

**INSTITUTO FEDERAL GOIANO - CAMPUS CERES  
BACHARELADO EM SISTEMAS DE INFORMAÇÃO  
JONATHAN SILVESTRE SOUSA**

**PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO EM COOPERATIVAS DE  
CRÉDITO POR MEIO DO MODELO COBIT5**

**CERES - GO  
2019**

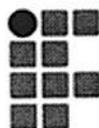
**JONATHAN SILVESTRE SOUSA**

**PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO EM COOPERATIVAS DE  
CRÉDITO POR MEIO DO MODELO COBIT5**

Trabalho de curso apresentado ao curso de Sistemas de Informação do Instituto Federal Goiano – Campus Ceres, como requisito parcial para a obtenção do título de bacharel em Sistemas de Informação, sob orientação do Prof. Dr. Marcos de Moraes Sousa.

**CERES - GO**

**2019**



**TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO**

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano, a disponibilizar gratuitamente o documento no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

**Identificação da Produção Técnico-Científica**

- |  |   |
|--|---|
| <input type="checkbox"/> Tese  | <input type="checkbox"/> Artigo Científico              |
| <input type="checkbox"/> Dissertação                                 | <input type="checkbox"/> Capítulo de Livro              |
| <input type="checkbox"/> Monografia – Especialização                 | <input type="checkbox"/> Livro                          |
| <input checked="" type="checkbox"/> TCC - Graduação                  | <input type="checkbox"/> Trabalho Apresentado em Evento |
| <input type="checkbox"/> Produto Técnico e Educacional - Tipo: _____ |   |

Nome Completo do Autor: Jonathan Silvestre Sousa

Matrícula: 2016103202030133

Título do Trabalho: Práticas de Segurança da Informação em Cooperativas de Crédito por meio do modelo cobit 5

**Restrições de Acesso ao Documento**

Documento confidencial:  Não  Sim, justifique: \_\_\_\_\_

Informe a data que poderá ser disponibilizado no RIIF Goiano:   /  /  

O documento está sujeito a registro de patente?  Sim  Não

O documento pode vir a ser publicado como livro?  Sim  Não

**DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA**

O/A referido/a autor/a declara que:

- o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

   29/10/2019  
Local Data

Jonathan Silvestre Sousa  
Assinatura do Autor e/ou Detentor dos Direitos Autorais

Ciente e de acordo:

    
Assinatura do(a) orientador(a)

#### ANEXO IV - ATA DE DEFESA DE TRABALHO DE CURSO

Ao(s) 22 dia(s) do mês de outubro do ano de dois mil e 19, realizou-se a defesa de Trabalho de Curso do(a) acadêmico(a) Jonathan Silvestre Sousa, do Curso de Sistema de informação, matrícula 206103202030133, cujo título é "Práticas de segurança da informação em cooperativas de crédito por meio do modelo COBIT 5". A defesa iniciou-se às 15 horas e 12 minutos, finalizando-se às 15 horas e 45 minutos. A banca examinadora considerou o trabalho aprovado com média 7.6 no trabalho escrito, média 7.8 no trabalho oral, apresentando assim média aritmética final 7.7 de pontos, estando o(a) estudante apto para fins de conclusão do Trabalho de Curso.

Após atender às considerações da banca e respeitando o prazo disposto em calendário acadêmico, o(a) estudante deverá fazer a submissão da versão corrigida em formato digital (.pdf) no Repositório Institucional do IF Goiano – RIIIF, acompanhado do Termo Ciência e Autorização Eletrônico (TCAE), devidamente assinado pelo autor e orientador.

Os integrantes da banca examinadora assinam a presente.

  
Assinatura Presidente da Banca

MARCOS DE MORAES SOUZA

  
Assinatura Membro 1 Banca Examinadora

Adriano Honorato Braga

  
Assinatura Membro 2 Banca Examinadora

Leonardo Paulo Arentes

## **AGRADECIMENTOS**

A Deus, em primeiro lugar, por ser a base de tudo na minha vida, me conduzir todos esses anos de faculdade e principalmente por concluir esse trabalho.

Aos meus pais, Eliane da Silva Silvestre Sousa e Maciel Carlos de Sousa, que sempre estiveram presentes me apoiando e me dando forças para que eu continuasse na luta durante essa etapa da minha vida.

Um agradecimento especial a minha filha Alice Ramos Silvestre Sousa e a minha esposa, Flávia Ramos de Sousa, que compartilhou comigo esse momento, foi muito paciente em minhas ausências e me ajudou bastante me dando dicas e apoio moral para o desenvolvimento deste e de todo os outros trabalhos da faculdade.

Agradeço também a toda minha família que sempre esteve presente nesta jornada, em especial aos meus avós, a minha madrinha e meu padrinho que sempre torceram por mim e me apoiaram.

Muito obrigado aos meus amigos e colegas da faculdade que sempre torceram por mim e me apoiaram no decorrer da faculdade.

Obrigado também ao Dr. Marcos de Moraes Sousa pelas cobranças no qual foram bastante produtivas e pelo apoio mútuo que foi dado entre nós na conclusão deste trabalho.

Enfim, um muito obrigado a todos que me apoiaram em mais esta jornada!

“Eu faço da dificuldade a minha motivação. A volta por cima vem na continuação.”

Chorão.

## RESUMO

Em virtude das condições mercadológicas crescentes, as instituições financeiras procuram melhorias e otimização em seus processos de controle internos da gestão de Tecnologia da informação (TI), com o intuito de diminuir os riscos de mercado e operacionais. Neste estudo, trata-se o grau de similaridade o qual a cooperativa estudada apresenta para a prevenção de riscos referente a segurança da informação. Para atingir o objetivo da pesquisa, realiza-se um estudo de caso, com procedimentos de gênero documental, qualitativa e descritiva. De acordo com os principais resultados obtidos, revela-se que a instituição estudada tem uma estrutura em período de crescimento. Entretanto, a mesma não se encontra completamente alinhado ao modelo estudado (Modelo COBIT5), ciente que este não é um modelo obrigatório, apenas recomendado às instituições financeiras pelo Banco Central do Brasil (BACEN). A instituição tem uma grande preocupação em manter um bom nível de eficiência e eficácia das operações, verificado em relatórios no qual foram apresentados.

**Palavras-chave:** Instituição Financeira. Governança em TI. Framework.

## **ABSTRACT**

Due to increasing market conditions, financial institutions are seeking improvements and optimization in their internal control processes of Information Technology (IT) management, in order to mitigate market and operational risks. This study deals with the level of compliance that the cooperative studied presents for the prevention of risks related to information security. To reach the objective of the research, a case study is carried out, with documental, qualitative and descriptive procedures. According to the main results obtained, it is revealed that the studied institution has a growing structure. However, it is not fully aligned with the studied model (COBIT5 Model), aware that this is not a mandatory model, only recommended to financial institutions by the Central Bank of Brazil (BACEN). The institution has a great concern to maintain a good level of efficiency and effectiveness of the operations, verified in reports in which they were presented.

**Keywords:** Financial institution. IT Governance. Framework.

## SUMÁRIO

1	INTRODUÇÃO . . . . .	9
2	REVISÃO BIBLIOGRÁFICA . . . . .	10
3	METODOLOGIA . . . . .	15
4	RESULTADOS . . . . .	18
5	CONCLUSÃO . . . . .	21
	REFERÊNCIAS . . . . .	22
	APÊNDICE A MODELO PARA SUBMISSÃO NA REVISTA BRASILEIRA DE SISTEMAS DE INFORMAÇÃO - ISYS . . . . .	24

# 1 INTRODUÇÃO

Atualmente, a Tecnologia da Informação (TI) tem-se tornado de suma importância para os negócios, de uma maneira que é difícil viver ou prosperar sem ela nas organizações. Constatase, simultaneamente pressões pela melhoria da governança nas organizações, o que requer mais da segurança das informações, bem como o maior comando e coordenação dos seus riscos.

As cooperativas de créditos estabelecem uma grande importância no cenário mundial e uma boa concepção no segmento da economia mundial. Conforme dados do *World Council of Credit Unions* (WOCCU), em 2017, as cooperativas de créditos abrangia um número de 89.026 distribuídas em 117 países, envolvendo ativos na ordem acima de 2 trilhões de dólares (WORLD COUNCIL, 2017).

Para poder amparar no desenvolvimento de gerência da segurança da informação, com dados confidenciais, principalmente ao se tratar de uma instituição financeira, há diversas normas e métodos de governança da Tecnologia da Informação. Constatase que as normas mais utilizadas e conceituadas no ramo para que haja uma implementação de qualidade em uma instituição são: ISO 27001, ITIL e o modelo COBIT (SUSANTO; ALMUNAWARAND; TUAN, 2011). Pelo fato de desenvolverem quesitos ou referências que procuram de alguma forma apoiar no gerenciamento de Segurança da Informação (SI), permitindo que as instituições possam acrescentar técnicas, conceitos, governança, dentre outros, no qual já consta traçados e implicados.

Referindo-se a uma instituição financeira, seus dados obtidos cotidianamente estão associados a gestão financeira e dados de seus clientes. Sendo assim, é necessário proteger as informações, pois estas são confidenciais, garantindo ao cliente que o serviço prestado apresenta vigor na sua organização e no seu funcionamento como um todo.

O trabalho proposto, tem como intuito, analisar se em uma organização onde utiliza de sistemas financeiros, e dados confidenciais de clientes, se existe uma preocupação e procedimentos que garantem a segurança dessas informações, e se estão sendo geridas da melhor maneira. Desse modo, foi feito um comparativo entre o modelo utilizado atualmente pela cooperativa e a norma escolhida para a pesquisa.

## 2 REVISÃO BIBLIOGRÁFICA

Desde a sua origem na Alemanha, em meados do século XIX, os pioneiros do cooperativismo de crédito vislumbraram na autogestão e na sua recíproca ajuda para oferecer aos agricultores e artesãos um custo mais barato em crédito (PINHEIRO, 2008). Como a possibilidade de juros e taxas mais baratas, as cooperativas se desenvolveram por toda a Europa e chegaram aos Estados Unidos (EUA) e ao Japão. No Brasil, apenas 50 anos depois foi estabelecida. A primeira cooperativa de crédito, no dia 28 de dezembro de 1902, no município de Nova Petrópolis (RS), pelo então padre jesuíta Theodor Amstadt (PINHEIRO, 2008).

A notoriedade crescente no qual as cooperativas de crédito está exercendo, chama atenção desde 2003, quando ocorreu a abertura oficial ao crédito cooperativo no Brasil, realizado com duas resoluções do Banco Central do Brasil: a de n 3.106 (25/06), onde houve apenas a inclusão para pequenos empresários, microempresários e microempreendedores utilizando cooperativas de crédito; resolução de n 3.140 (27/11), que possibilitou a inclusão de grandes empresários, para a utilização de cooperativas de créditos. (PINHO, 2004).

Segundo dados do Banco Central do Brasil (BACEN), em janeiro de 2019, existiam 928 cooperativas singulares de crédito autorizadas a funcionar no país. Dessas, 921 estavam em atividade, essa diferença deve-se a processo de incorporações, cancelamentos e outros.

Juntamente com um levantamento efetuado pelo Fundo Garantidor do Cooperativismo de Crédito (FGCOOP) em dezembro de 2018, as cooperativas de créditos detinham 6.219 unidades de atendimento em funcionamento (Pontos de atendimentos). Destacando a região Sul ocupando a liderança com 2.614 unidades, um percentual de 46,61% do total de unidades de atendimento, seguida pela região Sudeste com 1.998 unidades 35, 45%, já na terceira posição Centro Oeste com 476 unidades 8,49%, logo em seguida Nordeste com 311 unidades 5,55% e Norte 219 unidades 3,91%. Atualmente 10,5 milhões de brasileiros possuem conta em uma cooperativa de crédito.

A Segurança tem como finalidade proteger contra as adversidades, sendo estas de forma proposital ou não. Já a segurança da informação afirma que a sustentação desta proteção se acolhe na informação e em seus fundamentos imprescindíveis, como por exemplo os *softwares* e *hardwares* que utilizam, processam e agregam essas informações (WHITMAN; MATTORD, 2008).

O *Information Systems Audit and Control Association* (ISACA) relata que a segurança da informação tem que ser garantida dentro da instituição. Sendo assim, esta deve ser amparada

da disseminação a pessoas ou algo não autorizado (sigilo), das alterações não autorizadas (integridade) e sempre disponível quando solicitado por alguém autorizado. (disponibilidade) (ISACA, 2012).

A preservação e precaução da segurança da informação, visam certificar os princípios fundamentais da informação (NIST, 2002), esses são constituídos por: confidencialidade – somente partes autorizadas terão aquisição a esta informação, e essa está sujeita à descrição do modo de como será acessada e a escala do período em que o mesmo é adequado. É de suma relevância resguardar a informação, seja ela privada ou pessoal; Integridade – impossibilitar as alterações ou destruição desta informação alguém não autorizado, de forma a assegurar a veracidade desta informação sempre que a mesma for solicitada; e Disponibilidade – a utilização e o acesso da informação devem ser de confiança. Sempre disponíveis para as pessoas autorizadas. Uma das razões mais relevantes na segurança dessa informação e seus princípios essenciais, consiste na definição e formação de uma boa estrutura para uma governança de maneira eficiente (ISACA, 2010).

O controle da segurança da informação está concentrado no ato de monitorar, reunir e verificar elementos que estão relacionados como o mesmo, reforçando as estratégias de monitoração contínua ou de alguma avaliação independente de controles de proteção, por meio da finalidade de dimensionar a eficácia dos controles executados e preservado pelas instituições (ROUSE, 2009). No que se refere à análise da governança de segurança da informação, as instituições perceberam que é mais aconselhável efetivar um agrupamento de regras ou processos que são de reconhecimento internacional, ao invés de elaborarem regras ou até processos que aplicasse somente a sua respectiva instituição (SOLMS, 2005).

No âmbito da segurança da informação, existem várias opções, como por exemplo: normas da série ISO27000 – agrupamento de regras que auxiliam as instituições a preservar os ativos de informações seguros; *Committee of Sponsoring Organizations of the Treadway Commission* (COSO); lei *Sarbanes-Oxley* (SOX); *Information Technology Infrastructure Library* (ITIL); *Control Objectives for Information and related Technology* (COBIT); entre outros (ARORA, 2010). Essas normas definem os conceitos substanciais, elementos e partes da governança de segurança da informação. Além disso, também disponibilizam referências relevantes às instituições para a utilização adequada dessa mesma governança (KAJAVA et al., 2006).

O ISACA, em companhia do IT Governance Institute (ITGI), apresentou no ano de

1996 a primeira versão do modelo COBIT (SUSANTO; ALMUNAWARAND; TUAN, 2011). O modelo COBIT tem como principal fundamento ser um framework de controle que ampara as instituições a certificar o comprometimento do uso de Tecnologia da Segurança da Informação (TSI), dispondo os seus métodos dirigidos para atender às utilidades do mesmo (RIDLEY; YOUNG; CARROL, 2004).

De acordo com ITGI - IT Governance Institute (2007), o COBIT5 é a mais recente versão do *framework* de boas práticas de governança e gerenciamento empresarial de tecnologia, que engloba teorias e conceitos. Lançado em 2012, o COBIT 5 foi desenvolvido e integrado com base em 20 anos de desenvolvimento. O mesmo é constituído em torno de cinco princípios fundamentais:

- Satisfazer a necessidade dos elementos envolvidos;
- Envolver a instituição como um todo;
- Impor um framework integrado e único;
- Possibilitar uma visão holística;
- Separar governança do gerenciamento.

Segundo ITGI - IT Governance Institute (2007) além dos cinco princípios básicos o COBIT5 também apresenta sete facilitadores que se encontram separados por categorias, sendo elas: princípios e *frameworks*; pessoas suas capacidades e competência; políticas e processos; cultura, ética e condutas; estrutura organizacional; informação; serviço, infraestruturas e aplicações. Estes facilitadores foram determinados com a intenção de auxiliar a aplicação dos sistemas de governança e gestão de TSI, considerando a abrangência dos propósitos da instituição. Além dos cinco princípios e dos sete facilitadores já citados, o COBIT5 apresenta um agrupamento de trinta e sete processos. Os projetos de TI do COBIT são agrupados em quatro domínios.

Planejar e Organizar (PO): visa apenas na identificação sobre o que TI pode otimizar para alcançar as metas de negócios; Adquirir e Implementar (AL): para executar a estratégia de TI, é necessário identificar as soluções da mesma, para que estas sejam desenvolvidas, adquiridas, implementadas e integradas ao processo de negócios; Entregar e Apoiar (DS): Trata-se da entrega dos serviços no qual foram solicitados, que inclui a própria entrega de serviço, gerenciamento da proteção e a continuidade, serviços de apoio aos usuários e gerenciamento de dados e recursos operacionais; Monitorar e Avaliar (ME): aborda o gerenciamento de seu funcionamento, o acompanhamento do controle interno, aderência regulatória e a governança.

Como determina o ITGI - IT Governance Institute (2007, p.19),

"o modelo de maturidade para o gerenciamento e controle dos procedimentos de tecnologia da informação é baseado num método de avaliar a organização, permitindo que esta seja pontuada de um nível de maturidade não existente (0) a otimizado (5)".

Os níveis são evidenciados no quadro a seguir.

Quadro 1 – Níveis de Maturidade da instituição

1) Inicial/ <i>Ad hoc</i>	Existem evidências de que a empresa reconheceu que existem questões e que precisam ser trabalhadas. No entanto, não existe processos padronizado; ao contrário, existem enfoques <i>ad hoc</i> que tendem a ser aplicados individualmente. O enfoque geral de gerenciamento é desorganizado.
2) Repetível, porém intuitivo	Os processos evoluíram para um estágio em que procedimentos similares são seguidos por diferentes pessoas que fazem a mesma tarefa. Não existe um treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixada com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e, conseqüentemente, erros podem ocorrer.
3) Processo definido	Procedimentos foram padronizados, documentos e comunicados por meio de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serem detectados. Os procedimentos não são sofisticados, mas existe a formalização das práticas existentes.
4) Gerenciado e mensurável	A gerência monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão sob constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.

Quadro 1 – Níveis de Maturidade da instituição

5) Otimizado	Os processos foram refinados a um nível de boas condutas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade, como em outras organizações. TI é utilizada como o caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e a efetividade, tornando a organização rápida em adaptar-se.
--------------	---

Fonte: Adaptado pelos autores, a partir de ITGI (2007, p.21).

### 3 METODOLOGIA

No que diz respeito a abordagem do problema, este estudo se classifica como qualitativa em função da análise dos dados não envolver mecanismos estatísticos como base do processo de estudo do problema. De acordo com Beuren (2013, p.92) “na pesquisa qualitativa concebem-se análises mais profundas em relação ao fenômeno que está sendo estudado”. Deste modo, esta pesquisa considerou sob os focos qualitativos os controles internos relativos à segurança da informação de uma cooperativa de crédito, verificando e comparando às normas do modelo COBIT e à literatura especializada.

De acordo com os propósitos desse estudo, a pesquisa se caracteriza como descritiva, pois descreve os principais aspectos para as seguranças informacionais utilizados na instituição de estudo. Conforme Gil (2008), esse tipo de estudo visa à divulgação da existência de associações entre variáveis.

A Pesquisa tem como lócus uma cooperativa de crédito do interior goiano, em que atua na região há vinte e seis anos e é considerada uma cooperativa de grande porte, vinculada a área financeira. Foi pesquisado o âmbito de segurança da informação, assegurando ser um parecer do sistema de gestão e não sendo uma avaliação de forma técnica. Cujas sua intenção foi verificar se na instituição onde trata de dados financeiros confidenciais de clientes, existe um processo que possa garantir a segurança da informação. Dessa maneira, foi feita a escolha da norma (COBIT5) a ser utilizada como base neste estudo.

Iniciou-se um confronto entre as diretrizes utilizadas no modelo COBIT5 e o que estava sendo colocado pela instituição, da qual, este último informe seria obtido por meio de uma entrevista com alguns colaboradores da instituição em análise.

Decidiu-se, pelo *framework* COBIT5, por o mesmo demonstrar um aspecto de forma extensa da gestão e governança da instituição, efetuando uma conexão com áreas opostas e a segurança da informação. Entretanto, devido a dimensão que o modelo COBIT5 apresenta, optou-se por diminuir seu plano de estudo a quatro facilitadores, sendo eles: Processos; Princípios, Políticas e *Frameworks*; Estrutura Organizacional; e Informação (SANTOS; IPP, 2014).

O facilitador Processos é um dos que se definiu no confronto realizado entre a instituição e norma. A estrutura desta análise interfere-se na imposição de alcançar uma compreensão referente a conquista das metas propostas pela instituição.

No que diz a respeito à escolha de adicionar o facilitador Princípios, Políticas e *framework*

na pesquisa desenvolvida, com principal foco na política e princípios sugeridos, sendo que esses mecânicos são os que garantem as estruturas administrativas relatar as regras que servirão de apoio para a conquista dos intuítos e das recomendações específicas, demonstrando como colocá-las em prática. Diante disso, optou-se uma parte da pesquisa na assimilação aos tipos de orientações e regras que se deparam documentadas na instituição.

O facilitador Estruturas Organizacionais, foi estabelecido com um dos pontos principais da pesquisa, já que, as mais diversas práticas e funções realizadas garantem a instituição atingir um resultado positivo, referindo-se a boas decisões.

Por fim, utilizou-se o facilitador Informação, considerado um método indispensável para todas as instituições. Com o propósito de analisar se o conhecimento da segurança da informação está presente na instituição, e os possíveis *stakeholders* que estão ligados diretamente ou indiretamente com a mesma.

Deste modo, após a seleção do ponto escolhido nesta pesquisa, foi iniciado o contato com a cooperativa escolhida, para posteriormente coletar as informações para executar a avaliação programada. Para o recolhimento dessas informações, passou-se a compreender a perspectiva dos colaboradores escolhidos, onde eles contam com uma grande presença no que diz a respeito de gestão da informação na cooperativa. Deste modo, foi escolhida a entrevista como um procedimento na qual possibilita a obtenção dessas informações, para posteriormente realizar o tratamento adequado dos dados obtidos.

Primeiramente foi iniciado o contato com a cooperativa de crédito escolhida, para posteriormente iniciar a comunicação com o departamento de tecnologia, que é um dos principais responsáveis pela gestão da segurança da informação. Logo em seguida, foi direcionado o contato com o analista de tecnologia e o assistente de tecnologia do departamento, por estes demonstrarem a visão geral da gestão de sistemas da informação e tecnologia, como alguns procedimentos e práticas, que são executados nessa área. O mesmo também apresenta um vasto entendimento da instituição em estudo. Foi possível assim, a cooperação do analista e assistente de tecnologia, que concordaram colaborar na realização desta pesquisa. Posteriormente foi efetuado a entrevista com o departamento de controle interno, por este ser responsável pelo controle das gestões de acessos e conformidades aos colaboradores da cooperativa, além de serem considerados departamentos de grande relevância para o estudo.

Ao decorrer da pesquisa na instituição, foram realizadas diversas conversas informais e uma entrevista aos colaboradores atuantes no departamento de tecnologia. Na qual foram

efetuadas algumas perguntas, sendo elas: quais são as normas utilizadas pela cooperativa de crédito?; como funciona o sistema de controle de acessos da cooperativa ?.

Deste modo, também foi solicitado e analisado junto ao departamento de tecnologia e o departamento de controle interno alguns documentos, que foram de fundamental importância para o estudo, sendo eles: Relatório de acesso ao Sisbr 2.0 (conjunto de aplicativos que efetua o controle administrativo e financeiro da cooperativa) no qual boa parte dos colaboradores utiliza para exercer sua rotina de trabalho; também foi analisado o funcionamento da PSI da cooperativa.

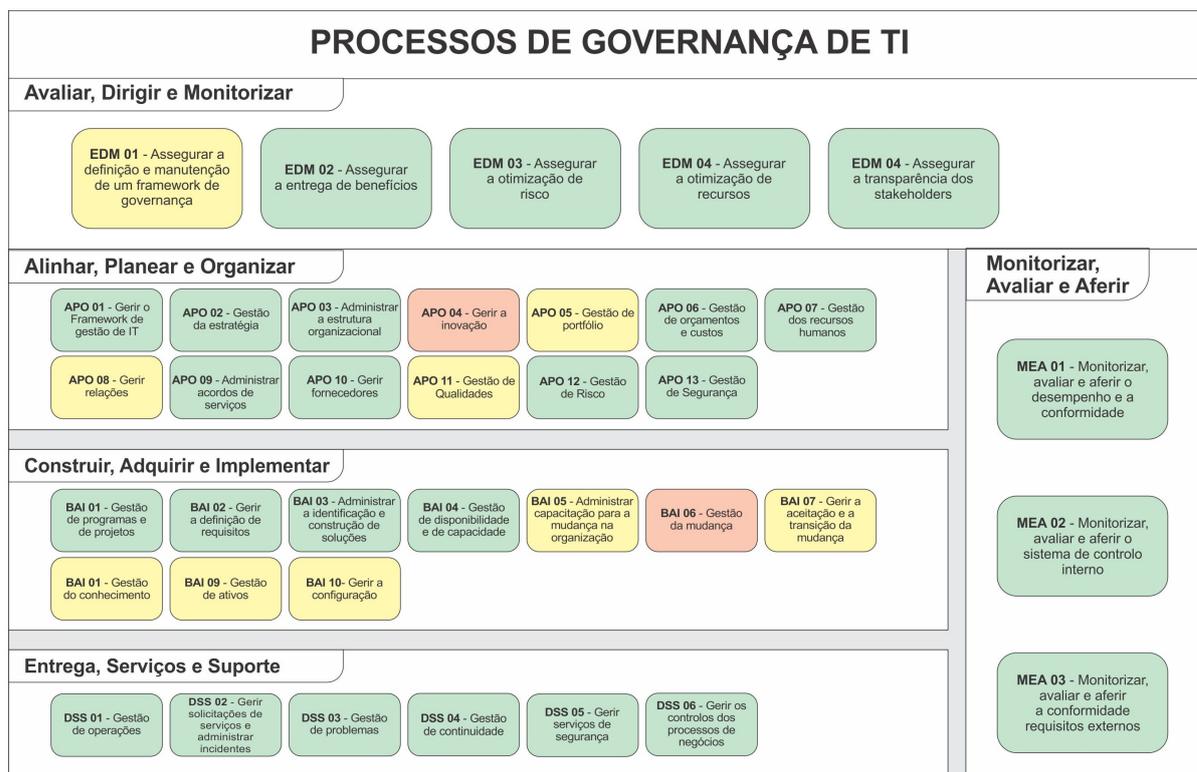
## 4 RESULTADOS

Foi desenvolvido um estudo em uma cooperativa de crédito, sendo uma empresa particular, a qual está vinculada a atividades financeiras. Como já descrito, o COBIT5 demonstra uma grande amplitude no que se refere a gestão e governança de tecnologia, sendo a norma utilizada para realização deste caso de estudo. As dúvidas realizadas, permitiram analisar quais são as orientações que atingem melhor a instituição, desta forma propiciando perceber qual nível de coincidência em que a mesma estaria com o *framework* COBIT5, nas condições analisadas. A princípio foram recolhidos alguns pontos como forma de confronto entre o modelo escolhido na pesquisa e a Política de Segurança Interna (PSI) da cooperativa.

O estudo verificou os mecanismos de segurança da informação e do controle interno, comparando com literaturas especializadas, como a realidade da instituição financeira, considerando a prevenção de riscos com seus dados e afins. Para isto, foi analisado políticas internas da cooperativa escolhida e comparadas com modelos preceituados pela literatura segurança da informação utilizando o *framework* de gestão de Tecnologia da Informação (COBIT5), formalizando-se um estudo comparativo dos documentos que foram coletados sob a base qualitativo, por meio do método descritivo.

Verificou-se então o facilitador Processos, para analisar se os mesmos estavam presentes e implantados na instituição, em que também foi avaliado qual etapa de implementação o mesmo estaria (figura 1). Por tanto, foi utilizado para apoio a escala do modelo *Capability Maturity Model Integration* (CMMI), visto que este agrega à otimização de procedimentos, desenvolvimento e conservação de produtos e serviços. Modelo CMMI aplica-se em 5 níveis sendo eles: Inicial - Processos são imprevisíveis, pouco controlado e reativos; Gerenciado - Processos são caracterizados por projetos e as ações são frequentemente reativas; Definido - Processos são caracterizados para organização e são proativos; Quantitativamente Gerenciado - Processos são medidos e controlados; Otimização - Foco contínuo na melhoria dos processos (CLINCH, 2009).

Figura 1 – Processos de Governança de TI



Fonte: Adaptado pelos autores, a partir de (ISACA, 2012).

Em uma avaliação geral de todos os procedimentos sugeridos pelo modelo COBIT5, nenhuma das fases presentes na figura 1 se obtêm em sua perfeita otimização, em que nove desses processos (representado pela cor amarela), foram classificados como já analisados alguma vez, ou ciente pela gestão da cooperativa; dois não estudados ou não adaptados pela instituição (representado pela cor vermelho); e os vinte e seis restante já se encontram ajustados (representado pela cor verde). Esta análise do controle de processos em comparação ao modelo COBIT5 pode ser utilizado pela cooperativa para definir quais são os procedimentos que carecem em serem melhorados ou aos que precisam de um aperfeiçoamento da mesma.

Referindo-se as estruturas organizacionais, foi identificado que a maior parte das práticas de segurança, solicitações de acessos ou funções, passam por uma autorização da Diretoria executiva, porém segundo Krag (2006) recomenda-se a criação de um comitê de segurança da informação (ISSC - *Information Security Steering Committee*), podendo incluir como membros como Diretoria executiva ou designados, chefe de informação (CIO - *Chief Information Officer*), Executivo-chefe de Segurança da informação (CISO - *Chief Information Security Officer*). Por fim pelo do facilitador Informação, foi identificado que a cooperativa também se aplica muito bem a este facilitador, com algumas informações, estratégias da segurança da informação

e estimativas de segurança, em que se encontravam documentadas em atas e relatórios apresentados pelo analista de controle interno da instituição. Embora esses documentos não se encontravam de forma individual, ou seja o documento era existente porém estava junto de outros normativos ou arquivos. Apesar de não ser da forma na qual o modelo COBIT5 aconselha, o modo de como a instituição faz a abordagem aos diversos tipos de informação consideráveis à área de segurança da informação indica não precisar de tratamento.

## 5 CONCLUSÃO

De acordo como Modelo de maturidade citado no capítulo 2 – Auxílio da TI pela escala de maturidade do COBIT, que pertence ao subprocesso APO 13 (Gestão de Segurança), a instituição estudada se classificaria como “processo definido” (nível 3) pois, segundo ITGI - IT Governance Institute (2007, p.42), “a Direção está a par da importância do plano de infraestrutura tecnológica. Há treinamento forma e comunicação de papéis e responsabilidades”.

Foi possível constatar, que na cooperativa de crédito situada no interior goiano, existe muita preocupação em garantir que as suas informações e de seus clientes estejam bem protegidas. No estudo é possível verificar que a cooperativa tem controle no que se trata de procedimentos recomendados do modelo COBIT5, um *framework* extenso no que se refere a gestão e governança. Também demonstra o fato, que a segurança da informação é um assunto de suma relevância para a instituição em análise, pois se encontra a elaborar controles, processos e práticas no qual permite que a sua informação seja protegida.

Apesar das limitações do presente estudo, o mesmo apresenta uma contribuição para amplificar o conjunto de publicações de estudos e dados, sobre métodos de conservação a direção de suas informações financeiras, ao propósito de evitar riscos ao ramo e conservar a segurança em suas atividades. Recomenda-se que a instituição sempre procure se aperfeiçoar em seus métodos.

O ideal é que a instituição procure sempre melhorar e se aperfeiçoar. Neste caso, sugere-se que a cooperativa de crédito encontre formas de alcançar o nível de maturidade 4 (gerenciado e mensurável), pois segundo ITGI - Governance Institute (2007) é o nível onde a gerência obtém o controle sobre os processos, onde os mesmos podem não estar funcionando adequadamente, porém estão em constante aprimoramento. Utilizando ferramentas adequadas, maior controle de adesão dos procedimentos que são aplicados, procurando encontrar maneiras para sanar ou diminuir as falhas.

Sugere-se para futuros estudos uma pesquisa qualitativa a respeito dos riscos que cercam a segurança da informação em cooperativas de crédito, com vista em aprofundar a análise de práticas de governança em tecnologia utilizando outros *frameworks* de gestão, já citados, conservando os controles e a segurança da informação atualizados em conformidade com a área da empresa e ao avanço do mercado.

## REFERÊNCIAS

ARORA, V. Comparing different information security standards: COBIT vs. ISO 27001. 2010.

BEUREN, I. M. **Como elaborar trabalhos monográficos em Contabilidade: teoria e prática**. São Paulo: [s.n.], 2013. v. 3ª ed.

CLINCH, J. ITIL v3 and information security. **Clinch Consulting White Paper**, n. May, p. 1 – 40, 2009. Disponível em: <[http://www.apmg-library.org/Player/eKnowledge/itil{\\\_}v{\\\_}and{\\\_}information{\\\_}](http://www.apmg-library.org/Player/eKnowledge/itil{\_}v{\_}and{\_}information{\_})>.

GIL, A. C. **Métodos e Técnicas de Pesquisa Social**. São Paulo: [s.n.], 2008. v. 6ª ed.

ISACA. **Certified Information Systems Auditor**. [S.l.], 2010.

ISACA. COBIT 5 for Information Security. 2012. Disponível em: <<https://m.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf>>.

ITGI - IT GOVERNANCE INSTITUTE. **COBIT 4.1**. Rolling Meadows: [s.n.], 2007.

KAJAVA, J. et al. Information Security Standards and Global Business. 2006.

KRAG, B. **Guidance for Boards of Directors and Executive Management**. [S.l.: s.n.], 2006. 52 p. ISBN 1933284293.

NIST. Federal Information Security Management Act of 2002. **National Institute of Standards and Technology**, p. 48–63, 2002.

PINHEIRO, M. A. H. Cooperativas de Crédito História da evolução normativa no Brasil. 2008.

PINHO, D. B. P. **O cooperativismo de crédito no Brasil: do século XX ao século XXI**. Santo André: [s.n.], 2004.

RIDLEY, G.; YOUNG, J.; CARROL, P. COBIT and its Utilization: A framework from the literature. **Hawaii International Conference on System Sciences**, 2004.

ROUSE, M. A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. **Indian Journal of Science and Technology** 5., 2009.

SANTOS, S. M.; IPP, I. Práticas de Segurança da Informação num Centro Hospitalar. n. Capsi 2014, p. 272–290, 2014.

SOLMS, B. V. Information Security governance: COBIT or ISO 17799 or both? **Computers & Security**, n. 24, p. 99–104, 2005.

SUSANTO, H.; ALMUNAWARAND, M. N.; TUAN, Y. C. Information Security Management. 2011.

WHITMAN, M.; MATTORD, H. Principles of Information Security. 2008.

WORLD COUNCIL. **WORLD COUNCIL OF CREDIT UNIONS - STATISTICAL REPORT**. [S.l.], 2017. Disponível em: <[https://www.woccu.org/our{\\\_}network/statrep](https://www.woccu.org/our{\_}network/statrep)>.

**APÊNDICE A – MODELO PARA SUBMISSÃO NA REVISTA BRASILEIRA DE  
SISTEMAS DE INFORMAÇÃO - ISYS**

## Instructions for Authors of iSys Articles

**Title: If the article is written in Portuguese, then place the title in English here**

**Author 1 Full Name<sup>1</sup>, Author 2 Full Name<sup>2</sup>, ..., Author N Full Name<sup>1</sup>**

<sup>1</sup>Department/Institute name – University name (Acronym)  
City, State/District – Country

<sup>2</sup> Department/Institute name – University name (Acronym)  
City, State/District – Country

<sup>N</sup> Department/Institute name – University name (Acronym)  
City, State/District – Country

{local-part-1, local-part-n}@domain, local-part-2@domain, e-mailx

**Abstract.** *This template describes the style to be used in articles for iSys – Brazilian Journal of Information Systems. For papers in English, you should add just an abstract while for the papers in Portuguese, we also ask for an abstract in Portuguese (“resumo”). In both cases, abstracts should not have more than 10 lines and must be in the first page of the paper.*

**Keywords.** *Add from 3 to 7 title-cased keywords, separated by semi-colon.*

**Resumo.** *Este modelo descreve o estilo a ser usado na confecção de artigos para publicação na iSys – Revista Brasileira de Sistemas de Informação. É solicitada a escrita de resumo e abstract apenas para os artigos escritos em português. Artigos em inglês deverão apresentar apenas abstract. Nos dois casos, o autor deve tomar cuidado para que o resumo (e o abstract) não ultrapasse(m) 10 linhas (cada), sendo que ambos devem estar na primeira página do artigo.*

**Palavras-Chave.** *Se o artigo for escrito em português, acrescente de 3 a 7 palavras-chave com a inicial em maiúsculo, separadas por ponto-e-vírgula.*

### 1. General Information

To avoid unnecessary errors, you are strongly advised to use the 'spell-check' and 'grammar-check'. We ask that authors follow the guidelines explained in this template, to achieve the highest quality possible and a standard presentation of the manuscripts of the journal. Be advised that manuscripts in a technically unsuitable form may be rejected anytime by the editors or reviewers.

All articles submitted to iSys should be written in English or in Portuguese. The format paper should be A4 with single column, 3.5 cm for upper margin, 2.5 cm for bottom margin and 3.0 cm for lateral margins, without headers or footers. The main font must be Times, 12 point nominal size, with 6 points of space before each paragraph.

As it is an Information Systems (IS) journal, it is expected the work is supported by IS theories, deals with innovative technology artifacts and correctly follows a scientific methodology, presenting novel contributions to the state-of-the-art of the area. We also welcome systematic reviews that include clear research questions, a critical analysis, and directions for new challenges in the area. There is no limit of number of pages for the manuscript, although usually it ranges from 15-30 pages.

## 2. First Page

The first page must display the paper title (if the article is written in Portuguese, then the “Title:” followed by the title in English is also mandatory), the name and address of the authors, the abstract and keywords in English, and “resumo” and “palavras-chave” in Portuguese (“resumos” and “palavras-chave” are required only for papers written in Portuguese). The title must be centered over the whole page, in 16 point boldface font and with 12 points of space before itself. Author names must be centered in 12 point font, bold, all of them disposed in the same line, separated by commas and with 12 points of space after the title. Addresses must be centered in 12 point font, also with 12 points of space after the authors’ names. E-mail addresses should be written using font Courier New, 10 point nominal size, with 6 points of space before and 6 points of space after.

The abstract and “resumo” (if it is the case) must be in 12 point Times font, indented 0.8cm on both sides. The word **Abstract** and **Resumo**, should be written in boldface and must precede the text. The keywords and “palavras-chave” (if it is the case) must follow the abstract and “resumo”, respectively, be in 10 point Times font, indented 0,8 on both sides, with 6 points of space before and 12 points of space after. The word **Keyword** and **Palavras-chave**, should be written in boldface and must precede the text.

## 3. Sections and Paragraphs

Section titles must be in boldface, 13pt, flush left. There should be an extra 12 pt of space before each title. Attention to the section numbering. The first paragraph of each section should not be indented, while the first lines of subsequent paragraphs should be indented by 1.27 cm.

### 3.1. Subsections

The subsection titles must be in boldface, 12pt, flush left.

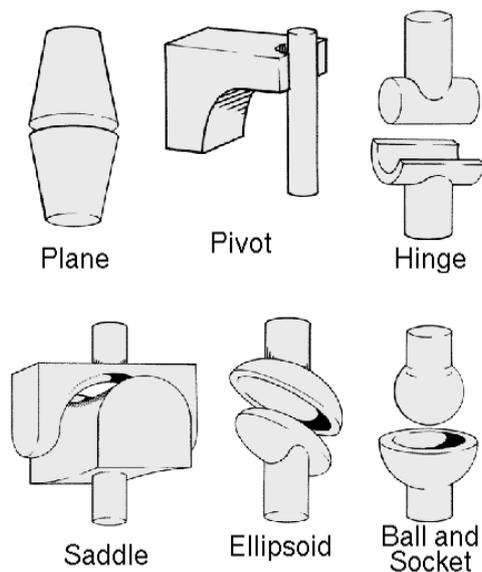
## 4. Figures and Captions

Figure and table captions should be centered if less than one line (Figure 1), otherwise justified and indented by 0.8cm on both margins, as shown in Figure 2. The caption font must be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.



*"No, you weren't downloaded.  
Your were born."*

**Figure 1. A typical figure**



**Figure 2. This figure is an example of a figure caption taking more than one line and justified considering margins mentioned in Section 5.**

In tables, try to avoid the use of colored or shaded backgrounds, and avoid thick, doubled, or unnecessary framing lines. When reporting empirical data, do not use more decimal digits than warranted by their precision and reproducibility. Table caption must be placed before the table (see Table 1) and the font used must also be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

**Table 1. Variables to be considered on the evaluation of interaction techniques**

	Chessboard top view	Chessboard perspective view
Selection with side movements	6.02 ± 5.22	7.01±6.84
Selection with in-depth movements	6.29±4.99	12.22±11.33
Manipulation with side movements	4.66± 4.94	3.47±2.20
Manipulation with in-depth movements	5.71 ±4.55	5.37 ±3.28

## 5. Images

Images and illustrations may be colorful, but attention to the possibility of black-and-white, or gray tones, print. The image resolution on paper should be about 600 dpi. Do not include images with excessive resolution, as they may take hours to print, without any visible difference in the result.

## 6. Submission instructions

Fill up the metadata information with the most complete data possible as some indexing entities require detailed information and also for helping us to organize the journal data. Notice that if the paper is written in Portuguese, it is necessary to fill up the metadata in both languages (English and Portuguese).

Start with information for each author. Please provide the information according to the order of the authors. Although it is possible to reorganize the order, sometimes the system does not work well on performing reordering. Avoid shortening middle names (as it may make harder to identify other publications of the same author). In the URL field, choose to fill in with the curriculum URL (for those who have a [Lattes curriculum](#), please fill in with the address to access the CV). Add the current affiliation of each author and fill in the country where the author works. Click on the “Add Author” button for adding other author, if that’s the case.

Add the Title and Abstract of the manuscript. Attention to the “Form language” on the top of the form. If the manuscript is in English, then provide the title and abstract information in English. If the manuscript is written in Portuguese, then it is necessary to fill the title and abstract also in English. In this case, just change the form language on the top of the form and fill in the corresponding information. Notice the “Form language” is related to the information that is filled in the metadata. It does not change the language of the page.

For “Academic discipline”, please consider the system suggestions, filling in the ones are related to the manuscript. For “Keywords”, the authors are free to choose all the terms they consider important to indexing the manuscript. If the work is related to a specific geo-spatial area, please, provide the corresponding information in “Geo-spatial

coverage”. Information about the research sample characteristics must be provided in the “Research sample characteristics” field. The research type, method and approach must be filled in the “Type, method or approach” field. The language field is related to the manuscript language. Therefore, this field is the same regardless of the form language. Attention to use semi-colon “;” to separate terms in each field of the indexing information.

Information about the contributors and supporting agencies must also be filled in the submission metadata. In case of approval, the authors may also add this information on the final version of the manuscript (usually it is added at the acknowledgement section). Again, attention to the “Form language”. If the manuscript is in Portuguese, the authors are also required to fill in the metadata in English as in the title and abstract.

Provide a formatted list of references for works cited in the manuscript and separate individual references with a blank line. This field is the same regardless of the form language. Notice we follow the active link procedure, which is highly recommended to also include on the article. Then, when generating the PDF file, make sure the hyperlinks are active.

## **Acknowledgement**

This template is based on the Brazilian Computer Society (SBC) template for papers.

## **References**

Bibliographic references must be unambiguous and uniform. We recommend giving the author names references in brackets, e.g. [Knuth 1984], [Boulic and Renault 1991]; or dates in parentheses, e.g. Knuth (1984), Smith and Jones (1999).

The references must be listed using 12 point font size, with 6 points of space before each reference. The first line of each reference should not be indented, while the subsequent should be indented by 0.5 cm.

Whenever possible, include the links to the references (URL, DOI and Google Scholar link):

### **A. When the reference has a Link**

- Make a clickable link on the respective URL (if you are using MS-Word, use the tool Insert Hyperlink, informing the URL).

### **B. Allow readers to search for the reference on Google Scholar**

- Copy the title of the reference and put in between “%22”, including the “+” character between each word: <http://scholar.google.com/scholar?q=%22PASTE+TITLE+HERE%22&hl=en&lr=&btnG=Search>
- If it is a common title, you may add the author, such as in:  
<http://scholar.google.com/scholar?q=PASTE+AUTHOR+HERE+%22PASTE+TITLE+HERE%22&hl=en&lr=&btnG=Search>
- Or you may use the publication year (YEAR) to restrict the results, such as in:  
<http://scholar.google.com/scholar?q=PASTE+AUTHOR+HERE+%22PASTE+TITLE+HERE%22&hl=en&lr=&btnG=Search>

E+TITLE+HERE%22&hl=en&lr=&btnG=Search  
&as\_ylo=YEAR&as\_yhi=YEAR

- It is highly advisable to confirm if the link is correct (and if Google Scholar presents a correct result).
- Include the term “[GS SEARCH]” at the end of each reference and make “GS SEARCH” a hyperlink with the URL just created.

### C. Allow readers to access references with DOI

- Add “doi:” followed by the DOI number. Then, make the DOI number a hyperlink using the corresponding URL (the URL can be created adding “http://doi.org/” in front of the DOI number).

### D. Allow readers to access references with DOI

- Add “doi:” followed by the DOI number. Then, make the DOI number a hyperlink using the corresponding URL (the URL can be created adding “http://doi.org/” in front of the DOI number).

Boulic, R. and Renault, O. (1991) “3D Hierarchies for Animation”, In: *New Trends in Animation and Visualization*, Edited by Nadia Magnenat-Thalmann and Daniel Thalmann, John Wiley & Sons Ltd., England. [[GS Search](#)]

Dyer, S., Martin, J. and Zulauf, J. (1995) “Motion Capture White Paper”, [ftp://ftp.sgi.com/cgi/A%7CW/jam/mocap/MoCapWP\\_v2.0.html](ftp://ftp.sgi.com/cgi/A%7CW/jam/mocap/MoCapWP_v2.0.html), December.

Holton, M. and Alexander, S. (1995) “Soft Cellular Modeling: A Technique for the Simulation of Non-rigid Materials”, *Computer Graphics: Developments in Virtual Environments*, R. A. Earnshaw and J. A. Vince, England, Academic Press Ltd., p. 449-460. [[GS Search](#)]

Knuth, D. E. (1984), *The TeXbook*, Addison Wesley, 15<sup>th</sup> edition.

Pawlak, Z. (1981). Information systems theoretical foundations. *Information Systems*, 6(3), 205-218. doi: [10.1016/0306-4379\(81\)90023-5](https://doi.org/10.1016/0306-4379(81)90023-5) [[GS Search](#)]

Smith, A. and Jones, B. (1999). On the complexity of computing. In *Advances in Computer Science*, pages 555–566. Publishing Press. [[GS Search](#)]