incidentes e Problemas

Enquanto o Gerenciamento de Incidentes tem como objetivo restaurar a operação normal do serviço o mais rápido possível e garantir os melhores níveis de qualidade e disponibilidade do serviço, o Gerenciamento de Problemas identifica e remove erros do ambiente de TI, através da busca da causa raiz dos incidentes registrados no Gerenciamento de Incidentes, garantindo a máxima estabilidade dos serviços de TI.

Os dois processos podem gerar certas confusões, sendo que Incidentes são interrupções não planejadas nos serviços de TI e Problemas são causa raiz de um ou mais incidentes recorrentes ou que causem impactos significativos no negócio. Registros de Incidentes são diferentes de Registros de Problemas, pois um Incidente não se transforma em um Problema, e sim gera a abertura de um Registro de Problema, sendo os dois registros diferentes, resolvidos e atendidos em diferentes atividades e estágios, com ciclos de vida e finalidades diferentes. O Gerenciamento de Incidentes busca restabelecer o serviço o mais rápido possível podendo ser aplicada uma Solução de Contorno temporária, enquanto o Gerenciamento de Problemas busca a causa raiz do Problema e aplica uma solução definitiva para sua normalização, evitando assim a recorrência do incidente.

A grande preocupação que as equipes operacionais têm sempre estarem apagando incêndios, pode tirar o foco do que é realmente importante, como planejamento anterior para evitar ocorrências mais graves e recorrentes que causam impactos significativos pro negócio. Freitas (2013, p. 326) aborda essa preocupação no trecho a seguir:

> O Gerenciamento de Problemas é uma atividade geralmente realizada pelas equipes técnicas com o maior nível de conhecimento. Muitas empresas somente possuem estruturas de Gerenciamento de Incidentes e passam todo

> o seu tempo aplicando Soluções de Contorno continuamente. A identificação desse tipo de operação é muito fácil: geralmente as equipes de suporte estão atoladas de Incidentes e fazem muitas horas extras, sem, contudo, reduzir a taxa de Incidentes nos meses.

Esse trecho demonstra que um ciclo de vida do serviço em que as equipes estão apenas preocupadas em apagar incêndios, com aplicação de Soluções de Contorno não é o suficiente para manter a alta qualidade e atender aos melhores níveis de serviços acordados.

2.8 Gerenciamento de Acesso

Quando se fala em Acesso refere-se a um nível de funcionalidade de um serviço ou dados a que um usuário possui direito de acesso e uso. Assim, o processo Gerenciamento de Acesso tem como objetivo controlar o acesso de usuários ao direito de utilizar os serviços, e restringindo o acesso àqueles não autorizados. É no Gerenciamento de Acesso que são executadas as políticas e ações definidas anteriormente nos processos de Gerenciamento da Disponibilidade e Gerenciamento da Segurança da Informação (processos pertencentes ao Desenho do Serviço (FERNANDES; ABREU, 2012).

O Gerenciamento de Acesso é um processo executado pelas Funções Gerenciamento Técnico e Gerenciamento de Aplicações, gerenciando os acessos dos usuários de acordo com a Política de Segurança da Informação definida no processo Gerenciamento da Segurança da Informação. É aqui que é feira a concessão de acesso, alteração de privilégios de acesso e remoção de acesso através de Requisições de Serviço.

Com o Gerenciamento de Acesso, pode-se ajudar a proteger a confidencialidade, integridade e a disponibilidade de ativos, pois há uma garantia de que somente aqueles usuários que possuem direito possam acessar ou modificar esses ativos.

2.9 Gerenciamento de Incidentes

Freitas (2013, p. 300) define Incidente como “uma interrupção não planejada de um serviço de TI ou a redução de sua qualidade conforme requisitos acordados”. Assim, o processo de Gerenciamento de Incidentes busca reestabelecer

a operação normal de um serviço no menor tempo possível, de forma a minimizar os impactos adversos para o negócio, garantindo que os níveis de qualidade e disponibilidade sejam mantidos dentro dos padrões definidos (FERNANDES; ABREU, 2012).

Com esse processo há uma constante preocupação com uma maior disponibilidade dos ativos de serviços entregues, elevando assim a produtividade dos usuários que, por sua vez, aumenta o desempenho da organização e mantem o nível de satisfação do usuário sempre elevado (NAZARENO, 2013).

Melendez Filho (2011) também afirma que para se ter sucesso no processo de Gerenciamento de Incidentes é necessária a implantação de um procedimento robusto de escalonamento e a interação com os demais processos de gerenciamento, principalmente o Gerenciamento de Problemas, com o intuito de implementar uma solução definitiva para o erro detectado.

2.9.1 Modelo de Incidentes

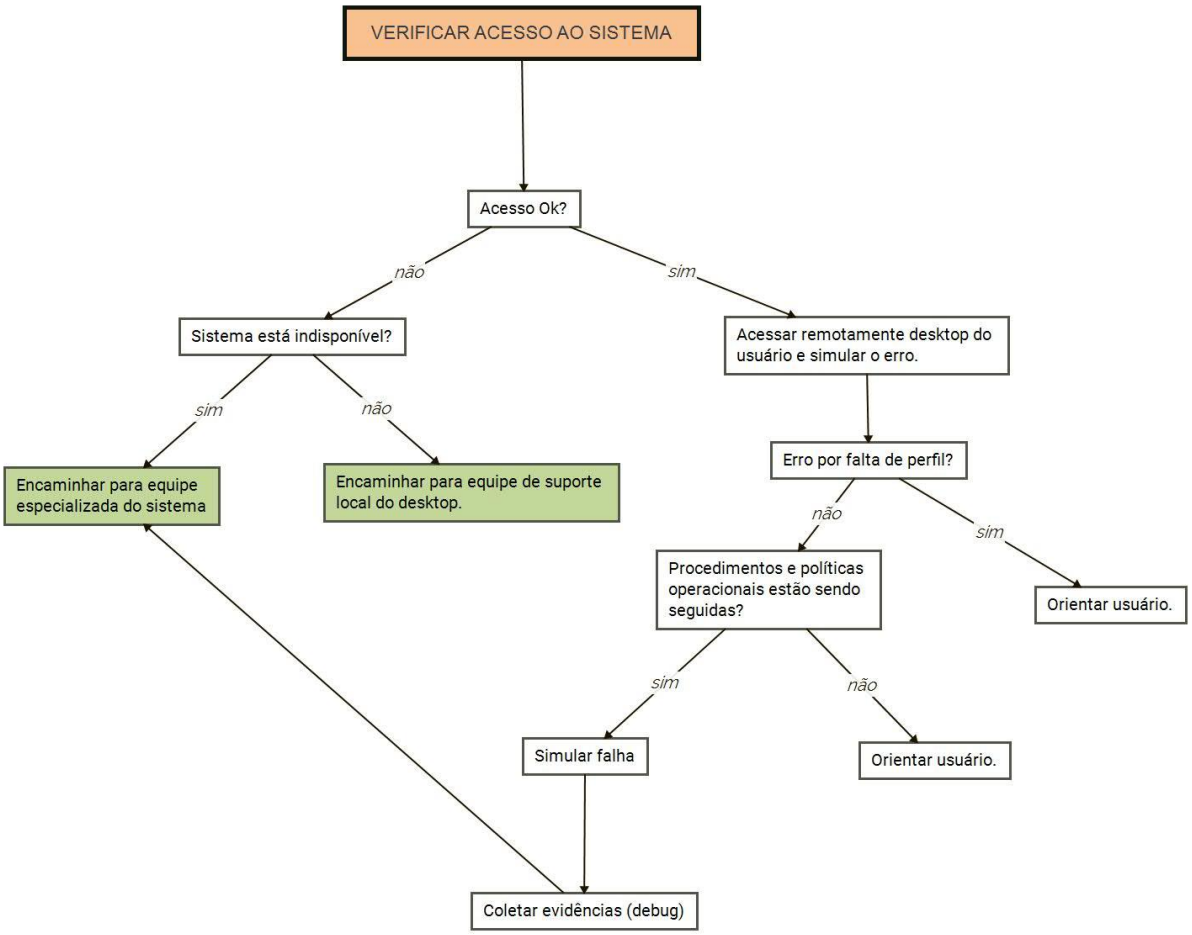
Incidentes ocorrem o tempo todo, e o Gerenciamento de Incidentes tem que estar pronto para atender às ocorrências no menor tempo possível e minimizar o seu impacto no negócio. Ele contempla o registro da falha reportada pelo usuário, a adoção de procedimentos rápidos de resolução, o acompanhamento da solução até o fechamento do registro de incidente, que só é efetivado com o aceito final do usuário. (MELENDEZ FILHO, 2011).

Entretanto, Freitas (2013) relata a notória preocupação com o fato de muitas equipes de suporte não documentarem e nem trocarem informações sobre os procedimentos realizados no tratamento e a resolução dos incidentes, gerando com isso tempo gasto desnecessariamente na busca de resoluções que já podem ter sido empregadas antes.

Uma solução para esse problema é a criação de modelos predefinidos de padrões (em formato de *scripts)* de atendimento para incidentes já conhecidos, que podem ajudar numa identificação mais rápida de ações a serem tomadas ou no encaminhamento de incidentes paras equipes responsáveis por resolvê-los. A seguir

exemplo de um modelo para reclamação de um usuário que não consegue cadastrar pedidos de vendas de produtos no sistema:

Figura 3 - Script Modelo de Incidentes



Fonte: Freitas (2013)

Com esse *script* de atendimento de Incidentes, o incidente pode ser rapidamente mapeado e resolvido orientando o usuário ou encaminhando para equipes especializadas. Freitas (2013) afirma que sem esses Modelos de Incidentes definidos, as seguintes situações são enfrentadas:

- Incidentes abandonados na fila de atendimento.
- Conflitos de responsabilidade: ninguém quer ser responsável pelo incidente.
- Incidentes parados na fila de atendimento esperando por alguma orientação para resolução.

- Equipes realizando as mesmas atividades repetidamente, como o contato com o usuário várias vezes para perguntar a mesma coisa.

O autor também lista o que deve contemplar um Modelo de Incidentes:

- Os passos predefinidos para atender aos tipos de incidentes.
- A ordem cronológica dos passos.
- Responsabilidades definidas.
- Prazos de atendimento.
- Procedimentos de escalação para outras equipes quando necessário.
- Todas as evidências necessárias sobre o incidente.

E os sistemas de Registro de Incidentes devem ser capazes de automatizar os Modelos de Incidentes.

2.9.2 Incidentes Graves (Críticos)

De acordo com Freitas (2013) “incidentes classificados como ‘graves’, ou seja, que causam impactos significativos no negócio, devem ser planejados para serem atendidos com urgência”. Esse tipo de incidente deve ter procedimento diferenciados do restante, garantindo assim seu atendimento em menor tempo possível e com garantias para que o impacto não seja maximizado.

A definição de gravidade e urgência dos incidentes é feita por acordos predefinidos no ciclo Desenho de Serviços, onde os cenários de riscos para os serviços de TI são mapeados.

2.9.3 Status dos Incidentes

Os incidentes devem ser identificados com *status* a fim de permitir o mapeamento de onde se encontram no seu ciclo de vida. Esses são exemplos de *status:*

Quadro 2 - Status dos Incidentes

Status	Definição
Aberto	Incidente registrado, porém sem vinculação a um responsável técnico para resolução.
Em progresso	Incidente em investigação e resolução.
Resolvido	O Incidente foi solucionado e a operação normal do serviço foi restaurada, porém sem validação do usuário.
Fechado	A operação normal do serviço foi restaurada e o usuário validou a resolução do Incidente.

Fonte: Freitas (2013)

Não é recomendável o *status* “aguardando” como algumas ferramentas de registro de Incidentes possuem. Esse status não deve ser considerado para contabilização de tempo do Incidente devido à TI ter que resolver a ocorrência sem nenhum motivo por fora. Os Acordos de Níveis de Serviço consideram os tempos em que os Incidentes impactam nos serviços, sendo que o que acontece nesse interim é de responsabilidades da TI e deve ser tratado pelos Acordos de Nível Operacional e Contratos de Apoio.

2.9.4 Atividades do Gerenciamento Incidentes

a) Identificação de Incidentes

Há várias formas de identificar um incidente, como pelo Gerenciamento de Eventos, pela equipe de TI ou reclamação/solicitação feita pelos usuários nos canais disponíveis, abertura de Registro de Incidente em software para tal, ou qualquer outra forma disponibilizada e gerenciada pela Função Central de Serviços.

b) Registro de Incidentes

Quando o Incidente for identificado deve ser imediatamente registrado em um sistema de Registro e Acompanhamento de Incidentes, assim como todas suas informações importantes que possam ajudar no seu atendimento. Os históricos dos Incidentes devem ser mantidos para analises futuras. Esse registro deve conter informações como:

- Código do Incidente.
- Categoria do Incidente.

- Urgência e priorização do Incidente.
- Impacto e sintomas do Incidente.
- Data e hora de abertura, assim como suas atualizações, resolução e fechamento.
- Identificação de quem está atendendo (pessoa ou equipe).
- *Status* do Incidente.
- Atividades realizadas para resolver o Incidente.
- Resolução aplicada.
- Metas de atendimento do ANS.

c) Categorização do Incidente

A categorização dos Incidentes baseia-se no Catálogo de Serviços de Negócio, no Catálogo de Serviços de TI, em Pacotes de Serviços, Linhas Base de Serviços, Sistemas de Gerenciamento de Configuração, etc.

d) Priorização do Incidente

Para se priorizar um Incidente deve-se embasar numa matriz de risco entre urgência do tratamento do Incidente e o impacto que o Incidente causa na operação do negócio.

A urgência é o tempo máximo que uma empresa deve aguentar os impactos do Incidente sem solução. A seguir um exemplo de matriz de definição de prioridades utilizando a Matriz GUT (Gravidade, Urgência e Tendência):

Quadro 3 - Matriz GUT de Priorização

Gravidade (Impacto)	**Urgência (Prazo)**	**Tendência (Agravamento)**	**Prioridade**
Muito Alto	Imediata	Piora imediata	1
Alto	Urgência média	Piora rápida	2
Médio	Urgência baixa	Piora lenta	3
Baixo	Atendimento normal	Piora muito lenta	4

Muito Baixo	Pode aguardar	Piora estagnada	5

Fonte: Freitas (2013)

Após a priorização definida, um ANS pode definir a escala de metas de atendimento de prioridade para os serviços:

Quadro 4 - Prioridade x Tempo para Resolução

Prioridade	**Tempo para Resolução**
1	1 hora
2	4 horas
3	8 horas
4	24 horas
5	40 horas

Fonte: Freitas (2013)

e) Diagnóstico Inicial do Incidente

Análise do sintoma ou consequências do incidente a fim de escolher o Modelo de Incidente adequado, caso haja. Para realização do diagnóstico, qualquer informação de histórico de Incidente é relevante, e podem ser encontradas na base de informações de Incidentes anteriores e na Base de Dados de Erros Conhecidos.

f) Escalação do Incidente

Com o diagnóstico em mãos e sem Solução de Contorno ou Resolução aplicada em primeiro nível, o Incidente deve ser direcionado para outro nível, ou equipe, capaz de solucioná-lo. Há dois tipos de Escalações:

1) Escalação Funcional: quando o Incidente é escalado para uma equipe especializada, diferente das equipes de níveis menores, capaz de resolvê-lo. Pode ser utilizado Acordos de Níveis Operacional entre as equipes para garantir o atendimento do ANS.
2) Escalação Hierárquica: quando Incidente necessitam de uma solução mais complicada, que um nível hierárquico mais alto necessita ser acionado ou notificados, para uma melhor tomada de

decisão para resolução; ou quando um nível hierárquico maior deve ser acionado para resolução de conflitos.

g) Investigação e Diagnóstico do Incidente

- Identificar o que está fora da operação normal de um serviço.
- Entender a cronologia dos eventos que levaram ao Incidente.
- Confirmar as informações que levem à classificação da priorização.
- Identificar os eventos que podem ter causado o Incidente.
- Analisar informações do Sistema de Gerenciamento de Conhecimento de Serviço para identificar Incidentes anteriores, registros de Problemas, Base de Erros Conhecidos, informações de Fornecedores, informações de Eventos ou Requisições de Mudanças.

h) Resolução e Recuperação do Incidente

Quando for encontrada uma Solução de Contorno ou Resolução para o Incidente, deve ser avaliado se ela altera algum atributo do IC no BDGC, caso sim e seja alteração de escopo para Gerenciamento de Mudanças, deve ser aberto uma RDM para resolução. Caso não necessite de abertura de RDM, a solução é aplicada e os Incidentes são fechados pela Central de Serviço.

i) Fechamento do Incidente

Com o Incidente resolvido, a Central de Serviços faz uma verificação final para ver se o Incidente foi mesmo solucionado e qual o nível de satisfação do usuário. As informações importantes que devem ser registradas e o histórico de tratamento do Incidente (de acordo com a política de registro de Incidente) também são verificados pela Central de Serviço. Caso nada disso esteja de acordo, a CS retorna o Incidente de volta para equipe responsável.

2.9.5 O Gerenciamento de Incidentes com outros processos

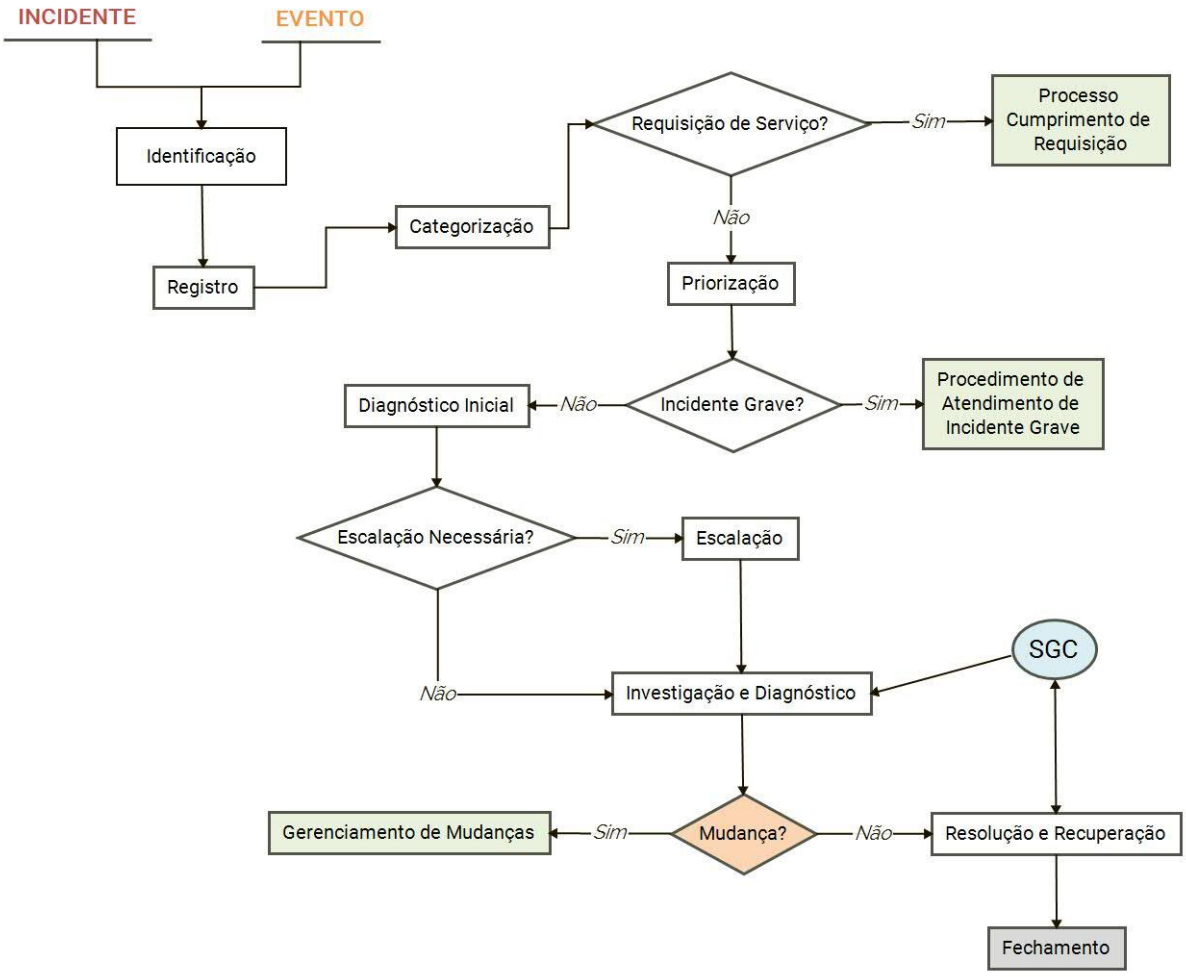
Como em todo processo, o Gerenciamento de Incidentes também possui entradas e saídas, e sua principal entrada são os incidentes, os quais podem se originar de diversos lugares como usuários, equipes de operação, redes ou ferramentas de monitoramento e até outros processos. O processo de Gerenciamento de Incidentes deve seguir o seguinte fluxo:

- **Entradas:**
  - Incidentes encaminhados pela Central de Serviços.
  - Eventos encaminhados pelo Gerenciamento de Eventos.
  - Informações sobre os ICs do Gerenciamento de Configuração e Ativos de Serviço.
  - Informações sobre os níveis de serviços do Gerenciamento de Nível de Serviço.
  - Informações sobre os serviços do Gerenciamento de Catálogo de Serviço.
  - Informações sobre Mudanças do Gerenciamento de Mudanças.
  - Informações sobre Erros Conhecidos do Gerenciamento de Problemas.
  - Informações do Sistema de Gerenciamento de Conhecimento dos Serviços do Gerenciamento de Conhecimento.
  - *Feedback* de usuários dos serviços para o Gerenciamento de Relacionamento com o Negócio.
- **Saídas:**
  - Informações sobre Incidentes para todos os outros processos.
  - Identificação de Incidentes relacionados com Itens de Configuração.
  - Incidentes resolvidos para a Central de Serviços.

- Abertura de Registro de Problemas.
- Abertura de Requisições de Mudanças.

A seguir o fluxo das atividades do Gerenciamento de Incidentes, representado como um *script* com procedimentos a partir da entrada do processo até a resolução do incidente:

Figura 4 - Fluxo de Atividades do Gerenciamento de Incidentes



Fonte: Freitas (2013)

2.9.6 Papeis e Responsabilidades do Gerenciamento de Incidentes

No quadro a seguir são definidos os papeis e responsabilidades de alguns dos envolvidos no Gerenciamento de Incidentes:

Quadro 5 - Papeis e Responsabilidades do Gerenciamento de Incidentes

Papel	Responsabilidades
Dono do Processo	• Garantir que o processo esteja adequado aos propósitos. • Desenhar Modelos de Incidentes e fluxos de trabalho para o tratamento de Incidentes. • Trabalhar com outros donos de processo garantindo colaboração para o Gerenciamento de Incidentes. • Garantir que a documentação do processo esteja atualizada e acessível a todos os envolvidos. • Garantir que os envolvidos sejam informados das mudanças realizadas no processo. • Auditar o processo para garantir que esteja sendo seguido de acordo com o especificado. • Garantir que os envolvidos sejam treinados adequadamente para execução do processo. • Garantir a autoridade necessária a todos os papéis do processo.
Gerente do Processo	• Garantir a eficiência e eficácia das atividades do Gerenciamento de Incidentes, que o processo seja seguido como o especificado. • Prover relatórios sobre os Incidentes dos serviços de TI da organização. • Gerenciar as equipes de atendimento de Incidentes, assim como indicar as pessoas adequadas aos papéis. • Monitorar as atividades do Gerenciamento de Incidentes e propor melhorias par ao processo. • Planejar e manter os sistemas de Gerenciamentos de Incidentes.

	• Gerenciar os Incidentes Graves. • Coordenar as interfaces entre o Gerenciamento de Incidentes e os outros processos, principalmente o Gerenciamento de Eventos e Gerenciamento de Problemas. • Desenvolver procedimentos e políticas de Modelos de Incidentes, escalação, priorização e resolução de conflitos no atendimento de Incidentes. • Garantir o alcance dos indicadores de desempenho do processo. • Manter os usuários informados sobre seus incidentes. • Decidir a respeito das escalações hierárquicas de incidentes. • Garantir a inclusão e atualização dos erros conhecidos na base de conhecimento. • Auxiliar os operadores na solução de incidentes.
Central de Serviços	• Registrar todos os incidentes reportados à Central de Serviços. • Categorizar os incidentes no prazo acordado do SLA. • Contatar o usuário para conseguir mais informações sobre o incidente quando necessário. • Realizar o atendimento dos incidentes que possuam solução na base de conhecimento. • Ajudar na atualização da base de conhecimento com os erros conhecidos.

Fonte: Freitas (2013)

3 ESTUDO DE CASO DA INSTITUIÇÃO PÚBLICA BANCÁRIA

Este estudo de caso surgiu a partir da observação da área de operações de tecnologia de uma Instituição Pública Bancária na minimização dos impactos causados por incidentes recorrentes e graves para os clientes finais da empresa. Muitas dessas ocorrências tem causa processos distintos para resolução de incidentes, canais variados para resgistro desses incidentes, falta de observação no histórico de incidentes já ocorridos antes, entre outros.

Este trabalho foi desenvolvido com o metodo de estudo de caso único, utilizando a analise do processo de Gerenciamento de Incidentes atual da Instituição Pública Bancária e seu alinhamento às melhores práticas do ITIL.

O contexto geral desse trabalho proporciona uma analise crítica sobre o processo implantado na área operacional de TI da intituição bancária, podendo assim ajudar na tomada de deciões para sua melhoria.

3.1 Instituição Pública Bancária

A Instituição Pública Bancária estudada é um banco múltiplo e agente responsável por auxiliar em algumas políticas de crédito do Governo Federal, dentre elas saneamento, habitação e políticas sociais. Com filiais em todo o território nacional, a Instituição estudada possui uma governança corporativa que atua num desempenho empresarial responsável, em conjunção com sustentabilidade e transparência, preocupada ainda com as dimensões sociais, econômicas e ambiental.

A área de tecnologia da Instituição, formada por uma vice-presidência, uma diretoria, três superintendências (Governança, Construção e Operacional), as quais possuem nove gerências nacionais, cinco centralizadoras e filiais de tecnologia, exerce um importante papel como agente transformador e estratégico para os negócios dentro e fora da organização.

O Planejamento Estratégico da Instituição, desdobrado em Iniciativas Estratégicas e Projetos Estratégicos, tem como finalidade a execução dos Objetivos Empresariais do Mapa Estratégico, com vistas à materialização da Visão de Futuro da empresa.

As orientações para Tecnologia no ciclo estratégico atual foram elaboradas a partir dos Objetivos Empresariais declarados no Plano Estratégico e das Aspirações Estratégicas da TI da Instituição, como:

- Ser a melhor área de TI entre os bancos do país;
- Dedicar no máximo 40% em manutenção e no mínimo 60% da capacidade de TI para inovação, crescimento e transformação;
- Ter disponibilidade mínima de 98% para os serviços críticos.

A Instituição utiliza como mecanismo de avaliação de seu desempenho o BSC – Balance Score Card, que tem como objetivo medir e avaliar o desempenho, qualificando ativos intangíveis críticos como pessoas, informação e cultura.

> O *Balanced Scorecard* é um sistema que sonsidera indicadores não somente financeiros, mas também não financeiros, oriundos da organização. Seu diferencial é a capacidade de comunicar a visão e a estratégia por meio de indicadores de desempenho originários de objetivos estratégicos e metas que interagem em meio a uma estrutura lógica de causa e efeito (KAPLAN e NORTON, 1997).

Essa ferramenta é utilizada pela Instituição como apoio para acompanhar e monitorar as evoluções de suas decisões, centradas em indicadores chaves, sendo muito importante para estratégia da empresa.

Para alcançar um dos Objetivos Empresariais “Ter disponibilidade e performance nos serviços de TIC”, foram estipulados Objetivos de TI dentro das perspectivas do BSC. Os Objetivos de TI “Alinhar entregas de Tias necessidades de negócios”, da perspectiva Governança e Financeira; “Garantir soluções e canais integrados, disponíveis e atualizados tecnologicamente”, da perspectiva Cliente e, principalmente, “Ter disponibilidade e performance nos Sistemas de TI”, da perspectiva “Processos Internos” são os beneficiados pelo Gerenciamento de Serviços de TI da empresa, que se torna assim de suma importância para atender à Governança de TI e, consequentemente, à Governança Corporativa.

3.2 Gerenciamento de Serviços de TI na Instituição

O Gerenciamento de Serviços de TI da Instituição consiste no conjunto especializado de processos organizacionais que, integrados, proporcionam visão unificada e sistêmica do serviço de TI (Documentação Normativa da Instituição, 2016).

Como objetivo visa garantir, continuamente, o alinhamento dos serviços de TI com o negócio da Instituição, integrando áreas e processos. Os processos do gerenciamento de serviços de TI devem ser padronizados, unificados e correlacionados, permitindo o acompanhamento do ciclo de vida dos serviços.

Os processos contemplados no gerenciamento de serviços de TI da Instituição são:

- Gerenciar Configuração de TI;
- Gerenciar Incidentes de TI;
- Gerenciar Mudanças de TI;
- Gerenciar Níveis de Serviços de TI;
- Gerenciar Problemas de TI.

A disciplina Gerenciar Conhecimento também é contemplada pela Operação de TI, compondo assim o gerenciamento de serviços de TI da Instituição.

3.3 O Processo de Gerenciamento de Incidentes na Instituição

De acordo com Freitas (2013), um incidente é uma interrupção não planejada de um serviço de TI ou uma redução da qualidade de um serviço de TI, podendo ocorrer a partir de uma falha de um Item de Configuração que ainda não tenha impactado um serviço de TI. A documentação normativa da Instituição (2016) define incidente como “qualquer falha que não faz parte da operação normal de um serviço e que causa interrupção ou redução na qualidade do serviço prestado”

De acordo com a documentação da Instituição, o objetivo do processo de Gerenciar Incidentes de TI é fornecer atendimento aos incidentes em tempo oportuno e eficaz, respondendo às requisições de usuários e negócio, e solução de ocorrências. Esse processo é de responsabilidade do Gerenciamento Integrado de TI, o qual consistem num conjunto especializado de processos organizacionais agregados que proporcionam visão unificada e sistêmica do serviço de TI.

Os papeis e responsabilidades do processo de Gerenciamento de Incidentes na Instituição é descrito de acordo com a Matriz de Responsabilidade a seguir:

Quadro 6 - Matriz de Responsabilidade do processo da Instituição

Matriz de Responsabilidade do Processo Gerenciar Incidentes de TI						
Atividades	**Gerente de Incidentes**	**Atendimento ao usuário**	**Agente de Monitoração**	**Analista de Service Desk**	**Analista de Suporte**	**Analista de Integração**
Monitorar			R			
Registrar		R	R	R	R	
Categorizar				R	R	
Prioriza	C			R	R	
Efetuar Relacionamentos (duplicação, rel. demais processos)				R	R	
Escalonar funcional e hierarquicamente	C	R	R	R	R	R
Gerenciar o ciclo de vida	I			R		I
Decretar Procedimento de Crise	R / A					R/ A
Solucionar					R	
Validação de solução		R		I	R	

Fonte - Documentação Normativa da Instituição Pública Bancária (2016)

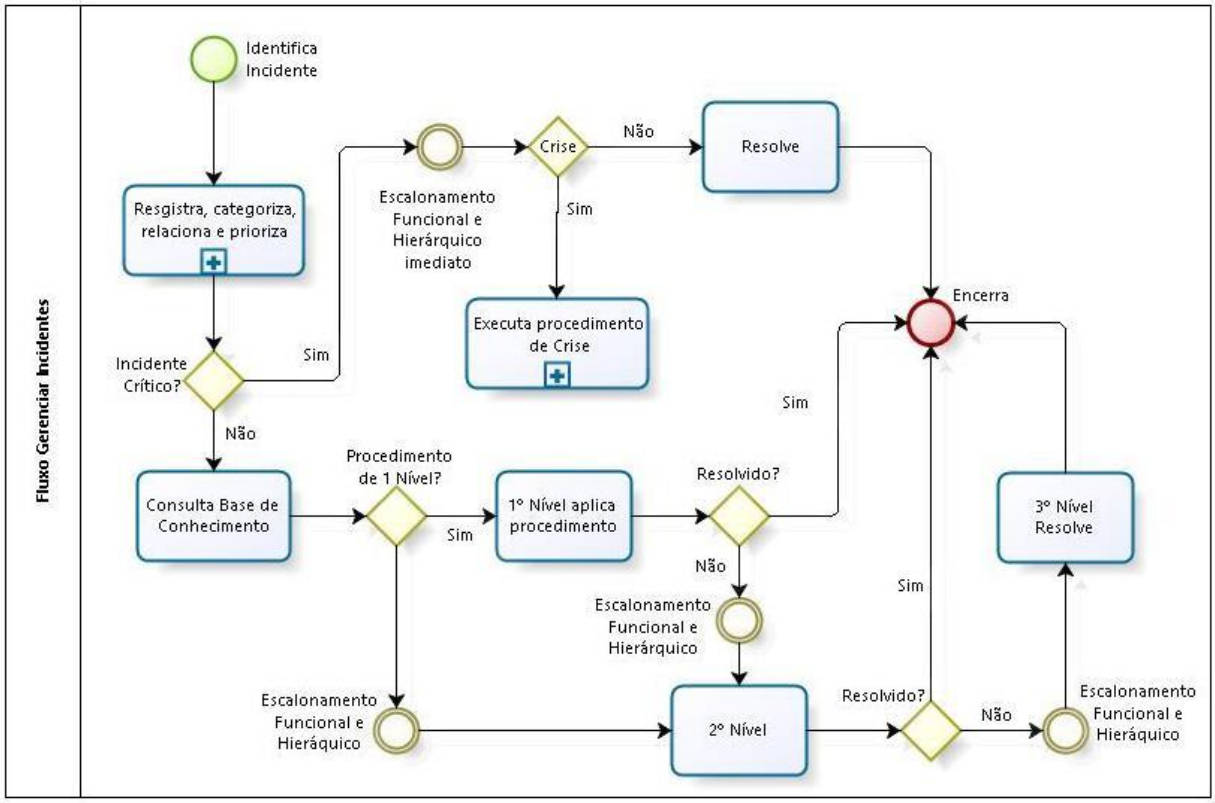
Legenda:
R – responsável por executar
A – aprovador
C – consultado
I – informado

A Instituição possui definido um ciclo de vida dos Incidentes, com as etapas percorridas pelo incidente que visam garantir que o mesmo seja registrado em ferramenta padronizada, sendo o incidente devidamente categorizado para que o tratamento ocorra de maneira priorizada. Nesse ciclo de vida também contempla o registro vinculado dos outros processos que fazem relacionamento com o Gerenciamento de Incidentes.

O relacionamento do Gerenciamento de Incidentes com os demais processos é contemplado de forma estruturada e objetiva na documentação da Instituição, com as entradas e saídas descritas de forma abrangente e sucinta, e com um Fluxo desenhado considerando todos os processos e artefatos dos relacionamentos.

A seguir o fluxo Modelo de Incidentes do processo definido na Instituição:

Figura 5 - Modelo de Incidentes da Instituição



Fonte: Documentação da Instituição Pública Bancária (2016)

O fluxo demostra os passos das atividades do Gerenciamento de Incidentes contemplados para alcançar grande parte das etapas do ciclo de vida do incidente.

3.3.1 Ciclo de Vida do Incidente

A documentação da Instituição define que as etapas percorridas pelo incidente durante seu ciclo de vida sejam registradas, assim como o próprio incidente, em ferramenta padronizada, assim como todos os registros dos demais processos que possuam vínculo com o incidente sejam a ele relacionados.

É definido que o incidente somente é fechado após validação do reclamante, que, caso não ocorra, o chamado é encerrado automaticamente após três dias. A documentação também aborta que procedimentos de Crise de devem ser instaurados sempre que um incidente crítico (ou grave) necessitar de um acompanhamento diferenciado.

3.4 Análise dos Resultados

Para verificação da aderência do processo de Gerenciamento de Incidentes implantado na Instituição Pública Bancária com as recomendações de melhores práticas do ITL, é apresentado um quadro com uma análise comparativa dos principais elementos citados pelos autores.

Quadro 7 - Analise comparativa do Gerenciamento de Incidentes da Instituição com o ITIL

Elemento	Visão Bibliográfica (Autores)	Visão da Instituição	Recomendações
Aderência ao ITIL	A adoção do ITIL eleva o grau de maturidade e qualidade da organização no uso dos ativos estratégicos de TI. (FERNANDES e ABREU (2012)	Foi identificado a adoção do ITIL na Instituição.	Manter os processos da Instituição atualizado de acordo com o ITIL e elevar a maturidade.
Ciclo Operação de Serviço	O ciclo Operação de Serviço deve manter a satisfação e a confiança nos serviços de TI por parte dos usuários e minimizar o impacto na execução diária do negócio pela empresa. (FREITAS, 2013)	Foi identificado o ciclo Operação de Serviços na Instituição composto por seis processos.	Alinhar o ciclo Operação de Serviços da Instituição ao recomendado pelo ITIL.
Aplicação do Gerenciamento de Incidentes	O Gerenciamento de Incidentes busca reestabelecer a operação normal de um serviço no menor tempo possível, minimizando os impactos adversos para o negócio. (FERNANDES; ABREU, 2012)	Foi identificado manual normativo especifico que trata de Gerenciamento de Incidentes na Instituição.	Manter o Gerenciamento de Incidentes atualizado.
Modelos de Incidentes	Modelos predefinidos de padrões (em formato de *scripts*) de atendimento para Incidentes conhecidos podem ajudar na identificação mais rápida de ações a serem tomadas ou no encaminhamento de Incidentes paras equipes responsáveis por resolvê-los. (FREITAS, 2013)	Foi identificado apenas um fluxo de Modelo de Incidente na Instituição, utilizado para todos os tipos de incidentes.	Criar submodelos para os tipos Incidentes mapeados.

Elemento	Visão Bibliográfica (Autores)	Visão da Instituição	Recomendações
Registro em Ferramenta	O Incidente deve ser imediatamente registrado em um sistema de Registro e Acompanhamento ao ser identificado, assim como todas as informações que possam ajudar no seu atendimento e em analises futuras. (FREITAS, 2013)	Foi identificado que o registro do Incidente é feito em ferramenta padronizada, assim como sua devida categorização para tratamento priorizado.	Monitorar o registro e armazenamento (histórico) das informações dos Incidentes.
Relacionamento entre os processos	Para ter sucesso no Gerenciamento de Incidentes é necessária a implantação de um procedimento robusto e a interação com os demais processos de gerenciamento. (MELENDEZ FILHO, 2011)	Foi identificado que o Gerenciamento de Incidentes tem relacionamento com todos os processos definidos na Instituição.	Garantir que os relacionamentos sejam aplicados.
Papeis e Responsabilidades	Deve haver uma definição dos papeis e responsabilidades dos envolvidos no Gerenciamento de Incidentes. (FREITAS, 2013)	A Instituição possui definido os papéis e responsabilidade do seu Gerenciamento de Incidentes.	Garantir que os papeis e reponsabilidades sejam implantados e seguidos.
Incidentes Graves	Incidentes classificados como ‘graves’ devem ser planejados para serem atendidos com urgência, possuindo procedimentos diferenciados do restante para seu atendimento em menor tempo possível e para que o impacto não seja maximizado. (FREITAS, 2013)	A documentação define procedimentos de Crise sempre que um incidente crítico (grave) necessitar de acompanhamento diferenciado.	Manter os procedimentos de atendimento a incidentes graves atualizados.
Fechamento do Incidente	Após o Incidente resolvido, deve ser feita uma verificação final com o usuário se o mesmo foi solucionado, retornando o Incidente à equipe responsável caso não possua a confirmação do usuário. (FREITAS, 2013)	De acordo com a documentação o Incidente só é fechado após validação do reclamante, e caso essa não ocorra, o chamado é encerrado.	Garantir que o usuário/reclamante sempre realize a validação da resolução.

Fonte – Elaborado pelo autor (2016)

A análise comparativa do processo da empresa de acordo com visão dos autores no quadro 7 (Analise comparativa do Gerenciamento de Incidentes da Instituição com o ITIL) demonstrou que os elementos elencados como requisitos importantes para o sucesso na implantação do Gerenciamento de Incidentes foram aplicados na Instituição, alinhados – totalmente ou parcialmente – com as recomendações do ITIIL.

Foi verificado que alguns elementos, como “Modelos de Incidentes” e “Fechamento do Incidente”, foram aplicados de forma parcialmente na Instituição. Para “Modelos de Incidentes” cujos autores recomendam haver modelos predefinidos para os incidentes conhecidos, foi identificado apenas um modelo na Instituição. Enquanto o elemento “Fechamento do Incidentes” cujos autores recomendam o retorno do incidente à equipe responsável caso o usuário não confirme sua resolução, foi identificado na instituição que neste caso o incidente o “chamado é encerrado”.

A partir dos resultados, percebe-se que para a manutenção e melhoria do Gerenciamento de Incidentes, são necessárias atualizações constantes em todo o processo, tanto para os elementos aplicados parcialmente, como para aqueles totalmente aderentes. Dessa forma, foram feitas recomendações para cada elemento elencado no quadro acima.

CONCLUSÃO

Observa-se que acompanhar a inovação para atender às exigências do negócio faz muitas áreas de TI tornassem incapazes de manter seus procedimentos já estabelecidos atualizados, passando muito tempo em intervenções reativas e resolvendo repetidamente incidentes e problemas, em vez de eliminá-los. Com as melhores práticas do ITIL, uma nova abordagem para a problemática do suporte aos serviços de TI é apresentada com benefícios notadamente alcançados (MAGALHÃES; PINHEIRO, 2007).

Percebe-se que, a partir da análise dos resultados com verificações embasadas no que os autores afirmam, para um bom Gerenciamento de Incidentes é necessário seguir e aplicar alguns elementos, como: realização do ciclo Operação de Serviço, adesão ao ITIL, aplicação do Gerenciamento de Incidentes, criação de modelos de incidentes, registro dos incidentes em ferramenta, relacionamento do Gerenciamento de Incidentes com outros processos, papeis e responsabilidades, atendimento prioritário para incidentes graves e fechamento do incidente após verificação do usuário reclamante. Esses são atributos necessários para uma gestão de serviços de TI e, consequentemente, Governança de TI.

Conclui-se que, a partir dos resultados obtidos com o estudo de caso sobre a análise do processo de Gerenciamento de Incidentes, a Instituição estudada tem aplicado as melhores práticas do modelo ITIL - *Information Technology Infrastructure Library*, fazendo deste uma métrica importantes para o alcance Objetivos de TI alinhados aos Objetivos Empresariais do Planejamento Estratégico da empresa.

Neste caso, recomenda-se manter atualizações continuas dos elementos e documentações que referenciam o processo de Gerenciamento de Incidentes, assim como os seus relacionamentos, dentro da Governança de TI da Instituição.

REFERÊNCIAS

ALVES, Estefan; RANZI, Thomas. **Governança de TI: Avaliação de Maturidade do COBIT em uma Empresa Global**. 2006. 90 Folhas. Trabalho de conclusão de curso – Universidade Federal de Santa Catarina, Florianópolis, 2006.

DARYUS. **Pesquisa Nacional de Segurança da Informação** – Uma visão estratégica dos principais elementos da Segurança da Informação no Brasil. 2014. Disponível em: http://datasus.saude.gov.br/images/Pesquisa_Nacional_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_2014_-_DARYUS.pdf. Acesso em: 31 jan 2017.

FERNANDES, Aguinaldo; ABREU, Vladimir. **Implantando a Governança de TI:** Da Estratégia à Gestão dos Processos e Serviços. 3. ed. Rio de Janeiro: Brasport. 2012.

FREITAS, Marcos Andre dos Santos. **Fundamentos do Gerenciamento de Serviços de TI**. 2ª Edição. Rio de Janeiro: Editora Brasport, 2010.

IBGC-INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. 2005. Disponível em: <http://www.ibgc.org.br/Secao.aspx?CodSecao=17>. Acesso em: 01 Ago. 2016.

ITIL® Glossary of Terms English. **ITIL glossary and abbreviations** – English. V. 1.0. AXELOS limited, 2011. Disponível em: https://www.axelos.com/corporate/media/files/glossaries/itil_2011_glossary_gb-v1-0.pdf. Acesso em: 7 fev. 2017.

KAPLAN, R. S.; NORTON, D. P. **A Estratégia em Ação:** Balanced Scorecar. Tradução de Luiz Euclydes Trindade Frazão Filho. 13.ed. Rio de Janeiro: Campus, 1997.

LEITE, K. V. B. S.; REIS, M. **O Acordo de Capitais de Basiléia III:** Mais do Mesmo? *EconomiA*, Brasíla, v.14 n.1A, p. 159-187, jan./abr. 2013.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de Serviços de TI na Prática:** Uma abordagem com base na ITIL. São Paulo: Novatec Editora, 2007.

MELO, Daniel Reis Armond. **A importância da tecnologia da informação nas estratégias das organizações contemporâneas**: breve revisão de literatura. In: V Convibra, 2008. Disponível em: http://www.convibra.com.br/2008/artigos/412_0.pdf. Acesso em: 01 dez. 2016.

MENDONÇA, Claudio Márcio Campos et al. Governança de tecnologia da informação: um estudo do processo decisório em organizações públicas e privadas. **Revista de Administração Pública**, Rio de Janeiro, v. 47, p. 443-468, 2013.

NAZARENO, Gustavo. **Implantação de uma Central de Service Desk à luz do ITIL v3:** propostas para as gerências de portfólio, demanda, incidentes e problemas. 2013. 48 Folhas. Trabalho de conclusão de curso – Serviço Nacional de Aprendizagem Comercial – SENAC, Brasília, 2013.

OGC - OFFICE OF GOVERNM ENT COMMERCE. ***Service Strategy*****.** UK.TSO.2007a.

SILVA, Jaqueline. **Aderência do Processo de Gerenciamento de Mudanças de uma Instituição Pública Bancária às Recomendações de Melhores Práticas da ITIL:** Estudo de Caso em uma Instituição Pública Bancária. 2014. 75 Folhas. Trabalho de conclusão de curso – Centro Universitário de Brasília, Brasília, 2014.

VAN GREMBERGEN, Wim; DE HAES, Steven; GULDENTOPS, Erik. Estructures Processes and Relational Mechanisms for IT Governance. In: VAN GREMBERGEN, Win (ed.). **Estrategies for Information Technology Governance**. Hersehey, PA, USA: Idea Group Publishing, 2004.

WEILL, Peter; ROSS, Jeanne W. **Governança de Tecnologia da Informação**. São Paulo: M. Books, 2006.

WEISS, M. C.; BERNARDES, R. C. **As Práticas de Governança e Gerenciamento de Serviços de TI como Vetor para a Melhoria do Desempenho Empresarial:**

Estudo de Caso em uma Empresa Atacadista*. Gestão e Planejamento*, Salvador, v.15 n.1, p. 100-117, jan./abr. 2014.

WELLINK, N. **The Basel Committee and Regulatory Reform**. Discurso proferido no Institute of International Finance, Viena, Junho, 2010.