Implantação de *IT Service Continuity Management*: um estudo sobre como conduzir

Natália Martins Valdiones
Pós Graduanda | MBA Gestão de Business Intelligence
UniFMU - São Paulo, 2020

Danilo Quelicone Costacurta
Professor responsável
Disciplina: Arquitetura de TI e Modelos de Negócios

Resumo

Este artigo tem como objetivo mostrar, através de revisão bibliográfica e aplicação prática, as etapas da implantação de *IT Service Continuity Management* em uma instituição financeira fictícia através da apresentação de uma situação próxima da realidade.

Palavras Chave: *IT Service Continuity Management*, Gerenciamento de Continuidade de Serviços baseados em Tecnologia da Informação, ITSCM, Arquitetura de TI.

Abstract

This article aims to present, through bibliographic review and practical application, the stages of implementing IT Service Continuity Management in a fictitious financial institution by presenting a situation close to reality.

Key Words: IT Service Continuity Management, ITSCM, IT Architecture.

1. Introdução

Nos dias de hoje é praticamente impossível imaginar a nossa vida sem a presença da tecnologia. Quase todas as atividades dos mais variados setores são baseadas por algum tipo de Arquitetura de TI, e uma das principais e talvez mais importante questão é a continuidade dessas atividades.

Não importa se estamos falando de um simples comércio que decide deixar de usar a caixa registradora para fazer a automação de seus processos ou se estamos falando de grandes instituições que buscam melhoria contínua, precisão e segurança máxima para todas as suas operações, a grande preocupação é o que fazer para que as suas atividades não fiquem indisponíveis.

Segundo [5], a Continuidade de negócios está diretamente ligada a um conjunto de conceitos que vão desde o tempo necessário para restabelecer um serviço, ou a parte dele que foi afetada, até ações para diminuir ou evitar a probabilidade de acontecer eventos que possam interromper os serviços prestados. Isso no ramo de arquitetura de TI é conhecido como *IT Service Continuity Management* (ITSCM) ou, em português, Gerenciamento de Continuidade de Serviços baseados em Tecnologia da Informação.

O ITSCM consiste no uso de técnicas para identificação de ameaças e vulnerabilidades do negócio, as probabilidades de tais ameaças ocorrerem e os possíveis impactos que causariam, para então desenvolver planos de ação com o objetivo de minimizar impactos ou evitar que tais ameaças aconteçam.

Neste artigo será apresentada a aplicação do ITSCM em uma situação hipotética próxima da realidade e faremos a análise de suas etapas e resultados identificando as melhores ações para a situação proposta.

2. Objetivo

O caso a ser analisado neste artigo nos apresenta o Banco Beta, uma instituição financeira consolidada no mercado com excelentes índices nas avaliações realizadas pelo Banco Central do Brasil (BCB), mas que por apresentar crescimento constante na demanda e consequentemente crescimento nos pontos de auditoria apontados pelo próprio BCB identificou a necessidade da implantação do ITSCM para evitar queda na sua avaliação e possíveis prejuízos para o negócio. O objetivo para este estudo é apresentar um modelo de implantação de ITSCM que atenda o Banco Beta em todas as necessidades apresentadas.

3. Discussão e Métodos

Segundo [6], ITSCM nada mais é do que *"um conjunto de estratégias, ferramentas e softwares que acompanham e gerenciam todo o ciclo de vida dos serviços de TI"*. A implantação do ITSCM, apesar de importante e complexa, ela acontece basicamente em 5 etapas:

1. Identificação das ameaças do negócio;
2. Identificação das vulnerabilidades do negócio;
3. Identificação das probabilidades de ocorrência das ameaças encontradas;
4. Identificação dos impactos e efeitos no negócio caso essas ameaças de fato aconteçam;
5. Construção de um plano de ação contra tais ameaças seja ele para evitar ou reduzir impactos.

3.1. Apresentação do caso

O Banco Beta, instituição financeira situada no interior do Paraná, com nome consolidado no ramo de crédito e com excelentes índices nas avaliações realizadas tanto pelo BCB quanto por seus clientes, decide que chegou a hora de realizar a implantação do ITSCM, pois nos últimos anos apresentou aumento da demanda por serviços como conta corrente, cartões de crédito, seguros, consórcios e empréstimos dos mais variados e com isso os pontos de auditoria têm aumentado em relação à falta de estratégias para a continuidade do negócio, todas elas apontadas pelo BCB, incluindo a possibilidade de encerramento de certos serviços e fechamento de algumas agências pela falta de continuidade adequada.

Sendo assim o diretor financeiro João decide ouvir José, diretor de Tecnologia da Informação (TI) e que sempre se mostrou a favor da implantação do ITSCM. José decide então convidar Maria para ser responsável pela implantação do ITSCM no Banco Beta, já que é uma profissional experiente na área que já atuou em várias instituições no país, estando adequadamente preparada para enfrentar tal desafio.

Além de ter que compor uma equipe partindo do zero, Maria terá de enfrentar vários outros desafios e dificuldades como:

- Adequar a atual infraestrutura de TI que é complexa e suporta toda a operação do banco atualmente;
- Conscientizar todos os colaboradores do banco sobre a importância do ITSCM para o crescimento do Banco Beta;
- Treinar os colaboradores da área de TI que apesar de conhecer o ITSCM não dominam o assunto;
- Propor ferramentas e processos que possibilitem a continuidade dos serviços de negócio;
- João solicita ainda que Maria cuide para que a transferência de conhecimento seja feita de eventuais fornecedores para a equipe interna de TI, o que obriga Maria ter que lidar, além de tudo, com o fator humano;

Maria identifica que os serviços essenciais do Banco Beta são conta corrente, crédito e cobrança bancária e decide então iniciar a implantação do ITSCM por esses serviços. Para isso, precisa se aproximar e convencer os coordenadores desses serviços, Lucas e Mariana, a aderirem à idéia.

Exposto o caso, temos a seguinte questão: Quais estratégias Maria precisa utilizar a fim de identificar as ameaças ao Banco Beta com as probabilidades e impactos para a construção de um plano que seja factível para resolver esse desafio?

3.2. Aplicação de técnicas para implantação de ITSCM no caso apresentado

No caso do Banco Beta, a primeira ação de Maria é se cercar de técnicas para identificação de ameaças e vulnerabilidades relacionadas aos serviços principais prestados pelo Banco: Cobrança Bancária, Crédito e Conta Corrente.

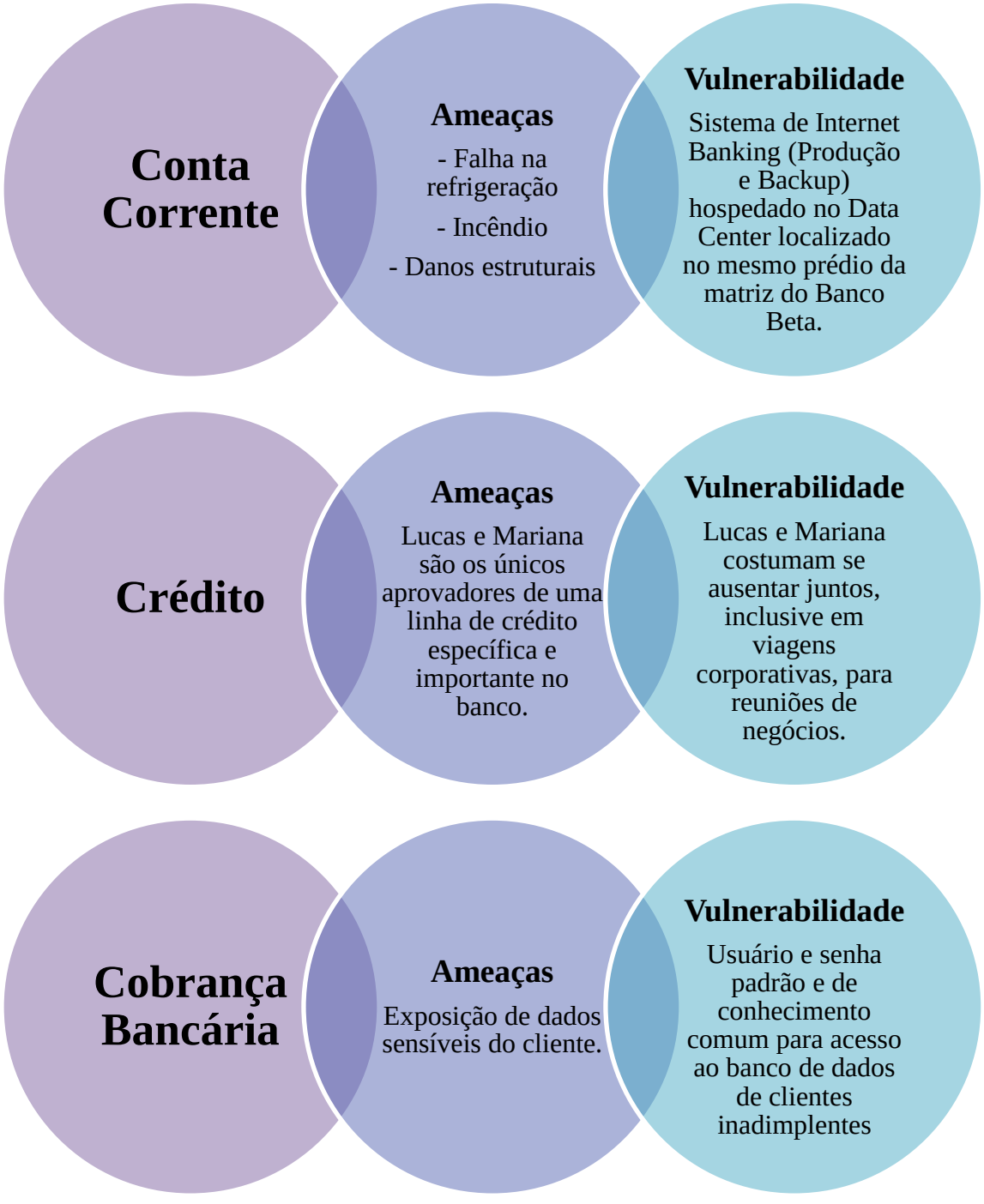
A princípio o ideal seria uma palestra para todos os colaboradores ligados aos principais serviços prestados e também para os cargos de gestão apresentando o projeto, sua importância, e até mesmo algumas noções de ITIL, a fim de conscientizar todos sobre a importância do ITSCM, afinal o ITIL, segundo [3], *"não é uma regra obrigatória a ser seguida, é um conjunto de recomendações baseadas em boas práticas de Gerenciamento de Serviços de TI"*. Assim os colaboradores teriam conhecimento da importância da inovação, da continuidade do negócio e da boa conduta durante a execução de suas respectivas atividades.

Como toda mudança gera naturalmente resistência e/ou receio nos envolvidos – que é a reação apresentada no primeiro momento por Lucas e Mariana, coordenadores dos serviços em questão – é importante que Maria envolva o uso de técnicas como *Brainstorming* com coordenadores e equipe, a fim de envolvê-los no projeto e ao mesmo tempo iniciar a identificação de ameaças que possam estar ligadas aos serviços coordenados por eles. Essa técnica, como tem o intuito de gerar idéias de forma não filtrada, além de trazer muita informação quebra parte da possível resistência existente nos colaboradores envolvidos.

Após a aplicação da técnica de *Brainstorming* Maria filtrou todas as idéias apresentadas e preparou um relatório com todas as considerações de ameaças identificadas pelos coordenadores Lucas e Mariana. Além disso, Maria fez o mapeamento detalhado de todos os processos relacionados aos serviços em questão junto com cada colaborador independente do cargo. Com isso, Maria conseguiu mapear e visualizar o cenário atual com todos os seus processos e procedimentos e conflitar com o resultado do *Brainstorming* realizado para identificar as ameaças.

Como Maria já carregava uma bagagem considerável de experiência e conhecimento adquiridos em projetos anteriores, ela pôde fazer um exercício de *Benchmarking* e comparar o resultado de suas análises com soluções de outras organizações em que ela atuou e que passaram por cenários similares. De acordo com [2], *"o Benchmarking consiste na pesquisa e conhecimento profundo de quem são os concorrentes do setor e como eles trabalham. É uma investigação contínua de comparação de produtos, serviços e práticas empresariais entre uma organização e seus concorrentes. A partir desse estudo é mais fácil entender o seu competidor e até prever qual será o próximo passo"*.

Feito tais exercícios Maria conseguiu identificar e relacionar ameaças e vulnerabilidades importantes e que estariam comprometendo a continuidade dos principais serviços prestados pelo Banco Beta, são elas:



Tendo relacionado as ameaças e vulnerabilidades dos principais serviços prestados pelo Banco Beta, Maria precisa identificar as probabilidades de ocorrência de tais ameaças e quais impactos o banco sofreria caso alguma delas viesse a ocorrer.

Vamos iniciar pela ameaça identificada para o serviço de conta corrente – considerado o principal serviço pelo fato aceitar transações fora do horário comercial – Maria identificou através de dados históricos que a manutenção nos equipamentos de ar condicionado do Data Center localizado no prédio da Matriz era feita de forma corretiva a cada 3 meses e que essa manutenção não tornou o serviço de conta corrente indisponível em nenhum momento, mas chegou perto disso, pois com o ar condicionado desligado para as manutenções ocorria o aquecimento das máquinas, e o risco das mesmas pararem de responder aumenta a medida que elas se aquecem. Para trabalhar com uma margem de erro na previsão de impactos se isso acontecesse Maria supôs que pudesse ocorrer indisponibilidade a cada dia de manutenção corretiva e considerou 4 dias no ano. Considerando um ano de 365 dias, Maria descobriu através de cálculos que a probabilidade de ocorrência dessa ameaça era de 1,09%, uma probabilidade considerada baixa.

Continuando ainda a falar de conta corrente, Maria identificou outras ameaças como incêndio ou outros danos estruturais, que nunca ocorreram, mas que não são impossíveis, e considerou a probabilidade de ocorrência baixa também. Mas, apesar de perceber a baixa probabilidade, notou que os impactos da falta de refrigeração, incêndio, ou danos estruturas seriam imensos, uma vez que Maria identificou que o Data Center contratado pelo Banco Beta, localizado em outro prédio da cidade, alocava o backup de todos os sistemas do Banco exceto a plataforma de Internet Banking, que tinha seu ambiente de produção e o seu backup alocados no mesmo Data Center localizado no prédio da matriz do banco. Maria descobriu, através de relatórios apresentados por Lucas e Mariana que o impacto causado pela indisponibilidade do Internet Banking seria de R$50.000,00 por dia.

Para esse serviço Maria sugeriu como plano de ação a manutenção preventiva semestral dos equipamentos de refrigeração do Data Center localizado no prédio da matriz, agendados em horários estratégicos fora do horário comercial e sugeriu também que o banco alocasse o backup do sistema de Internet Banking no Data Center contratado pelo Banco, dessa forma, se algo acontecer na matriz o banco tem como reestabelecer as atividades com segurança.

Tratando do serviço de crédito, Maria identificou que Lucas e Mariana são os únicos no banco responsáveis pela análise e aprovação de uma determinada linha de crédito muito importante para o banco e viu isso como uma ameaça para a continuidade desse serviço.

O que torna o banco vulnerável nessa questão é o fato de que Lucas e Mariana se ausentam juntos para reuniões e viagens curtas de negócio. Maria pensou que se algo acontecer no trajeto ou no local de destino ferindo a integridade física dos dois ao mesmo tempo tornaria a principal linha de crédito do banco indisponível ou com atrasos nas aprovações, já que para realizar esta atividade era importante uma análise bem feita para evitar aprovações errôneas e somente os dois eram treinados para isso. Outra opção seria passar a aprovação para cargos superiores (gerência ou direção), mas isso não resolveria já que os gerentes e diretores também têm suas atribuições e não conseguiriam se dedicar da mesma forma para a atividade.

Acidentes dessa maneira nunca aconteceram na história do banco. Maria então opta por avaliar a quantidade de acidentes aéreos e de rodoviários nos últimos 2 anos nos trechos em que Lucas e Mariana normalmente passavam. Maria, através de verificação de dados históricos, notou que não

aconteceu nenhum acidente aéreo e foram registrados 47 acidentes rodoviários entre ônibus e carros no perímetro avaliado.

Considerando somente os acidentes rodoviários registrados nos últimos 2 anos, Maria concluiu que a probabilidade de ocorrência dessa ameaça era de 6,44%, mas através de estudos dos relatórios do banco descobriu que o impacto da indisponibilidade dessa linha de crédito é de R$25.000,00 por dia.

Como plano de ação para essa atividade Maria propôs o treinamento de uma terceira pessoa para a realização da análise e aprovação dessa linha de crédito caso um dos dois coordenadores se ausente e, ao mesmo tempo, sugeriu que o banco adotasse medidas de segurança para Lucas e Mariana como evitar viagens compartilhando o mesmo carro, ônibus ou avião independente da distância e não terem períodos de férias coincidentes.

Quanto ao serviço de cobrança bancária Maria identificou uma ameaça interna que poderia trazer grandes prejuízos para o Banco Beta: a exposição de dados sensíveis dos clientes inadimplentes. Maria identificou durante o mapeamento dos processos que os analistas de banco de dados (DBAs) realizavam frequentemente acessos ao banco de dados de clientes inadimplentes utilizando usuário e senha padrão e de conhecimento comum.

Considerando que a equipe é formada por seis analistas e através de análise do histórico de acessos Maria notou que a equipe realizava acessos diários, ela considerou que a probabilidade de alguém da equipe roubar essas informações para vender ou fazer qualquer outro tipo de ação ilegal era próxima de 100% já que nunca se sabia quem estava acessando o banco e nem por qual motivo os acessos ocorriam e o não acontecimento dessa ameaça dependia única e exclusivamente da índole e bom senso de cada funcionário envolvido.

O impacto causado por essa ameaça é imenso já que se enquadra na Lei Geral de Proteção de Dados (LGPD) que aplica multas que variam de 2% do faturamento bruto até R$50 milhões por infração. Tendo em vista a possibilidade de tamanho prejuízo Maria sugere como plano de ação para essa ameaça a alteração do modo de acesso dos DBAs ao banco de dados, passando a fazer o uso de usuários nominais com senhas individuais e junto com isso implantar rígidos logs de auditoria para esses acessos.

Feito isso Maria já tinha informações suficientes para apresentar o projeto da implantação do ITSCM para os responsáveis do Banco Beta.

4. Resultados

Maria preparou uma apresentação com a tabela a seguir e informou que de acordo com cálculos baseados no lucro líquido do Banco Beta em relação ao investimento total para a implantação do ITSCM, o banco teria o retorno do investimento em até um ano após o término da implantação.

Serviço	Ameaça	Vulnerabilidade	Probabilidade	Impacto	Ação
Conta Corrente	- Falha na refrigeração - Incêndio - Danos estruturais	Sistema de Internet Banking (Ambiente de Produção e Backup) hospedado no Data Center localizado no mesmo prédio da matriz do Banco Beta	Calculada em 1,09% e considerada Baixa	R$50 mil por dia	Alocar o Backup do sistema de Internet Banking no Data Center contratado pelo Banco Beta
Crédito	Lucas e Mariana são os únicos aprovadores de uma linha de crédito específica e importante no banco	Lucas e Mariana costumam se ausentar juntos, inclusive em viagens corporativas, para reuniões de negócios	Calculada em 6,44% e considerada Baixa	R$25 mil por dia	- Treinar mais uma pessoa para realizar a análise e aprovação da linha de crédito em questão - Adotar medidas de segurança como: A) Lucas e Mariana não se deslocarem dividindo o mesmo meio de transporte independente da distancia B) não terem períodos de férias coincidentes.
Cobrança	Exposição de dados sensíveis do cliente inadimplente	Usuário e senha padrão e de conhecimento comum para acesso ao banco de dados de clientes inadimplentes	Estimada em um valor próximo de 100% e considerada Alta	Multas que variam de 2% do faturamento bruto até R$50 milhões (por infração)	- Acesso com usuário nominal e senha individual - Implantar rígidos logs de auditoria para acesso ao banco de dados

Analisando a tabela junto com a análise apresentada por Maria, os responsáveis pelo Banco Beta e pelos serviços essenciais por ele prestados não tiveram dúvidas e além de aprovar o plano, iniciaram a implantação do ITSCM.

Com o ITSCM o Banco conseguiu uma melhor e mais robusta estrutura, mais segurança para acompanhar o crescimento da demanda e também passou a ter uma melhor avaliação perante o BCB.

5. Conclusão

Após o estudo do caso do Banco Beta, apesar de se tratar de uma situação fictícia, é possível perceber a importância da implantação do ITSCM nas organizações. Além de dar mais segurança para o crescimento da empresa o Gerenciamento de Continuidade de Serviços baseados em Tecnologia da Informação proporciona a visão de ameaças que talvez não sejam possíveis de ser identificadas de forma natural e sem análises.

Um estudo de identificação de ameaças e vulnerabilidades bem realizado nos proporciona um melhor estudo de probabilidades e uma melhor análise de impactos e isso, com certeza, resultará em um plano de ação de sucesso.

Vivemos em um mundo que muda constantemente e a tecnologia avança a cada dia, por isso é importante a conscientização desses conceitos por parte das pessoas no cenário atual, pois colaboradores menos resistentes a grandes mudanças tendem a gerar idéias, sugestões e até mesmo ações de maior qualidade.

Podemos então afirmar que uma empresa com Gerenciamento de Continuidade de Serviços baseados em Tecnologia da Informação (ITSCM) devidamente implantado e funcionando apresenta melhor arquitetura e estrutura, traz mais segurança para seus clientes e colaboradores, é melhor avaliada pelos índices a ela relacionados e com certeza uma organização de sucesso.

6. Referências Bibliográficas

[1] D'ANDREA, E.; BATISTA, E.; JURICIC, M. **LGPD**: o que muda na prática com a Lei 13.709/18. Disponível em: https://www.pwc.com.br/pt/sala-de-imprensa/artigos/lgpd-muda-pratica-plc-53.html. Acesso em 21 de Abril de 2020.

[2] EQUIPE IBC. **O que é e como funciona o benchmarking?** 2020. Disponível em: https://www.ibccoaching.com.br/portal/o-que-e-e-como-funciona-o-benchmarking/. Acesso em 20 de Abril de 2020

[3] FREITAS, M. S. A. **Fundamentos do gerenciamento de serviços de TI**: preparatório para a certificação ITIL Foundation. 2. Ed. São Paulo: Brasport, 2013.

[4] GOMEDE, E. **Arquitetura de TI e modelos de negócios**: apresentação do caso. São Paulo, 2020.

[5] GOMEDE, E. **Arquitetura de TI e modelos de negócios**: roteiro de estudos. São Paulo, 2020.

[6] JANKOVSKI, I. **O que é ITSM (gerenciamento de serviços de TI)**: benefícios e melhores práticas de gerenciamento de serviços de TI. 2019. Disponível em: https://conteudo.movidesk.com/o-que-e-itsm/. Acesso em 17 de Abril de 2020.

[7] REVILLA, E. **O dilema da criatividade**. Ver. Adm. Empres. V. 59. N. 2. São Paulo, 2019. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-75902019000200149&lng=en&nrm=iso&tlng=pt. Acesso em 15 de Abril de 2020.