Information Systems and Technology Management 2

Marcos William Kaspchak Machado
(Organizador)

Atena Editora
Ano 2019

Marcos William Kaspchak Machado

(Organizador)

Information Systems and Technology Management 2

Atena Editora
2019

2019 *by Atena Editora*

Editora Chefe: Profª Drª Antonella Carvalho de Oliveira
Diagramação e Edição de Arte: Lorena Prestes e Karine de Lima
Revisão: Os autores

Dados Internacionais de Catalogação na Publicação (CIP)
(eDOC BRASIL, Belo Horizonte/MG)

I43 Information systems and technology management 2 [recurso eletrônico] / Organizador Marcos William Kaspchak Machado. – Ponta Grossa (PR): Atena Editora, 2019. – (Information Systems and Technology Management; v. 2)

Formato: PDF
Requisitos do sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
ISBN 978-85-7247-202-9
DOI 10.22533/at.ed.029191903

1. Gerenciamento de recursos de informação. 2. Sistemas de informação gerencial. 3. Tecnologia da informação. I. Machado, William Kaspchak. II. Série.

CDD 658.4

Elaborado por Maurício Amormino Júnior – CRB6/2422

APRESENTAÇÃO

A obra denominada "*Information Systems and Technology Management*" contempla dois volumes de publicação da Atena Editora. O volume II apresenta, em seus 26 capítulos, um conjunto de estudos sobre a aplicação da gestão do conhecimento aos processos de gestão organizacional, operacional e de projetos.

As áreas temáticas de gestão organizacional e de projetos mostram a importância da aplicação dos sistemas de informação e gestão do conhecimento na cultura organizacional e no desenvolvimento de novos projetos.

Este volume dedicado à aplicação do conhecimento como diferencial competitivo para inovação em processos produtivos, traz em seus capítulos algumas aplicações práticas de levantamento de dados, gestão da cultura e governança empresarial, além de ferramentas de monitoramento da qualidade da informação.

Aos autores dos capítulos, ficam registrados os agradecimentos do Organizador e da Atena Editora, pela dedicação e empenho sem limites que tornaram realidade esta obra que retrata os recentes avanços científicos do tema.

Por fim, espero que esta obra venha a corroborar no desenvolvimento de novos, e valorosos conhecimentos, e que auxilie os estudantes e pesquisadores na imersão em novas reflexões acerca dos tópicos relevantes na área de gestão do conhecimento e aplicações dos sistemas de informação para formação de ambientes cada vez mais inovadores.

Boa leitura!

Marcos William Kaspchak Machado

SUMÁRIO

CAPÍTULO 10

DIRETRIZES PARA UM MODELO ÁGIL DE GOVERNANÇA, GESTÃO E MATURIDADE DA SEGURANÇA DA INFORMAÇÃO

Gliner Dias Alencar
Instituto Brasileiro de Geografia e Estatística (IBGE)
Recife, Pernambuco

Alcides Jeronimo de Almeida Tenorio Junior
Instituto Brasileiro de Geografia e Estatística (IBGE)
Maceió, Alagoas

Hermano Perrelli de Moura
Centro de Informática (CIn), Universidade Federal de Pernambuco (UFPE)
Recife, Pernambuco

RESUMO: A governança e a gestão da segurança da informação, especialmente quanto à implementação de suas políticas e a adequação a normas de segurança da informação, não são tarefas simples. Consequentemente, podem surgir dificuldades relevantes em sua implantação, devido, muitas vezes, a complexidade das normas vigentes. O que demonstra a necessidade de se pesquisar alternativas para buscar suprir esta deficiência. Assim, este estudo propõe diretrizes para um modelo de governança, gestão e maturidade ágil para segurança da informação, concebido com base nos princípios expostos na família de normas ISO/IEC 27000, no COBIT e na Governança Ágil. Fazendo uso de perspectivas técnicas, de negócio (processo) e humanas. A pesquisa utilizou uma revisão bibliográfica e um *survey* com 157 empresas. A avaliação e os conseguintes refinamentos foram realizados com base em questionários enviados a empresas e a especialistas.

PALAVRAS-CHAVE: Governança de TIC, Governança Ágil, Segurança da Informação, Modelo de Maturidade.

ABSTRACT: Governance and information security management, especially with regard to the implementation of their policies and compliance with information security standards, are not simple tasks. Consequently, there may be significant difficulties in its implementation, often due to the complexity of the current norms. These difficulties demonstrate the need for a research focused on new ways to overcome such deficiency. Thus, this study proposes guidelines for an agile model of governance, management and maturity for information security based on the principles exposed on the ISO/IEC 27000 standards family, COBIT and on the Agile Governance. Using technical, business (process), and human perspectives. The research used a bibliography revision and a survey with 157 companies. The evaluation and refinement were obtained by relying on surveys sent to companies and experts.

KEYWORDS: IT Governance, Agile

Governance, Information Security, Maturity Model.

1 I INTRODUÇÃO

A segurança das informações de uma empresa carece de investimentos e estudos contínuos, devido à crescente importância da área de TIC e da sua complexidade, assim como das mutações e melhoramentos constantes dos diversos tipos de ameaças. O que torna extremamente relevante e justifica as constantes pesquisas para ampliação das tecnologias de segurança e seus processos. Sendo necessário, também, a melhoria e simplificação dos processos de alinhamento da segurança da informação ao negócio, bem como o estudo da variável pessoa que, normalmente, está envolvida desde a concepção da informação e dos meios de armazenamento até o seu descarte (ALENCAR; LIMA; FIRMO, 2013).

Atualmente, no ambiente corporativo, existem diversos padrões, *frameworks,* normas e regulamentos para a implementação de modelos de segurança. Esses modelos fornecem um conjunto de boas práticas visando a Governança e Gestão da Segurança da Informação que, em sua maioria, para incorporar todos os possíveis pontos inerentes ao tema, tornam-se grandes e complexos, fazendo com que, de uma forma geral, as empresas não apliquem e não gerenciem as características de Segurança da Informação de forma adequada.

A complexidade dos modelos tradicionais mais utilizados atualmente abre uma oportunidade para rever os processos de implantação de tais padrões, modelos, normas ou *frameworks*, adequando-os às necessidades específicas de cada organização. Visto que mesmo não implantando todos os processos ou controles, a organização pode gerar relevante mudança organizacional, com possível melhoria dos processos internos e um maior alinhamento entre a área de TIC e as estratégias organizacionais, como demonstram os resultados de Silva Neto, Alencar e Queiroz (2015) e Prado *et al.* (2016). É importante destacar, também, a escassez de estudos que investigam esta temática, comparando com outras áreas da administração e da computação (ALENCAR *et al.,* 2018a).

Neste contexto, acredita-se ser relevante para a área de segurança da informação, realizar estudos na tentativa de se produzir modelos para aferir a sua maturidade, bem como dar subsídios para um melhor alinhamento da área à Governança de TIC, analisando a tríade de perspectivas técnicas, processuais e humanas, buscando meios menos complexos e burocráticos que os atuais.

1.1 Problema de Pesquisa e Objetivo

Para manter a continuidade da empresa é primordial a proteção dos ativos de valor e a eficácia na gestão dos riscos, para que assim possa maximizar os lucros e aumentar

o valor da organização. Com base neste contexto, a ISO (*International Organization for Standardization*) criou a Família de normas 27000, que abordam temas relativos à Segurança da Informação (ISO, 2018). Sendo consideradas importantes mecanismos para a área, no que tange, principalmente, os aspectos táticos e operacionais.

Apesar destes modelos serem muito bem estruturados, o formalismo, por algumas vezes excessivo, tem tornado a adoção e melhoria contínua de seus processos uma tarefa complexa, como abordam Silva Neto, Alencar e Queiroz (2015) e Prado *et al.* (2016).

Esta pesquisa pretende explorar a lacuna supracitada como uma oportunidade para expandir e abordar tal paradigma, respondendo o seguinte questionamento: "De que maneira seria possível unificar os procedimentos, modelos, padrões e normas atuais para melhor avaliar a maturidade e gerir a Segurança da Informação corporativa de forma ágil?".

Para responder a este questionamento, o presente trabalho tem por objetivo, propor, de forma teórica, um modelo de governança, gestão e maturidade ágil para segurança da informação, interligando procedimentos, modelos, padrões e normas existentes. Bem como prover a junção dos princípios de Governança Ágil de TIC com a área de Segurança da Informação, diminuindo a burocracia e os formalismos dos modelos atuais.

1.2 Método Utilizado

Tendo um objetivo exploratório, o trabalho passará por procedimentos de pesquisa bibliográfica, por um *survey* com dado da empresa, dados do respondente e 5 questões sobre o tema deste trabalho, abaixo listadas:

- As normas, modelos e padrões atuais (por exemplo COBIT, ISO/IEC 27001, 27002, 27005, 27014, ITIL, etc) atendem às necessidades da empresa? (Opções: Concordo Totalmente, Concordo, Neutro, Discordo, Discordo Totalmente);
- Quais os principais motivos para as Empresas não adotarem (parcialmente ou em sua totalidade) as normas, modelos ou padrões atuais (por exemplo COBIT, ISO/IEC 27001, 27002, 27005, ITIL, etc)?
- De 1 a 5, onde 1 é o mais baixo nível de segurança e 5 é o mais alto:

  - Qual o nível de segurança desejado por você para a empresa?

  - Qual o nível de segurança você acredita que a empresa esteja atualmente?
- Quais os maiores problemas ou desafios de segurança da informação encontrados na empresa?

A solução proposta será analisada pelas empresas respondentes e por

especialistas na área, através de um segundo questionário, como forma de avaliação da estratégia pretendida.

2 I SEGURANÇA DA INFORMAÇÃO

Ao analisar a evolução das espécies animais, inclusive da espécie humana, verifica-se que é notável a busca por segurança em seus diversos aspectos.

No caso específico da segurança das informações, mesmo que a temática já possua centenas de anos, passou a ganhar lugar de destaque quando de fato formalizou-se a Era da Informação (CASTELLS, 2007).

O aumento exponencial do número de dispositivos computacionais, de usuários, e com as informações assumido o papel estratégico, gerou a necessidade de compartilhamento, disponibilidade e, consequentemente, de segurança. Fato agravado com a evolução das redes de computadores, particularmente com a popularização da Internet. Este novo ambiente foi percebido pelas organizações como uma possibilidade de expansão de negócios e da consequente ampliação de lucros. Entretanto, o aumento da lucratividade não era possível sem o incremento das vulnerabilidades dos sistemas de informação, as quais necessitavam ser combatidas.

Joia e Neto (2004) reforçam esse pensamento da evolução da economia, atrelado ao da segurança da informação, quando defendem que, já no início da década de 80, a Tecnologia da Informação (TI) não era mais utilizada apenas como uma ferramenta de processamento mais rápido, mas sim como uma forma estratégica e essencial para alavancar o negócio, necessitando de maiores proteções.

Cientes de que a ausência de níveis suficientes de segurança da informação poderia acarretar em danos irreparáveis, até mesmo a sua falência. Bem como, que no mundo atual, globalizado e de grande concorrência, todo investimento carece de justificativas e alinhamentos, as empresas passaram a fazer maior uso da visão sistêmica e organizacional em todas as áreas. Na perspectiva da Segurança da Informação no ambiente corporativo, isso passa a se refletir diretamente na atenção dada à Governança, Maturidade e Gestão da segurança da informação. Temas que serão tratados na sequência.

3 I GOVERNANÇA DE TIC

Atualmente, é impossível imaginar uma empresa sem que possua uma área de TIC estruturada para manipular os dados e prover informações, essenciais ao negócio e, principalmente, aos tomadores de decisões (CASTELLS, 2007). Mesmo que a estruturação, organização e manutenção desta infraestrutura de TIC, incluindo pessoas, processos e tecnologias especializados, requeiram altos investimentos

(ALENCAR; QUEIROZ, DE QUEIROZ, 2013).

Entretanto, algumas vezes, são impostas restrições orçamentárias aos investimentos de TIC no meio coorporativo. Em alguns casos por restrições orçamentárias da própria instituição. Em outros, por seus gestores duvidarem dos reais benefícios de tal investimento. Mesmo sendo sabido que a carência de investimentos na área de TIC pode ocasionar o fracasso de um empreendimento no cenário atual, competitivo e globalizado. Por outro lado, alguns gestores de TIC apresentam os projetos ou solicitam investimento sem demonstrar a real necessidade de sua aquisição, ou dos riscos associados ao não investimento. Em outras situações, tais riscos e necessidades são inseridos no projeto, mas os gestores não possuem habilidade para demonstrá-los de forma correta, ou debatê-los de modo a convencer a alta direção.

Para melhorar o processo de tomada de decisão baseado em uma correta análise de riscos, torna-se necessária boa estrutura para gerenciar e controlar as atividades de TIC nas empresas. Para garantir o retorno de investimentos e a adição de melhorias nos processos. Este movimento é conhecido como Governança de TIC (FERNANDES; ABREU, 2014).

O termo Governança de TIC, pode ser visto como uma estrutura de relações e processos que visam dirigir, bem como controlar, uma determinada instituição visando aditar valor ao negócio, por meio do gerenciamento dos riscos e garantindo um melhor retorno do investimento de TIC (DE HAES; VAN GREMBERGEN, 2015). Bem como o processo pelo qual decisões são tomadas sobre os investimentos de TIC, envolvendo vieses de como as decisões são tomadas, quem toma as decisões, quem é responsabilizado pela função de operação e gestão da área, e como os resultados são aferidos e monitorados. Ou seja, um processo que abrange o como dirigir, avaliar e monitorar todos os recursos de TIC (MANOEL, 2014). Gonçalves, Gaspar e Cardoso (2016) corroboram com o tema e afirmam que a Governança de TIC deve abranger as áreas de alinhamento estratégico, entrega de valor, gestão de recursos, gestão de riscos e mensuração de desempenho.

Segundo Gomes *et al.* (2016), entre os principais modelos, *frameworks* ou normas para Governança de TIC, podem ser citados: para Serviços de TIC - ITIL, ISO/IEC 20000; para Segurança da Informação - A família de normas ISO/IEC 27000; para Projetos - PMI e PMBOK; para Fornecedores - E-SCM e SAS70; e para *Software* - CMMI e MPSBR. Eles ainda apontam o COBIT, que aborda melhores práticas a serem utilizadas em todas estas áreas. Atualmente ele é desenvolvido e mantido pela ISACA, em sua versão 5 (ISACA, 2012).

Diante dos fatos expostos, DuMoulin (2015) enaltece a necessidade de uma forma mais simples e didática para implantação de uma política de gestão e governança única e alinhada ao negócio, inserindo a nova versão do COBIT como uma possível solução, devido às suas melhorias. Ponto que é corroborado por Fernandes e Abreu (2014). Outro possível viés, mas não excludente aos demais, é a utilização da Governança

Ágil de TIC, tema que será abordado em seção própria posteriormente.

Tal visão de análise da segurança da informação, que abrange o alinhamento entre o negócio e os riscos de negócios atrelados à TIC, pode ser entendida como Governança de Segurança da Informação.

3.1 Governança de Segurança da Informação

Pode ser entendida como um conjunto de ações e práticas para o alinhamento das atividades da área de segurança da informação com a estratégia da corporação (ALENCAR; TENORIO JUNIOR; MOURA, 2017). A GSI é uma parte da Governança de TIC, podendo haver sobreposição entre as duas (MANOEL, 2014). Deve ter o objetivo de: Alinhar os objetivos de negócio com a estratégia da segurança da informação; garantir que os riscos da informação sejam elucidados e encaminhados aos responsáveis; assim como, aditar valor para o negócio, para a alta direção e para as partes interessadas. Tendo como princípios: Estabelecer a segurança da informação em toda a organização; adotar uma abordagem baseada em riscos, recomendando-se a utilização em conjunto da ISO/IEC 27005; estabelecer e alinhar os investimentos; assegurar a conformidade com os requisitos internos e externos; promover um ambiente positivo de segurança, incluindo um tratamento especial às pessoas; e analisar criticamente o desempenho e resultado das ações de segurança da informação em relação aos resultados de negócios (ABNT, 2013c). Aplicando corretamente a GSI, além de atingir os objetivos supracitados, tende-se a encaminhar a organização ao atendimento e conformidade com requisitos externos, por exemplo, legais (MANOEL, 2014).

Assim, é possível perceber que Gestão da Segurança da Informação é diferente da GSI. Mas, verifica-se que as duas se complementam, a Gestão sendo mais voltada para os aspectos táticos e operacionais. Já a Governança mais direcionada para as camadas táticas e estratégicas. Diferença esta, também enfatizada e demonstrada por Amorin e Bernardes (2017).

Por fim, Manoel (2014) aponta que uma correta aplicação da GSI visa um tratamento mais ágil à área. Entendimento acompanhado, com maior abrangência (Governança de TIC) por Fernandes e Abreu (2014). O que reforça a necessidade de que os arcabouços utilizados sejam mais simples e rápidos, para auxílio das tomadas de decisão. Neste contexto, serão apresentados a seguir, os princípios da Governança Ágil.

3.2 Governança Ágil

A burocracia existente nos processos, bem como a dificuldade na aplicação dos modelos ou *frameworks* atuais, tornam-se entraves em diversos casos (PRADO *et al.*, 2016). Neste sentido, é possível observar um conflito entre o formalismo apresentado pela maioria destas iniciativas e a agilidade imposta por um mercado cada vez mais

competitivo. Com este pensamento, surgem ações para tentar impor agilidade e respostas mais rápidas.

A Abordagem Ágil pode ser inserida em ações específicas. Dentre elas destaca-se o desenvolvimento de software ágil, por exemplo. Mas também pode ser inserida em contextos mais amplos, como os de abrangência organizacional (GREGORY *et al.,* 2016), onde se insere a abordagem de Governança Ágil. Ela propõe a aplicação de agilidade sobre o sistema de gestão e governança organizacional tornando-o competitivo (LUNA *et al.*, 2014). Sendo a agilidade, neste contexto, entendida como a capacidade de uma organização reagir a mudanças em seu ambiente, mais rapidamente que o ritmo dessas mudanças (LUNA *et al.*, 2014).

Agilidade no nível do negócio exige flexibilidade, capacidade de resposta e adaptabilidade, que devem ser aplicadas em combinação com a capacidade de gerência, alinhamento estratégico e envolvimento entre as áreas incluídas, especialmente em ambientes competitivos (LUNA *et al.*, 2014). A agilidade pode ser entendida como a capacidade que as organizações apresentam, de forma dinâmica, para sentir a necessidade de mudança a partir de fontes internas e externas e realizar essas mudanças rotineiramente, sem a queda de seu desempenho (RAMLAOUI; SEMMA; DACHRY, 2015). Neste sentido, a Governança Ágil seria a capacidade de uma organização de sentir, adaptar-se e responder às mudanças no seu ambiente, de uma forma coordenada e sustentável, mais rápido do que a ritmo dessas mudanças (LUNA *et al.*, 2016).

Meios mais ágeis no ambiente corporativo, bem como com essa visão mais ampla dada à Governança Ágil, são uma necessidade, visto que a governança de TIC tradicional é muitas vezes um conjunto muito rígido de regras e processos, evitando que a área de TIC possa evoluir e mudar junto com a necessidade da empresa (RAMLAOUI; SEMMA; DACHRY, 2015).

A Governança Ágil não é uma substituta aos modelos convencionais, frameworks e métodos já existentes, por exemplo, ITIL e COBIT (LUNA *et al.*, 2014). A proposta é a de inserir uma nova visão para a Governança. Com este intuito, os meta-valores da Governança Ágil podem ser comparados com os da Governança tradicional como segue (LUNA *et al.*, 2016):

- Comportamento e prática *vs* processos e procedimentos;
- Alcançar a sustentabilidade e a competitividade *vs* realização de auditoria para buscar a conformidade;
- Transparência e envolvimento das pessoas *vs* monitoramento e controle;
- Sentir, adaptar e responder determinado estímulo *vs* seguir um plano.

Tais embasamentos podem nortear a área de segurança da informação, trazendo uma nova visão (complementar) frente aos modelos atuais.

3.3 Modelos de Maturidade

Para um correto alinhamento da área de TIC ao negócio, são essenciais métricas e modelos para se definir o estágio atual, além dos próximos passos para se chegar a um nível mais avançado de maturidade (ALENCAR; TENORIO JUNIOR; MOURA, 2017; SILVA; BARROS, 2017), sendo o modelo de maturidade considerado o propício para isto. Trata-se de um conjunto de características, atributos, indicadores ou padrões que representam a capacidade e a progressão em uma determinada disciplina. Seu conteúdo exemplifica tipicamente as melhores práticas e pode incorporar padrões ou outros códigos de prática da disciplina (REA-GUAMAN *et al.,* 2017).

O uso deste modelo permite uma avaliação contínua e a identificação de lacunas que representam riscos. Auxiliando também na explicitação dos riscos e fragilidades à equipe e envolvidos. Baseados nesta análise, planos podem ser avaliados e desenvolvidos para a melhoria dos processos e de controles considerados deficientes, buscando-se o nível desejado (RIGON *et al.*, 2014). Fato que é corroborado por Alencar *et al.* (2018b), que demonstram uma nova estratégia para maturidade da segurança da informação. Com isto, percebe-se que um modelo de maturidade nesta área é essencial para a obtenção de níveis de gestão e governança eficazes e eficientes, trabalhando em conjunto.

Assim, após a apresentação dos diversos estudos sobre a área de Modelos de Maturidade, torna-se necessário tratar sobre os normativos da área de segurança, mais especificamente a família de normas ISO 27000.

4 I FAMÍLIA DE NORMAS ISO/IEC 27000

A família 27000 da ISO é composta por um aglomerado de normas, em que a maioria pertence à área da segurança da informação. Por isso, muitas vezes é chamada de família de normas ISSO, da Segurança da Informação. Cada uma das normas ou relatórios técnicos possui finalidade específica e voltada a uma área da segurança, conforme detalhadas por ISO (2018). Entre as mais utilizadas neste escopo, podem ser destacadas as seguintes:

- ISO/IEC 27.001:2013: a norma que define os requisitos para um Sistema de Gestão da Segurança da Informação (SGSI) (ABNT, 2013a);
- ISO/IEC 27.002:2013: é um conjunto de práticas com um grupo completo de controles que auxiliam a aplicação do Sistema de Gestão da Segurança da Informação (ABNT, 2013b);
- ISO/IEC 27.005:2011: cobre a gestão de riscos em segurança da informação. Grande parte do escopo da ISO 27.005 pode ser interpretada como a sessão 4 da norma ISO 27.001, detalhada quanto a perspectiva dos riscos

(ABNT, 2011).

- ISO/IEC 27.014:2013: técnicas para Governança de Segurança da Informação. Nela constam especificações de como avaliar, dirigir, controlar e comunicar todas as práticas internas da empresa relacionadas à segurança da informação, de forma que sejam compreendidas e estejam alinhadas com necessidades da área de negócio (ABNT, 2013c).

5 I ANÁLISE DOS DADOS E PROPOSTA

A pesquisa aplicou um *survey* para melhor entendimento do ambiente atual, entre os anos de 2015 e 2017. Para facilitar a abordagem do trabalho, todos os respondentes são denominados de "empresa", indiferente da sua classificação, porte ou abrangência. Obteve-se 157 respostas distintas em conformidade com os objetivos da pesquisa. Ressalta-se que todos os respondentes eram da área de TIC. Além disso, 93 deles (59,24%) trabalhavam exclusivamente ou prioritariamente com a área de segurança da informação.

Das empresas pesquisadas, observa-se que a maioria se denomina como representante do setor terciário da economia, classificadas, portanto, como privadas, como pode ser visto na Figura 1. Todos os gráficos apresentam a categoria, o valor absoluto de empresas e o percentual.

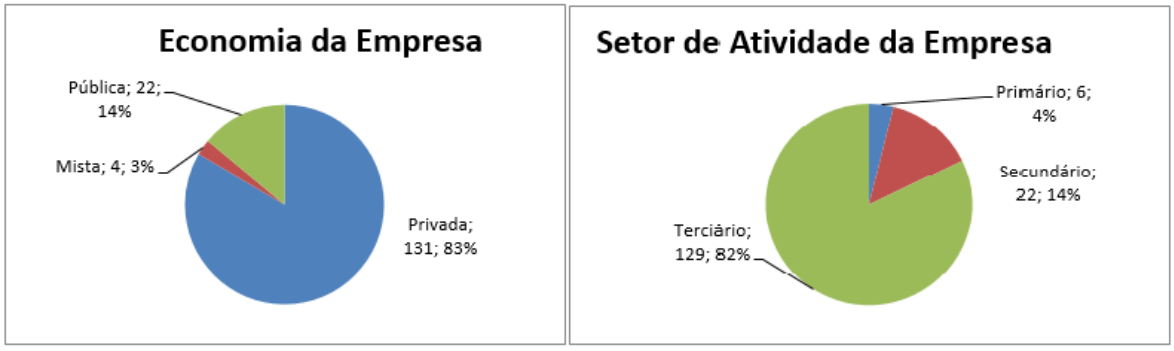

Figura 1. Classificação das Empresas Pesquisadas

A amostra de empresas alcançadas abrange 94,9% de empresas sediadas no Brasil, atingindo todas as regiões, e 5,10% de empresas sediadas no exterior (Argentina, Estados Unidos, Inglaterra e Portugal). A maioria possui atuação nacional e entre 50 e 100 funcionários, como pode ser visto na Figura 2. Ressalta-se, também, que 16,03% (25 empresas) têm a TIC como área fim.

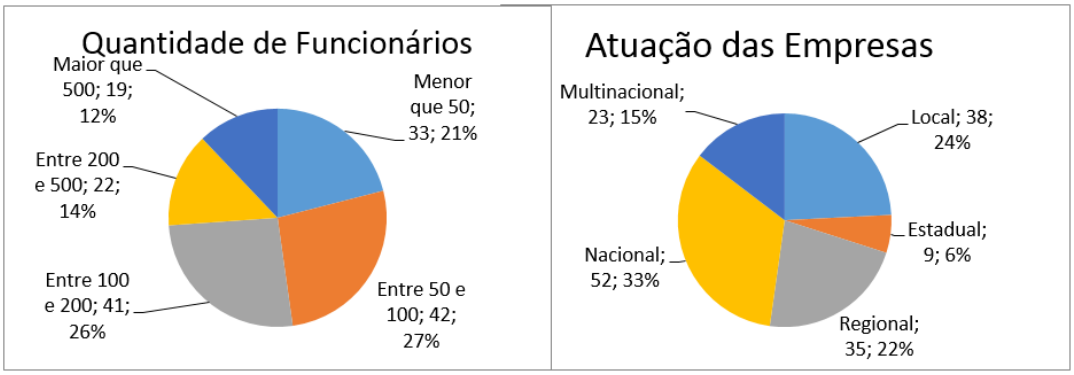

Figura 2. Atuação e Funcionários das Empresas Pesquisadas

Ao questionar se as normas e padrões atuais atendem à empresa, 95,54% apontaram “Concordo” ou “Concordo Totalmente”. Ciente de que as mesmas se adequam à grande maioria das empresas pesquisadas, mas que isso, de acordo com a literatura da área, não reflete na quantidade de empresas que realmente as aplica, foram questionados os motivos para a não utilização formal das normas e padrões. Neste caso, foram apontados vários motivos, destacando-se como principais categorias citadas:

- A complexidade das normas (41,4%);
- A falta de apoio ou definição estratégica por parte do alto escalão (30,6%);
- Os custos de implantação e gestão (21,6%).

Tais fatores levantados ratificam a situação e os problemas expostos na fundamentação teórica, e corroboram com a justificativa deste trabalho.

Outro ponto relevante também analisado é o desejo das empresas em alcançar patamares avançados no que tange a segurança da informação. Ao serem questionadas sobre o nível de segurança da informação desejado, 91,1% (143) das empresas apontaram o desejo de estar no nível máximo. Porém, o cruzamento de dados revela que a situação real da empresa é bem diferente. Ao serem questionadas sobre o nível de segurança da informação que a empresa se encontra atualmente, 54,8% delas responderam que acreditam que se encontram no nível mínimo, e apenas 9 (5,7%) afirmaram estar no nível máximo. Ambos os dados em uma escala de 5 níveis. O que aponta a dificuldade em se alcançar níveis de excelência na área, mesmo quando desejados, e que ainda deverá ser traçado um caminho árduo para se atingir níveis aceitáveis na segurança da informação coorporativa.

A partir deste cenário, os resultados sugerem que mesmo com os avanços nas pesquisas elencadas na fundamentação teórica, pouca alteração se viu no meio corporativo, que ainda tem como problemas a serem resolvidos, dilemas debatidos há anos na literatura, porém ainda sem soluções realmente efetivas. Assim, como forma de fazer o elo entre as principais pesquisas levantadas e o meio coorporativo,

o presente trabalho se concentrou em elencar diretrizes para que seja possível a aplicação da evolução teórica.

No levantamento teórico, ficou evidenciado que existe um conjunto de padrões, normas, *frameworks* e guias para a gestão e o alinhamento da área de segurança da informação. Porém, após o levantamento e a análises, ficou evidenciado na literatura que para se ter uma visão unificada do negócio, é necessário que se aponte diretrizes para as áreas de: Alinhamento e Governança; Controles e Políticas de Segurança da Informação; Riscos e Mensuração da Maturidade. Percebe-se também a necessidade de uma melhor interação entre o arcabouço proposto para cada uma dessas áreas, bem como da diminuição da complexidade de implantação e gestão, sendo necessária uma visão mais unificada e ágil.

Acredita-se, por fim, ser essencial a inclusão de uma análise mais profunda das perspectivas humanas, pois podem se tornar mais uma camada de segurança, como apresentado por Alencar, Lima e Firmo (2013). Assim como outros estudos mostram a incapacidade da gestão da segurança da informação sem o correto desenvolvimento do enfoque social. Eles apontam, inclusive, que os ataques mais comuns à informação se iniciam através da exploração de fraquezas humanas. Para o atendimento dessas diretrizes elencadas na literatura com as principais áreas a serem tratadas, criou-se a proposta exposta na Figura 3, abaixo.

Já a aplicação das normas ISO/IEC 27001, 27002, 27005, 27014, do COBIT e de seus detalhamentos para Segurança da Informação e Risco, atende a contento todas as áreas levantadas no trabalho. Sendo esses os arcabouços mais utilizados, segundo a literatura. Porém a sua simples implantação ainda não trata duas questões elencadas: a complexidade das normas e modelos, bem como a análise dos fatores humanos.

Ciente que as informações são, na grande maioria dos casos, criadas, manipuladas, administradas ou utilizadas por pessoas, não há como, simplesmente, tratar essas pessoas como um elo fraco da segurança. Torna-se necessário então, implementar ações contínuas de treinamento e conscientização, com preza a ISO/IEC 27001 e 27002. Também são necessárias políticas efetivas para controle, por exemplo, de senha e segregação de função, também indicadas nas mesmas normas ISO/IEC. Diante disto, as “Perspectivas Humanas” foram inseridas na base proposta como um elemento adicional. De forma que todas as ações sejam pensadas como proteção, também, para este elemento.

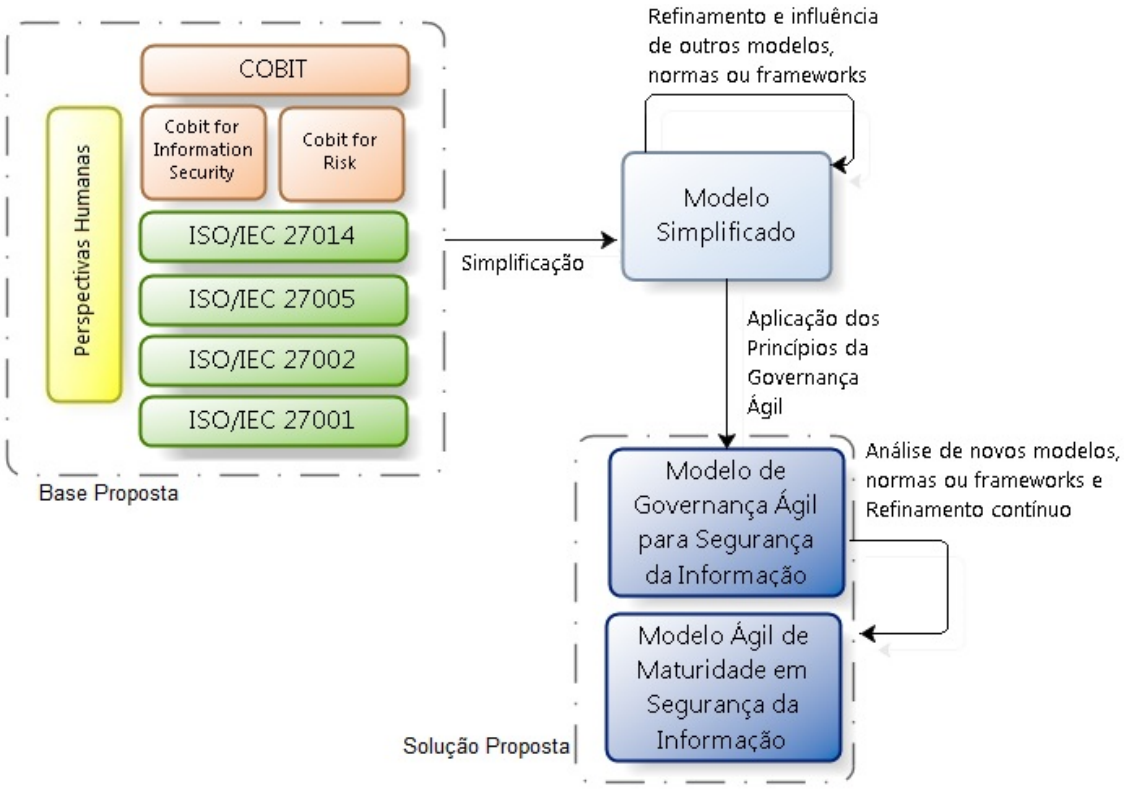

Figura 3. Diretrizes Teóricas

Salienta-se que todo esse arcabouço deve ser bancado pelo alto escalão da empresa. Ações implantadas pela área de TIC sem o devido consentimento e apoio da alta direção tendem, frequentemente, ao fracasso, como é relatado em diversos trabalhos. Sendo esta uma das premissas também inseridas nos normativos da área de segurança da ISO.

Por conseguinte, resta apenas o tratamento da “complexidade das normas”. Elencado na literatura como item normalmente problemático e que também foi ressaltado na amostra do *survey* deste trabalho, pois os resultados apontaram este como principal problema citado. Assim, entende-se que a diminuição desta complexidade, além de sanar o problema citado, passa a auxiliar o atendimento de outro problema levantado: Os “custos de implantação e gestão”. Pois, com um modelo unificado e de menor complexidade, acredita-se que seus custos de implantação e gestão sejam diminuídos sensivelmente.

Neste quesito, o modelo exibido na Figura 3 aponta uma primeira ação de simplificação. Acredita-se que para esta etapa devam ser elencados os 114 controles das ISO/IEC 27001 e 27002, e relacionados apenas os que realmente se aplicam ao negócio, sendo descartados neste momento os demais. Com os controles levantados, deverão ser inseridos apenas os controles, processos e procedimentos dos demais itens da base proposta (ISO/IEC 27005, 27014, do COBIT e de seus detalhamentos para Segurança da Informação e Risco) que se relacionam com a listagem dos controles selecionados. Desta forma, em uma primeira instância, já se vislumbra a diminuição do arcabouço como um todo, bem como o alinhamento entre eles, gerando

a partir daí, um Modelo Simplificado.

Conforme demonstrado na Figura 3, o Modelo Simplificado pode sofrer influência e refinamentos de outros modelos, normativos ou da legislação externa, que se aplicam ao negócio, ou até mesmo alguma alteração na etapa da base proposta.

Com o Modelo Simplificado avaliado e refinado, parte-se para a terceira etapa, que consiste na aplicação dos conceitos da Governança Ágil. Tal etapa servirá para diminuir o formalismo do modelo gerado, criando a versão final a ser aplicada, já contemplando todas as etapas levantadas neste trabalho. É nesta etapa que se deve gerar e aplicar o modelo de maturidade. Modelo que pode ser criado pela empresa, ou, de forma alternativa, podem ser adaptados e utilizados modelos elencados na fundamentação teórica. Sendo este último, o caminho levantando na literatura como sendo o de maior êxito.

A validação da presente proposta de modelo simplificado foi realizada em duas etapas. A primeira, ao enviar a proposta para seis especialistas na área de segurança da informação. Quando se obteve a resposta de cinco deles. Todos se posicionaram de forma positiva ao serem questionados sobre: se a mesma abrangia os principais pontos para uma correta adequação da empresa nas áreas de Alinhamento e Governança, Controles e Políticas de Segurança da Informação, Riscos e Mensuração da Maturidade, para se formar uma proposta de Governança Ágil de Segurança da Informação. Um dos especialistas ainda afirmou que ao cumprir todos os passos, a empresa estaria em patamar bastante elevado se comparado com o mercado.

A segunda etapa da validação consistiu em enviar o modelo simplificado proposto para as 157 empresas respondentes do primeiro *survey,* além de questioná-las se o modelo atenderia as suas necessidades, e se elas implantariam esta versão simplificada. Adicionalmente, foi solicitada a justificativa da resposta. Dos 157 questionários enviados, 104 (66,2%) foram retornados. Destes, todos afirmaram que o modelo atendia as necessidades da empresa. E somente 16 empresas (15,4% dos respondentes deste questionário de validação) afirmaram que, mesmo atendendo as necessidades da empresa, não o implantariam, visto que ainda o consideravam muito complexo.

Diante do exposto, entende-se que o modelo proposto teve sua validade atestada por atender as expectativas dos especialistas em segurança consultados, bem como de quase 85% das empresas respondentes do questionário de validação.

6 I CONSIDERAÇÕES FINAIS

Os resultados da pesquisa revelam a grande importância das informações para as empresas. Uma vez que atualmente se concentram nos dados criados, guardados e manipulados por pessoas e aparatos tecnológicos.

O crescimento das ameaças em quantidade, qualidade e “inteligência” também

é um fato verificado. Assim como a evolução da segurança da informação que, por motivos diversos, ainda se desenvolve em ritmo inadequado para acompanhar os avanços e necessidades da TIC.

Através da pesquisa, confirma-se que muitas das empresas não se encontram em adequação com algum tipo de norma ou padrão de segurança da informação. Diante de diversos fatores a serem considerados para a não adequação às normas de segurança da informação, pode-se destacar: (i) A complexidade das normas, (ii) a falta de apoio ou definição estratégica por parte do alto escalão e (iii) os custos de implantação e gestão.

Ou seja, é necessária uma simplificação das normas de forma a melhorar a questão apontada no item i, assim como auxiliar na redução dos valores do item iii. Também é necessário um melhor debate e conscientização da área com o alto escalão, visto que existe um consenso atual quanto à necessidade de segurança, mas que, entretanto, esbarra na falta de apoio ou definição dos superiores hierárquicos. Um dos maiores problemas apontados.

Outro ponto relevante é o desejo de alcançar patamares avançados no que tange a segurança da informação. Visto que 91,1% apontaram o desejo de estar no nível máximo, mas somente 54,8% desta mesma amostra responderam que acreditavam encontrar-se apenas no nível mínimo. O que demonstra que ainda deverá ser traçado um caminho árduo, pelas empresas.

Por fim, verifica-se que é imprescindível a criação de um modelo que auxilie as empresas a gerirem com eficácia e eficiência os recursos de TIC, mantendo a segurança das informações (visto que são patrimônios a serem preservados) e respondendo as demandas de forma ágil.

Além disso, o trabalho também teve por objetivo abordar os desafios de adoção e melhoria contínua da área de Segurança da Informação em organizações de naturezas variadas. Através da concepção e definição de diretrizes para um modelo de governança, gestão e maturidade concebido segundo os princípios expostos na família de normas ISO 27000 e no COBIT. Bem como, lançando-se mão das perspectivas técnica, de negócio (processos), humana e de direcionamentos ágeis. O que acredita-se ter sido cumprido através da das diretrizes expostas na Figura 3, bem como com a validação de especialistas e das empresas pesquisadas, quanto ao modelo simplificado proposto.

Portanto, acredita-se que a implementação deste modelo pode contribuir de forma relevante com a área de segurança da informação, tanto no contexto acadêmico, quanto no meio coorporativo. Espera-se que o modelo proposto: Promova apoio relevante à adoção e melhorias contínuas para a segurança da informação, ajudando a mensurar a maturidade da empresa; possibilite a comparação do “nível de segurança” entre setores ou empresas através do modelo de maturidade; ajude a quebrar o paradigma de aplicação da segurança da informação de forma tradicional, através da utilização dos conceitos da Governança Ágil; e que propicie maior agilidade

na gestão da segurança da informação, ajudando a promover um ambiente de GSI.

Durante este processo foi possível verificar, por meio da observação dos dados e estudos já realizados, que há uma carência de práticas e modelos de segurança nas empresas, havendo assim a necessidade por mais trabalhos e pesquisas, além da ampliação da sua divulgação, visando subsidiar as corporações para que melhorem seu nível de segurança da informação e consigam atuar de forma mais competitiva no mercado globalizado.

Ciente que esta é a primeira apresentação do modelo proposto, são esperadas proposições de melhorias e atividades complementares, visando a sua evolução. Assim, para trabalhos futuros, acredita-se serem importantes, dentre outros: Verificar formas de validação dos controles das ISO/IEC 27001 e 27002 elencados como base simplificada; realizar avaliações e comparativos com outros modelos e propostas que venham a ser inseridas na literatura; e criar e validar um modelo de maturidade para Segurança da Informação inserindo os princípios da Governança Ágil.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos**. Rio de Janeiro, p. 30. 2013a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Rio de Janeiro, p. 99. 2013b.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro, p. 87. 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27014: Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação**. Rio de Janeiro, p. 12. 2013c.

ALENCAR, G. D.; LIMA, M. F.; FIRMO, A. C. A. A perspectiva de análise comportamental como forma de combate à engenharia social e phishing. **Revista Eletrônica de Sistemas de Informação**, v. 12, n.3, 2013.

ALENCAR, G. D; MENEZES, B. P.; AMORIM, E. S.; FARIAS JUNIOR, I. H.; MOURA, H. P. Governança, Gestão e Maturidade da Segurança da Informação: um mapeamento sistemático do cenário nacional**. Revista de Sistemas e Computação**, v. 8, n. 1, p. 153-173, 2018a.

ALENCAR, G. D.; MOURA, H. P.; FARIAS JUNIOR, I. H.; TEIXEIRA FILHO, J. G. A. An Adaptable Maturity Strategy for Information Security. **Journal of Convergence Information Technology (Gyeongju)**, v. 13, p. 1-12, 2018b.

ALENCAR, G. D.; QUEIROZ, A. A. L; DE QUEIROZ, R. J. G. B. Insiders: Análise e Possibilidades de Mitigação de Ameaças Internas. **Revista Eletrônica de Sistemas de Informação**, v. 12, n. 3, p. 1-38, 2013.

ALENCAR, G. D.; TENORIO JUNIOR, A. J. A.; MOURA, H. P. Theoretical Guidelines for an Agile Model of Governance, Management and Maturity for Information Security. In: **14th International**

Conference on Information Systems & Technology Management – CONTECSI, Anais… p. 3661–3690, 2017.

AMORIM, E. S.; BERNARDES, M. C. A Model for Information Security Governance in Retail Enterprises. In: **14th International Conference on Information Systems & Technology Management - CONTECSI**, Anais… p. 1062–1092, 2017.

CASTELLS, M. **Era da Informação: A Sociedade em Rede.** Volume 1. 10ª Edição. São Paulo: Editora Paz e Terra, 698 p., 2007.

DE HAES, S.; VAN GREMBERGEN, W. **Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5**. Springer, 2ª ed., 2015.

DUMOULIN, T. **Governance of Enterprise IT Missing In Action**. COBIT, Reportagem, 2015. Disponível em: http://www.isaca.org/COBIT/focus/Pages/governance-of-enterprise-it-missing-in-action.aspx. Acesso em: 17 jun. 2016.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI: Da estratégia à Gestão de Processos e Serviços.** Brasport, 2014.

GOMES, L. D.; GOULART JÚNIOR, C. R.; SIMEÃO, J. L. C.; SOUSA, T. J. R.; SANTANA, A. C. Best Practices in Governance of Information and Technology Management. In: **13 International Conference on Information Systems & Technology Management - CONTECSI**, Anais... 2016.

GONÇALVES, A. P.; GASPAR, M. A.; CARDOSO, M. V. Maturity Level of Information Technology Governance in Companies Operating in Brazil. In: **13 International Conference on Information Systems & Technology Management - CONTECSI**, Anais... 2016.

GREGORY, P.; BARROCA, L.; SHARP, H.; DESHPANDE, A.; TAYLOR, K. The challenges that challenge: Engaging with agile practitioners' concerns. **Information and Software Technology**, v. 77, p. 92-104, 2016.

ISACA. **COBIT 5: A Business Framework for the Governance and Management of Enterprise IT**. ISACA, 2012.

ISO. **International Organization for Standardization**. Disponível em: http://www.iso.org/. Acesso em: 12 out. 2018.

JOIA, L.; NETO, A. Government-To-Government Enterprises in Brazil: Key Success Factors Drawn From Two Case Studies. In**: BLED 2004**, Anais… v. 20, 2004.

LUNA, A. J. D. O., KRUCHTEN, P., PEDROSA, M. L. D. E., NETO, H. R., MOURA, H. P. State of the art of agile governance: a systematic review. **International Journal of Computer Science & Information Technology**, v.6, n.5, 2014.

LUNA, A. J. H. O.; KRUCHTEN, P.; RICCIO, E. L.; MOURA, H. P. Foundations For An Agile Governance Manifesto: A Bridge For Business Agility. In: **13 International Conference on Information Systems & Technology Management - CONTECSI**, Anais... 2016.

MANOEL, S. S. **Governança de Segurança da Informação: Como criar oportunidades para o seu negócio**. Brasport, 2014.

PRADO, E. P. V.; MANCINI, M.; BARATA, A. M.; SUN, V. Governança de TI em Organizações do Setor de Saúde: um Estudo de Caso de Aplicação do COBIT. In: **SBSI - Simpósio Brasileiro de Sistemas de Informação**, Anais... 2016.

RAMLAOUI, S.; SEMMA, A.; DACHRY, W. Achieving a balance between IT Governance and Agility. **IJCSI - International Journal of Computer Science Issues**, v. 12, n. 1, 2015.

REA-GUAMAN, A. M.; SANCHEZ-GARCIA, I. D.; FELIU, T. S.; CALVO-MANZANO; J. A. Maturity models in cybersecurity: A systematic review. In: **12th Iberian Conference on Information Systems and Technologies (CISTI)**, Anais… p. 1–6, 2017.

RIGON, E. A.; WESTPHALL, C. M.; SANTOS, D. R.; WESTPHALL, C. B. A cyclical evaluation model of information security maturity. **Information Management & Computer Security**, v. 22, n. 3, p. 265-278, 2014.

SILVA, M. P.; BARROS, R. M. Maturity Model of Information Security for Software Developers. **IEEE Latin America Transactions**, v. 15, n. 10, p. 1994–1999, 2017.

SILVA NETO, G. M.; ALENCAR, G. D.; QUEIROZ, A. A. L. Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas. In: **SBSI - Simpósio Brasileiro de Sistemas de Informação**, Anais... p. 299-306, 2015.

SOBRE O ORGANIZADOR

Marcos William Kaspchak Machado - Professor na Unopar de Ponta Grossa (Paraná). Graduado em Administração - Habilitação Comércio Exterior pela Universidade Estadual de Ponta Grossa. Especializado em Gestão industrial na linha de pesquisa em Produção e Manutenção. Doutorando e Mestre em Engenharia de Produção pela Universidade Tecnológica Federal do Paraná, com linha de pesquisa em Redes de Empresas e Engenharia Organizacional. Possui experiência na área de Administração de Projetos e análise de custos em empresas da região de Ponta Grossa (Paraná). Fundador e consultor da MWM Soluções 3D, especializado na elaboração de estudos de viabilidade de projetos e inovação.

Agência Brasileira do ISBN
ISBN 978-85-7247-202-9