UNIVERSIDADE CATÓLICA DE PERNAMBUCO

PRÓ-REITORIA ACADÊMICA

MESTRADO PROFISSIONAL EM INDÚSTRIAS CRIATIVAS

IZAAC JOSÉ SILVA ESPÍNDOLA

Aplicação da estratégia PRIMASIA visando à segurança da informação em ambiente de Data Centers

Recife

2019

IZAAC JOSÉ SILVA ESPÍNDOLA

Aplicação da estratégia PRIMASIA visando à segurança da informação em ambiente de Data Centers

Dissertação apresentada ao Programa de Pós-Graduação do Mestrado Profissional em Indústrias Criativas da Universidade Católica de Pernambuco, como requisito parcial para a obtenção do título de Mestre.

Orientador: Prof. Dr. João Guilherme de Melo Peixoto

Recife

2019

Agradecimentos

Depois de uma longa caminhada o Mestrado está chegando ao final. Neste momento se analisa tudo que foi encontrado nesse desafio refletindo sobre o aprendizado técnico, evolução pessoal e profissional, chegando a hora de agradecer aos que contribuíram para que fosse possível a conclusão desta etapa. Desta forma inicio meu agradecimento primeiramente a Deus por ter possibilitado concluir mais uma etapa em minha vida.

Agradeço ao professor e orientador João Guilherme de Melo Peixoto, pelo empenho durante toda jornada, contribuindo com seus e esclarecimento técnicos, sugestões de livros feitos até mesmo antes de ser meu orientador. Posso dizer que ele foi mais do que um orientador, foi amigo que passou tranquilidade nas horas mais difíceis e sempre acreditou que chegaríamos ao fim.

Agradeço a minha família representada pelos meus pais que sempre apoiam meus estudos. Sem eles não estaria onde estou. Agradeço de foram imensurável a minha esposa Liliane da Silva Ferreira que foi compreensiva nos momentos ausentes que aconteceram durante a jornada, sempre incentivando e auxiliando para um decorrer tranquilo do projeto sempre mostrando incentivo em todos os sentidos. Agradeço a minha filhota Izabelle da Silva Ferreira Espindola, por descontrair o ambiente nos momentos que estive nervoso. Ao meu próximo filho que foi concebido nesta fase final do mestrado e mesmo ainda no ventre de minha esposa, passou forças para concluir mais uma etapa em minha vida.

Agradeço a todos os professores que contribuíram de alguma forma com as pesquisas e levantamento bibliográfico conhecimento técnico. Aos meus colegas de metrado que sempre acreditaram que chegaríamos a esse dia tão esperado.

Agradeço ao meus amigos que compreenderam os momentos de ausência, especialmente agradeço ao meu amigo Gliner Dias Alencar, que sempre incentivou a realizar o mestrado e foi coautor deste projeto contribuindo muito tecnicamente para realização dos meus estudos.

Agradeço imensamente as Diretores e Gerente de TIC das organizações que contribuíram para aplicação da estratégia. Não é fácil encontrar pessoas que te recebam a fim de contribuir com um projeto que fala de segurança da informação. Não posso deixar de agradecer aos especialistas que responderam ao longo questionário proposto por este projeto, sem eles não se conseguiria um resultado satisfatório. E finalmente a todos que contribuíram de forma direta para finalização de mais um ciclo de aprendizado obtido.

Resumo

O presente trabalho apresenta um estudo sobre maturidade, com especificação e aplicação prática da estratégia Primasia de forma independente, embasada por controles da família ISO 27000 e níveis de maturidade do COBIT, visando melhorias de processos e priorização de controles utilizados para manter e melhorar a segurança da informação em ambiente de *data center*. Tendo, como objetivo geral: analisar o nível de maturidade dos ambientes de *data centers* corporativos no que tange à segurança da informação. A utilização da metodologia da pesquisa-ação-participativa, foi realizada através de questionários com especialistas da área de estudo embasados na estratégia Primasia. Para aplicação da metodologia foram identificados diversos modelos de maturidade, baseados por normas e procedimentos com foco no tema estudado. A implementação desses modelos em sua maioria, levam em consideração todos os possíveis controles definidos pelos modelos, o que dificulta por falta de um gerenciamento das organizações, a definição dos aspectos que são mais relevantes, bem como o nível de complexidade dos controles. O resultado final desse estudo é a aplicação da estratégia Primasia de forma independente, criando uma classificação independente dos controles mais importantes a serem aplicados ao ambiente de *data center*, garantindo que os aspectos mais relevantes sejam priorizados com maior pontuação. Conclui-se que dentro deste contexto, este estudo possibilitou identificar e classificar o nível de maturidade em ambientes de *data center*s, no que tange os critérios de segurança da informação, atendendo o objetivo principal deste projeto que é de analisar o nível de maturidade dos ambientes de *data centers* corporativos no que tange à segurança da informação.

Palavras-chave: Maturidade, Segurança da Informação, *Data center*

Abstract

The present work presents a study on maturity, with specification and practical application of the Primasia strategy independently, based on ISO 27000 family controls and COBIT maturity levels, aiming at process improvements and prioritization of controls used to maintain and improve safety of information in a data center environment. With the general objective of analyzing the level of maturity of corporate data center environments with respect to information security. The use of participatory action-research methodology was carried out through questionnaires with specialists from the study area based on the Primasia strategy. For the application of the methodology, several maturity models were identified, based on norms and procedures focused on the studied theme. The implementation of these models mostly takes into account all the possible controls defined by the models, which makes it difficult to manage the organizations, define the aspects that are most relevant, and the level of complexity of the controls. The final result of this study is the application of the Primasia strategy independently, creating an independent classification of the most important controls to be applied to the data center environment, ensuring that the most relevant aspects are prioritized with higher scores. It is concluded that within this context, this study made it possible to identify and classify the level of maturity in data center environments, regarding the information security criteria, meeting the main objective of this project that is to analyze the level of maturity of the environments of corporate data centers with regard to information security.

Keywords: Maturity, Information Security, Data Center

Lista De Figuras

Lista de Quadros

Lista de Abreviações

ISO - *International Organization for Standardization*
IEC - *International Electrotechnical Commission*
NIST - *National Institute of Standards and Technology*
DoS - *Denial of Service*
DDoS - *Distributed Denial of Service*
COBIT - *Control Objectives for Information and related Technology*
CMM - *Capability Maturity Model*
AD – *Active Directory*
TI – *Teconologia da Informação*
TIC – *Teconologia da Informação e Comunicação*

Sumário

1 INTRODUÇÃO

A necessidade da segurança da informação para uma sociedade cada vez mais conectada em rede passa a ser essencial. Organizações buscam cada vez mais a proteção contra a utilização inadequada de suas informações. Neste contexto, a informação tornou-se um dos ativos mais valiosos sendo considerado em algumas situações como um ativo intangível, como descreve Castells (2009). A forma com que as organizações tratam essas informações pode garantir o crescimento, mantendo-se no mercado de maneira competitiva, ou acumular prejuízos que cheguem a extinção destas organizações. Assim percebe-se necessidade de investimento no setor que gerência as informações tornando-os estratégico (CASTELLS, 2009; SEMOLA, 2013).

Nesta nova situação, percebe-se a ampliação dos papéis da Tecnologia da Informação (TI) ou, de forma mais ampla, da Tecnologia da Informação e Comunicação (TIC), que é responsável pelo gerenciamento de um bem com valor, muitas vezes, imensurável. Em consequência disto, estas informações são extremamente visadas e os mais diversos tipos de ameaças buscam alcançá-las.

Ciente desta grande quantidade de informação inserida e manuseada, se faz cada vez mais necessária a implementação da segurança da informação nas organizações, a fim de garantir um melhor controle da informação, evitando que ameaças possam ocasionar prejuízos, além da perda de credibilidade junto ao mercado ou clientes. Sendo assim, surge utilização de modelos e normas que zelam por princípios básicos da informação, destacando-se a disponibilidade, confidencialidade e integridade. Porém percebe-se a necessidade de utilização de novos princípios, que auxiliam na garantia da segurança da informação, associados muitas vezes por evolução das ameaças, que podem ser inseridos no contexto como sendo intencionais ou não.

Mesmo diante da consideração da criticidade dos riscos, muitas organizações não contam com aplicação de planos adequados na área de segurança da informação e alinhamento dos mesmos aos negócios, sendo utilizadas medidas de segurança para atender apenas forças externas, normalmente definidas de obrigações legais e regulamentares, como descreve Albuquerque Junior e Santos (2014).

Diante do cenário exposto, percebe-se inevitavelmente a necessidade de aplicação de técnicas de mensuração e análise de indicadores de melhores práticas para o gerenciamento de recursos e componentes da administração em *Data centers*, Ono (2014) relata que

indicadores do ambiente físico de um *Data center* objetivam a eficiência dos ativos e abrangem várias áreas de interesse da organização. Pesando desta forma é inevitável ampliação da área de Tecnologia da Informação para uma nova estrutura mais abrangente definida como Tecnologia da Informação e Comunicação. Gerando, assim, uma nova incumbência, responsável pelo gerenciamento de informação nas organizações, a qual é detalhada por Castells (2009).

A definição de complexidade para implantação e utilização de modelos de maturidade mais utilizados no mercado, abre uma oportunidade para rever modelos associados aos processos, controles, normas e *frameworks*, adequando-os às necessidades específicas de cada organização, uma vez que mesmo não implantando todos os processos ou controles, a organização já consegue obter uma melhoria em seus processos e um maior alinhamento entre a área de TIC e áreas estratégicas das organizações. No entanto, observa-se a necessidade, em algumas situações, de mudança na estrutura organizacional para conseguir atingir as melhorias, como demonstram os resultados de Prado *et al.* (2016).

Traduzir as necessidades de demandas por serviços associados à área de TIC tem aumentado os investimentos em soluções tecnológicas e complexos centros de processamento de dados. O Brasil, em 2015, possuía o sexto maior mercado de TIC do mundo, de acordo com empresa de consultoria IDC – International Data Corporation, considerada com líder no segmento de tecnologia da informação e comunicação, fatos que foram compartilhados por Ono (2014). Percebe-se com isso a necessidade de investimentos não só nos recurso de hardware para montagem dos complexos *data centers*, mas também investimentos em processos e pessoas, como estudo de variável, uma vez que as pessoas estão envolvidas no processo de criação, armazenamento e descarte das informações.

Saleh (2011b) aponta que é possível mensurar a segurança da informação nas organizações através de um modelo de maturidade, no entanto, destaca a necessidade de mais pesquisas, a fim de ter mais subsídios e avanços na área. Neste sentido, Proença e Borbinha (2018) apontam também necessidade de se aferir a maturidade da segurança da informação, entretanto ressaltam que os principais modelos de maturidades existentes não atendem completamente aos aspectos de segurança da informação, por não levarem em consideração todos os possíveis controles definidos pelo modelo, além disso falta definição dos aspectos que são mais relevantes e exigem, na maioria das vezes, uma grande quantidade de implementação de controles que são complexos para serem praticados nas organizações.

1.1 Motivação e justificativa

A concepção deste estudo surgiu da necessidade das organizações buscarem a melhoria na área da segurança da informação em consequência do aumento de ameaças internas e externas existentes. Verificar e adequar as melhores práticas a fim de garantir e mensurar um melhor controle passou a ser essencial não apenas para a área de TIC, mas para existência da organização no atual mundo globalizado e de alta concorrência. Sendo considerado com desafio árduo que precisa ser vencido (LESSING, 2008).

Lessing (2008) ressalta que mais da metade das organizações não tem a capacidade de capturar e armazenar de forma segura e confiável grande volume de dados. A crescente utilização dos dispositivos móveis, redes sociais e serviços de computação em nuvens, resultam em mudança de paradigma nas organizações, que buscam manter a competitividade do mercado, ao garantir segurança no armazenamento de todo o tipo de informação, oriunda de diversas fontes. Estas exigências tornam necessária a utilização de meios de controles, normas e padrões de segurança, de forma a evitar manchar a imagem e reputação da organização junto aos clientes e sociedade.

Para as organizações, torna-se necessária a busca de conhecimento dos especialistas em segurança da informação, com objetivo de analisar e auditar sistemas de maneira eficaz, propondo ou adequando soluções com intuito de atender as necessidades operacionais. Chatzipoulidis e Mavridis (2010) corroboram do pensamento que as organizações deveriam começar a perceber que a gestão da segurança da informação é uma disciplina, que precisa ser trabalhada desde especialistas a qualquer pessoa que tenham acesso à informação.

Outro fator importante a ser mencionado é que as organizações não estão preparadas para ataques, principalmente quando considerados os *data centers.* Lima (2018) descreve que estudos realizados pelo instituto Ponemon demonstram que invasões a *data centers* causaram inatividade de 34% no ano de 2013, sendo 19% a mais se comparado ao ano de 2010. Lima (2018) também aponta que em 2016, devido a ataques contra *data centers*, mais de um terço das organizações obtiveram perdas substanciais de clientes, oportunidades e receitas em mais de 20%, conforme relatório da Release (2017). Ciente da grande importância das informações para o sucesso e sobrevivência das organizações, entende-se os *data centers*, como o coração tecnológico das empresas.

Por estes motivos, este estudo aplicou a metodologia de pesquisa-ação-participativa implementando a estratégia PriMaSIA, descrita por o acrônimo de Priorização e Maturidade em Segurança da Informação Adaptável, desenvolvida por Alencar (2019) em sua tese de doutorado. Foi analisada a estratégia, descrevendo como funcionam as métricas para os controles definidos, focando na segurança da informação, bem como a exploração de novas possibilidades, como aplicar a estratégia Primasia direcionando-a para a análise em *data centers*. O cenário escolhido, análise da maturidade de segurança da informação dos *data centers,* foi idealizado devido a importância de métricas de maturidade da segurança da informação, em especial para analisar *data centers,* como já mencionados, e pela carência de materiais na literatura.

O estudo permitiu que organizações pudessem implementar a estratégia a fim de aproveitarem as oportunidades que aplicações de normas e procedimentos podem trazer para os negócios, otimizando a eficiência e qualidade dos seus serviços, de forma a obter maiores índices de performance e desempenho, sem esquecer a segurança da informação com papel fundamental para crescimento da organização.

É importante salientar o papel da TIC como setor estratégico da organização, trazendo, dentre outras vantagens, redução de custo, com a identificação de novas estratégias de negócio mais eficientes e rápidas (PRASAD; SHETH, 2013), que só podem ser alcançadas se os princípios da segurança da informação estiverem bem definidos e aplicados a todos os setores que manipulem informação, sendo ela interna ou externa a organizações, garantindo desta forma uma maior eficiência e segurança.

1.2 Pergunta de pesquisa

Esta pesquisa pretende explorar as dificuldades e lacunas supracitada como uma oportunidade para expandir conhecimento e explorar tal paradigma respondendo o questionamento:

Como avaliar o nível de maturidade da segurança da informação nos ambientes de *data center*s corporativos?

O presente trabalho pretende resolver o questionamento guiando-se pelo objetivo geral que é desmembrado em mais cinco objetivos específicos que podem ser vistos como passos para aplicação da estratégia a fim de se chegar à solução.

1.3 Objetivos

A seguir serão apresentados o objetivo geral e os específicos que nortearam a condução deste projeto.

1.3.1 Objetivo Geral

O objetivo principal deste projeto é analisar o nível de maturidade dos ambientes de *data centers* corporativos no que tange à segurança da informação, através da aplicação estratégia Primasia elaborada por Alencar (2019) em sua tese doutoral.

Para o atendimento, foi aplicado de forma independente a estratégia Primasia (ALENCAR, 2019), conforme descrito pelo autor criador da estratégia, fazendo as devidas alterações para sua aplicação na área de *data centers*.

1.3.2 Objetivos Específicos

Para atendimento da pergunta de pesquisa e do objetivo geral, o presente trabalho passará por cinco objetivos específicos. Tais objetivos são descritos a seguir:

- Realizar levantamento bibliográfico sobre normas e modelos de maturidades associados a segurança da informação, que permitem a utilização em ambiente de *data center*, a fim de melhor compreender o assunto a ser estudado.
- Apresentar suporte teórico consolidando uma visão de como a avaliação da maturidade pode auxiliar no gerenciamento da informação.
- Identificar e priorizar controles da estratégia Primasia focando-a na avaliação da segurança da informação em ambientes de *Data center*s, através da aplicação de forma independente da estratégia Primasia.
- Gerar subsídios que permitam acompanhamento de estágios de classificação da organização, baseada em controles que foram priorizados com a aplicação da estratégia, a fim de definir o nível de maturidade da organização, considerando os aspectos relacionados a segurança da informação aplicados em ambiente de *data center*.
- Aplicar em novo contexto a especificação da estratégia Primasia de forma independente para área de *Data centers* em ambientes reais.

1.4 Metodologia

A pesquisa realizada no trabalho utilizou a metodologia de pesquisa-ação para o presente estudo, estando amparada pelos princípios de compreensão da interpretação humana dos fatos, como metodologia de pesquisa para a resolução de problemas.

Para Thiollent (2000), nem toda pesquisa pode ser considerada pesquisa-ação. Thiollent (2000), define a metodologia de pesquisa-ação como sendo:

> "Uma pesquisa pode ser qualificada de pesquisa-ação quando houver realmente uma ação por parte das pessoas ou grupos implicados no problema sob observação. Além disso, é preciso que a ação seja uma ação não trivial, o que quer dizer uma ação problemática merecendo investigação para ser elaborada e conduzida (THIOLLENT, 2000, p.15)".

O modelo de pesquisa-ação possui características próprias que precisam ser ressaltadas, a principio a mesma deve produzir conhecimento sobre o tema a ser estudado. E isso é a própria intenção científica, seja qual for a área de pesquisa o tema de estudo ou o instrumento metodológico. Não existe pesquisa na ação se esta não se caracterizar como produção de conhecimento (JANKE, 2005).

De modo geral, a pesquisa-ação possui algumas características em termos práticos, sendo necessário algumas etapas pré-estabelecidas as quais, segundo Vasconcellos (1997, p. 126), compõem os requisitos indispensáveis ao projeto de pesquisa que são:

> - a existência de uma pergunta à que se deseja responder;
> - a elaboração (e sua descrição) de um conjunto de passos que permitam obter a informação necessária para respondê-la;
> - a indicação do grau de confiabilidade na resposta obtida.

Thiollent (2000) afirma que, do ponto de vista científico, a metodologia da pesquisa-ação possibilita a organização da pesquisa social sem enfatizar os procedimentos convencionais de produção de dados, permitindo maior flexibilidade tanto dos meios de aplicação como na concepção.

Para fundamentar a construção do estudo foi definida da pergunta à que se deseja responder:

"Como avaliar o nível de maturidade da segurança da informação nos ambientes de *data center*s corporativos?"

Em seguida foi elaborado o conjunto de cinco macro passos que permitiram a obtenção de resultados para responder a pergunta de pesquisa objeto estudo deste trabalho.

Em síntese, os macro passos deste trabalho foram:

1. Análise da literatura existente através da revisão bibliográfica Ad-Hoc, esta etapa serviu para a definição dos problemas, verificar possíveis soluções e criação da fundamentação teórica.
2. Seleção da Estratégia Primasia (ALENCAR, 2019) para resolução do problema proposto.
3. Adaptação da Estratégia Primasia (ALENCAR, 2019) focando-a para a análise e avaliação dos aspectos da segurança da informação em *data center*s;
4. Verificação e classificação de correlação dos 114 controles da ISO/IEC 27.001 e 27.002, principais normativos da área de segurança da informação, com a área de *data center*s. Esta correlação categorizou os controles em "diretamente relacionado", "parcialmente relacionado" e "pouco relacionado" através da aplicação de questionários com especialistas.
5. Aplicação da Estratégia Primasia adaptada para *Data center*s em organizações. Esta etapa serviu como avaliação do modelo adaptado proposto.

A revisão bibliográfica também analisou as normas existentes na família ISO/IEC 27.000, família de normas que abordam a área de segurança da informação, como detalha Palma (2016). Foi também analisada a definição e características dos níveis de maturidade utilizados pelo COBIT 4.1, facilitando entendimento para aplicação da Estratégia Primasia. Segundo Alencar (2019), a Estratégia Primasia pode ser aplicada com qualquer arcabouçou teórico de controles e de estrutura de níveis de maturidade. Porém o autor utilizou as normas da família ISO/IEC 27.000 e o COBIT devido à sua aceitação e utilização na indústria, bem como por ser, nesta área, os arcabouços mais utilizados e testados. Tal configuração também foi seguida nesta presente pesquisa.

A metodologia de desenvolvimento utilizada neste trabalho envolveu as etapas de aplicação prática da estratégia Primasia de forma independente, foi confeccionado um questionário que permitiu a classificação dos controles utilizados na estratégia, buscando,

através da análise dos formulários de pesquisa, uma classificação de prioridade para os controles que são diretamente relacionados, parcialmente relacionados ou pouco relacionados, voltado ao assunto da segurança da informação aplicado ao ambiente *data center*.

A priorização dos controles foi feita após a análise dos formulários respondido por especialistas da área de tecnologia da informação e comunicação que trabalham diretamente com ambientes de *data center*, utilizando de mecanismo de peso para realizar ponderação e assim melhor classificar o controle. Tais ações são detalhadas em seção específica, que aborda a aplicação e análise dos citados questionários.

Para aperfeiçoar o estudo foi aplicado um levantamento com organizações que possuem *data center* próprio, com objetivo de definir o nível de maturidade da organização, apontar os pontos mais fracos, permitindo correções a fim de alcançar melhorias. As organizações foram do segmento do comércio de médio a grande porte, segundo classificação do IBGE (Instituto Brasileiro de Geografia e Estatísticas, 2018) por número de empregados, como critério de classificação do porte das empresas representado no Quadro 1.

Quadro 1 – Critério de Classificação do Porte de Empresas pelo Número de Empregados

Classificação	Número de Empregados	
	Indústria	Comércio e Serviços
Micro	até 19	até 09
Pequenas	de 20 a 99	de 10 a 49
Médias	de 100 a 499	de 50 a 99
Grandes	acima de 500	acima de 100

Fonte: Adaptada do IBGE (2018)

Foi aplicada a estratégia Primasia em duas empresas da região metropolitana do Recife, capital de Pernambuco, localizado no país Brasil. Como fonte de informações para aplicação da metodologia.

A primeira organização avaliada, foi uma rede de lojas do varejo do grande Recife com mais de 500 funcionários sendo considerada uma empresa de grande porte. O *data center* foi implantado a cerca de 20 anos.

A segunda organização também foi uma rede de lojas do varejo do segmento de peças automotiva do grande Recife, contendo cerca de 60 funcionários, utilizando um *data center* implantado a cerca de 10 anos, sendo considerado uma empresa de médio porte.

1.5 Riscos, benefícios e dificuldades

A avaliação de um nível de maturidade em segurança da informação é uma área que enfrenta ainda muitos riscos técnicos que devem ser abordados, por exemplo, a veracidade não assegurada gera incerteza nos resultados obtidos (ZHANG, 2006). Outro risco a ser considerado está intrinsicamente associado aos modelos serem muito bem estruturados, gerando, em algumas situações, o excesso de formalismo devido à complexidade da abordagem, o que torna muitas vezes inviável à aplicação e melhoria contínua dos processos, como abordam Silva Neto, Alencar e Queiroz (2015) e Prado et al. (2016). Além disso, existem problemas adicionais como privacidade, proveniência e modelagem que pode por em risco a segurança (ZHANG, 2006).

Com este pensamento, espera-se que uma visão sistêmica da área de segurança da informação, envolvendo o melhor entendimento do nível de maturidade no qual a organização se encontra, bem como uma melhoria no processo de gestão da organização, seja essencial para a análise e aplicação de um modelo de maturidade de segurança da informação.

Benefícios esperados estão associados à contribuição para comunidade acadêmica e principalmente para as organizações, no tocante de utilização da estratégia a fim de determinar o nível de maturidade em segurança da informação nos *data centers* das organizações, bem como, gerar forma de se analisar a situação da organização, através da possibilidade de comparar o nível dela com outras. Tal consideração, pode ser útil para atribuir um nível de qualidade agregado a organização.

Dificuldades foram encontradas em conseguir material bibliográfico para o tema recente e encontrar gestores que contribuíssem com informações para aplicação prática da estratégia, a fim de permitir um levantamento formal mais próximo dos utilizados no mercado em busca de alcançar os objetivos.

1.6 Organização do trabalho

O trabalho prossegue dividido no conjunto de Capítulos descritos a seguir:

No Capítulo 2 foi apresentado a fundamentação teórica, inserindo, principalmente, os assuntos: Segurança da Informação, Modelos de Maturidade, Normativos da área de Segurança da Informação, *Data center*s e a Estratégia Primasia.

Para o Capítulo 3 foi feito a abordagem de classificação dos controles da estratégia Primasia adaptado para ser utilizado em ambiente de *data center*

Para Capítulo 4 foi realizado a aplicação prática com os estudos de caso reais aplicados em duas organizações brasileiras localizadas em Pernambuco.

Finalizando com o Capítulo 5 será apresentada a considerações finais do trabalho, abordando as conclusões objetivos alcançados e possíveis trabalhos futuros.

Como complemento, tem-se as referências, apêndices e anexos do presente trabalho.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os principais conceitos utilizados neste trabalho. Primeiro, são apresentados, os conceitos segurança da informação, normas de segurança da informação e modelo de maturidade que servirá de base para este estudo. Em seguida são abordados conceitos sobre *Data centers* onde será enfatizado aspectos de segurança. Por último, será apresentada a estratégia Primasia, como principal componente para apresentação dos resultados do estudo realizado.

2.1 A Evolução da Segurança da Informação

A sociedade atual está cada dia mais conectada por redes, proporcionadas por organizações e pessoas, criando uma competitividade que necessita de ações em segurança e tomadas de decisões, alinhadas muitas vezes a necessidade do indivíduo ou de uma organização. A forma de obter e guarda o conhecimento é imprescindível, para crescimento dessas organizações. A segurança da informação torna-se fator primordial para garantia do crescimento com credibilidade para organizações, onde muitas dessas informações envolvem dados pessoais de seus clientes e informações confidenciais das organizações, utilizadas para planejamento estratégico.

Diante do exposto, a informação tornou-se um dos mais valiosos ativos das organizações, uma vez que as informações manuseadas nas corporações podem gerar lucro e se mal administradas prejuízos, assim como o setor que gerência essas informações tornou-se estratégico para organizações (CASTELLS, 2009; SEMOLA, 2013). O termo “Segurança da Informação” tornou-se mais utilizado na sociedade, quando Castells (2009) definiu um novo ambiente denominado por ele como “Era da Informação”. O novo contexto esboçado, possibilita a ampliação dos papéis da Tecnologia da Informação (TI), e define de forma mais ampla o termo de Tecnologia da Informação e Comunicação (TIC), criando uma nova responsabilidade para o gerenciamento da informação como um bem, com valor que torna-se difícil muitas vezes de ser mensurável. Consequentemente, estas informações tornam-se extremamente cobiçadas, e diversos tipos de ameaças buscam alcançá-las. A nova forma de classificação da informação, gerou a alta valorização da informação, tornando um bem decisório e peça fundamental nas estratégias organizacionais (RAMOS, 2007; ARAÚJO, 2009; FERREIRA, 2009).

Fontes (2012) compartilhava o pensamento, ressaltando que a informação é um recurso único que atualmente move o mundo, ofertando conhecimento do passado e guiando a forma para onde chegaremos ao futuro. Sendo considerada também a informação um recurso, crítico, único e intangível, para realização do negócio e execução dos mais diversos planejamentos das organizações, necessitando assim ser protegido.

Inicialmente os problemas de segurança da informação eram restritos ao acesso físico, basicamente controlado pelos militares, uma vez que a computação era restrita a essa parte da sociedade (LANDWEHR, 2001). Segundo Côrte (2014) o assunto vêm sendo discutido há mais de 70 anos, referindo-se ao artigo publicado por Edward Uhier Condon intitulado *Science and Security* (CONDON, 1948), o qual discute temas como a tradição da ciência em compartilhar conhecimentos, em face dos acontecimentos da Segunda Guerra Mundial e do pós-guerra, quando talvez as informações mais bem protegidas tenham sido aquelas relativas à confecção da bomba atômica. O mesmo artigo citado por Côrte (2014) menciona questões de equilíbrio, para que não ocorram problemas de segurança em excesso, a ponto de não se encontrar, dentro da própria organização, informações necessárias à tomada de decisão.

Com o surgimento dos computadores, a tecnologia da informação tornou-se uma grande fonte de oportunidades, mas também de riscos. Os *data centers* da década de 50 eram grandes e com poder computacional pequeno comparados com os da atualidade. Os mesmos eram utilizados em grandes salas fechadas com ar-condicionado, e operados por poucos profissionais, com elevado conhecimento técnico. Na sua grande maioria não existiam usuários que fossem autenticados, por que não existia politica de autenticação com o nome do usuário e senha para se ter acesso aos seus sistemas. Existam inúmeros problemas como interrupção de serviços, erros nos aplicativos, mau funcionamento do hardware, que eram usualmente resolvidos pelos próprios profissionais da empresa que operam esses equipamentos nos *data center*. Essas características faziam com que os eventuais problemas de segurança fossem mais rapidamente percebidos e prontamente monitorados uma vez que os computadores estavam isolados sem conexão de rede. A segurança da informação limitava-se aos técnicos e operadores através de acesso físico aos computadores.

Com o aumento de forma exponencial da utilização dos computadores citado por Castells (2009), impulsionado pela academia, governo e, posteriormente, as organizações, através da introdução dos computadores de menor porte, os usuários passaram a contar com computadores da organização através dos terminais burros, ou seja, sem capacidade de processamento local. Ao final dos anos 60 surgem os computadores que foram interconectados por intermédio de linhas telefônicas dedicadas. Essa inovação permitiu, pela

primeira vez, os sistemas computacionais gerenciados por computadores localizados em *data centers* distintos fossem acessados de fora da organização, e assim ficaram expostos ao mundo exterior. A partir deste momento, tornou-se possível interagir com outros computadores, de qualquer lugar físico. Com a expansão das redes e dos terminais remotos, os controles de segurança com foco apenas no acesso físico a salas de computadores, já não eram suficientes.

Surgem assim outros problemas com a segurança dos computadores, criada com a necessidade e o compartilhamento do processamento de informações e de usuários, que poderiam estar fisicamente em diversos lugares na organização. Criou-se então a possibilidade de inserir, de alterar e de apagar dados nos sistemas remotamente, porém, necessitavam ser previamente autenticados pelos sistemas, por um usuário e uma senha individual. Este fato alinhado a padronização dos computadores para atender a demanda crescente, levou ao desenvolvimento de sistemas operacionais de tempo compartilhado. Tais sistemas, em sua concepção ideal, deveriam ser desenvolvidos de forma a garantir o referido compartilhamento de forma segura, tendo ciência de que o compartilhamento de recursos (terminais de acesso, programas, impressoras e dispositivos de armazenamento de dados) gera possíveis problemas e vulnerabilidades (BENZ, 2008).

No inicio dos anos 80, a Internet já era utilizada principalmente por profissionais da área computacional, academia e organizações de sistemas, Nesse período começou a ser fomentada a questão sobre a "segurança em computador" conforme citam Pfleeger, Pfleeger e Margulies (2015). Ciente deste crescimento de utilização, cada vez mais tornava-se necessário a implementação da segurança em computador nas organizações, garantindo que dados que serão transformados em informação em algum determinado momento estejam seguros. Segundo Alencar (2019), essa preocupação coincide com a cadeia de valor da economia citada por Castells (2009). Onde no mesmo período "os códigos maliciosos e vírus não eram comuns, os crimes cibernéticos raramente eram notícia de jornal e as pessoas não tinham noção das ameaças por meio de computador" (MENDONÇA, 2007, p. 64).

Reforçam esse pensamento Joia e Neto (2004), quando citam a evolução da economia associado ao da segurança da informação, compartilhando de conhecimento, que no inicio da década de 80, a tecnologia da informação e comunicação, não era mais utilizada apenas como uma ferramenta de processamento de dados, que geram um resultado mais rápido, e sim como uma nova maneira de utilização do computador a fim de possibilitar alavancar o negócio e fidelizar o cliente, através das criações de estratégias extraídas das informações

processadas de dados coletados. Porém, Joia e Neto (2014) e Alencar (2019), ressaltam a necessidade de maiores proteções associada a segurança.

Neste ambiente que se formava, dependendo da falha na estratégia de gerenciamento das informações, poderiam acarretar em consequências que vão de acúmulos de prejuízo e até o encerramento de atividades de algumas organizações. Uma vez que aquele que obtém e consegue auferir conhecimento das informações do concorrente primeiro, teria uma grande vantagem sobre os mesmo no mercado (NOBRE, 2009). Sugiram assim varias formas de garantir a segurança da informação pensando inicialmente no princípio de confidencialidade. Alencar (2019) corrobora de pensamento, que mesmo que não fosse reconhecida com esse nome, a segurança da informação iniciava seus primeiros passos, começando a expandir para uma área de estudo sistemática da segurança da informação antes não explorada.

Na década de 90 com a expansão da internet, surge outro desafio associado à questão do ambiente. Algumas organizações começaram a perceber o potencial de expansão referente a visão do negócio com grande possibilidade de lucro impulsionado pela possibilidade de abrangência da limitações físicas, conquistadas com a utilização da internet, Porém o aumento dos lucros veio com a necessidade de investimento para diminuir possíveis vulnerabilidades que necessitavam ser combatidas. Diante desta nova realidade exposta, Benz (2008) descreve que diversos documentos e procedimentos foram criados e implementados, na tentativa de fazer com que usuários autorizados tivessem acesso seguro a determinadas informações, garantindo desta maneira, o acesso não autorizado. Alencar (2019) compartilha de conhecimento que entre os primeiros marcos da década de 90 remetidos à segurança da informação têm-se as publicações conhecida como The Orange Book, e a publicação especial número 800-12, em 1995, "*An Introduction to Computer Security: The NIST Handbook*" e a BS 7799 (British Standard).

2.2 Segurança da Informação

A informação torna-se recurso que deve ser considerado como um ativo crítico não apenas pelo valor estimado para realização de negócios ou execução de planejamento estratégico. O fato de estarem armazenadas em formatos digitais, cria uma nova responsabilidade referente aos princípios de segurança dessas informações, sejam elas utilizadas por redes internas e externas de computadores. Uma vez que as informações poderem ser divulgadas, alteradas, apagadas ou mesmo não estar disponíveis por estarem corrompidas, quando necessário para as atividades do negócio (FERREIRA, 2003, p. 2).

Com uma importância cada vez maior para as organizações, as informações precisam ser mantidas e protegidas, a fim de garantir os princípios da segurança da informação alcançados através integridade, disponibilidade e confidencialidade, para que se mantenha a continuidade das atividades de negócio e até mesmo a existência da organização.

2.2.1 Definições e termos de segurança da informação

Na literatura o conceito de segurança da informação ainda está em processo de consolidação, e existem várias definições que o abordam com diferentes contextos e focos.

Sêmola (2003, p. 43) define a segurança da informação como sendo "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua disponibilidade". Nesse contexto ele considera a informação como um bem que deve ser considerado e protegido, para isso a aplicação de controles de segurança que reduzam riscos a níveis adequados, viáveis e administráveis.

Ferreira (2003, p. 1) define que "a segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades".

A segurança da informação pode ser considerada como uma estrutura de "blindagem" para a proteção do ativo intangível de uma organização, e "engloba um conjunto de ações que devem ser planejadas e programadas de forma a abranger as questões técnicas, comportamentais e, também, jurídicas" (PINHEIRO; SLEIMAN, 2009, p.27.).

A NBR ISO/IEC 27.002:2005 define:

> "Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio."

Vários autores propuseram definições para a segurança da informação e estudaram suas características:

- Zapater e Suzuki (2005) corroboram de conhecimento, que a segurança da informação está associada ao processo de identificação das possíveis vulnerabilidades e a gestão dos riscos envolvidos com os diversos ativos informacionais de uma organização, independentemente da forma ou da estrutura em que são compartilhados ou armazenados.

- Ramos (2006) definiu segurança da informação como uma componente conjugada ao uso de computadores, estabelecendo uma meta a ser atingida, a fim de proteger os sistemas de informação, contra ameaças existente por meio do principio básico da segurança da informação: confidencialidade, à integridade e à disponibilidade.

- Peltier (2001), entende que a segurança da informação está vinculada ao uso de controles de acessos físicos e lógicos para os dados, com objetivo de garantir a utilização de forma adequada da informação de forma a não permitir modificações acidentais ou que não sejam autorizadas, prevenir e não permitir a destruição, quebra de sigilo, perda ou acesso aos registros de informação de forma automática ou manual, realizados por procedimentos e pessoas não autorizados.

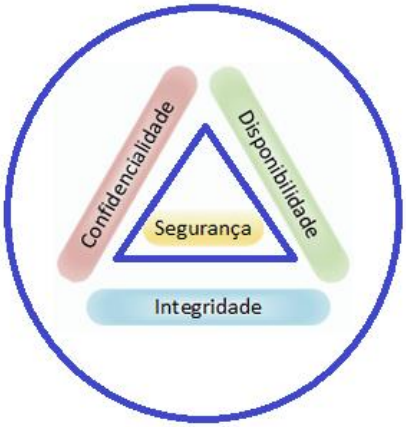
- O *National Institute of Standards and Technology* (NIST) define o propósito da segurança computacional (NIST *Handbook*, 1995, p. 9 - tradução livre do autor):

> "O propósito da segurança computacional é proteger os valiosos recursos de uma organização, tais como informação, hardware e software. Através da seleção e aplicação de medidas de controle apropriadas, a segurança auxilia na missão da organização protegendo os seus recursos físicos e financeiros, reputação, posição legal, empregados e outros recursos tangíveis e intangíveis."

A definição "segurança da informação", é visto com muitas interpretações, por se tratar de um termo ambíguo, podendo em determinadas situações ser tratada como uma prática interdisciplinar adotada para possibilitar um ambiente seguro (segurança da informação como um meio), como pode ser definido como conjunto de característica que a informação adquire ao ser alvo de uma prática da segurança (segurança da informação como fim) (SÊMOLA, 2003, p. 44).

A premissa fundamental da segurança da informação é de não existir uma maneira de segurança absoluta. Jamais serão tratadas todas as possíveis situações de prejuízo. Principalmente por não se ter como gerenciar, um número razoável de situações inesperadas (RAMOS, 2006, p. 22). Ramos (2006) acrescenta ainda que segurança da informação é traçada sobre três pilares: confidencialidade, integridade e disponibilidade.

Figura 1 – Pirâmide ou tríade da Segurança da Informação



Fonte : Adaptada de RAMOS, 2006, p. 21

A NBR ISO/IEC 27.002 também estabelece como principal objetivo da segurança da informação, a preservação da confidencialidade, integridade e disponibilidade da informação (ASSOCIAÇÃO, NBR ISO/IEC 27.002, 2005). Esses termos foram assim definidos na NBR ISO/IEC 27.001:2006 (ASSOCIAÇÃO, NBR ISO/IEC 27001, 2006):

- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

- Integridade: propriedade de salvaguarda da exatidão e completeza de ativos;

Em pesquisa literária de aprofundamento aos três princípios confidencialidade, disponibilidade e integridade, foram encontrados diversos documentos (ABNT, 2006; ARAÚJO, 2009; DA SILVA, 2009; SÊMOLA, 2013; CÔRTE, 2014; ALENCAR, 2019). Alencar (2019) sintetiza os mesmos princípios como base para garantir a segurança das informações:

- Confidencialidade: busca limitar o acesso somente às entidades (pessoas, sistemas, objetos) autorizadas, garantindo que informação esteja disponível para o grupo autorizado e proibido o acesso às demais;

- Disponibilidade: propriedade que pretende garantir que a informação, esteja disponível para o uso de um grupo autorizado, sempre que solicitada;

- Integridade: propriedade que garante que a informação manipulada mantenha as características originais, ou seja, que os dados obtidos estejam íntegros. Pode ser vista como a capacidade de verificação se modificações intencionais ou acidentais dos dados ocorreram.

Segundo Pfleeger, Pfleeger e Margulies (2015), que tratam o assunto como "segurança de computador" afirma que harmonia só vai existir, se as três características fundamentais supracitadas, funcionarem de forma conjunta, e que se relacionem de forma a se obter um resultado coerente e eficiente. Alencar (2019) corrobora de conhecimento apresentando o pensamento que foi compartilhado por Laureano e Moraes (2005) o qual descreve que a combinação apropriada dos itens confidencialidade, disponibilidade e integridade serve como base para que as organizações alcancem suas metas.

Levando em consideração a ampliação dos requisitos da segurança da informação, (CÔRTE 2014; ALENCAR 2019), compartilham de mesmo pensamento adicionando mais duas propriedades. A primeira está voltadas as fontes das informações e a segunda ao controle de acesso. Segundo Alencar (2019, p.58) essas propriedades já são utilizadas em algumas abordagens (MARCIANO; LIMAMARQUES, 2006; TIPTON; NOZAKI, 2016) sendo elas:

- Autenticidade: propriedade que garante que a informação é autêntica, provinda das fontes anunciadas;

- Não repúdio: propriedade que associa ações e acessos a usuários e entidades de forma inquestionável, ou seja, o ato realizado não pode ser negado por quem o realizou.

Para Côrte (2014, p.70) o sistema que administra as informações deverá atentar para utilização além dos cinco itens citados, definindo assim os pontos complementares:

- Confiabilidade/Credibilidade propriedade que valida habilidade em prestar o serviço prometido com confiança e precisão (COOK, 2000). Para engenharia de software, confiabilidade é a capacidade do produto de software manter um nível de desempenho especificado, quando usado em condições especificadas.

- Auditoria: propriedade que consiste em rastrear e analisar os diversos passos que uma pessoa ou processo realizou ou a que uma informação foi submetida, visando identificar características como: os participantes, meios, horários e locais de cada fase;

- Legalidade: propriedade que visa garantir a legalidade da informação perante normas em vigência, visto que a mesma se adere a um sistema de legislação;

- Privacidade: propriedade que restringe e controla a exposição e disponibilidade das informações. Uma informação privada deve ser vista, lida ou alterada somente pelo seu dono ou grupo que detêm o privilégio;

Embora não estabeleça hierarquia entre os requisitos dos princípios de controle Côrte (2014) ressalta que, dependendo do caso, pode-se perceber maior relevância de um sobre os outros. Como exemplo, pode ser citado as aplicações de e-commerce ou operações bancárias realizada por dispositivos móveis, computadores ou terminal de atendimento, onde o requisito de disponibilidade tem sido o item mais requerido pelos usuários, porém a existência da correlação entre os diversos princípios é uma necessidade como demonstra, entre outros, Laureano e Moraes (2005), Shirey (2007), Alencar (2008) e Sêmola (2013) ressaltam que a confidencialidade depende da integridade, uma vez que perdida a integridade de um sistema, as estruturas que controlam a confidencialidade tornam-se duvidosas. Alencar (2019) relata que integridade depende da confidencialidade, pois se algum dado confidencial for perdido, pessoas não autorizadas terão acesso ao sistema, colocando em risco assim, os mecanismos de integridade que podem ser desabilitados. A disponibilidade e a auditoria dependem da integridade e confidencialidade, visto que de nada adiantará ter todos os dados disponíveis sempre que necessário, assim como realizar a correta auditoria e ter todos os seus registros históricos, se os dados são inválidos, seja pela falta de integridade ou confidencialidade da informação.

Alencar (2008) e Sêmola (2013) dividem de pensamento que cada princípio citado gera um custo adicional para a organização ao ser implantado, sendo necessário a validação feita

por um estudo da viabilidade associada aos critérios de segurança que serão abordados, uma vez que, nem sempre, é possível e implementar e prover todos os itens segurança para todas as informações. Em algumas situações podem até não ser vantajoso, devido ao investimento e tempo necessário. Além disso, os mesmos ressaltam, que diversos sistemas, principalmente os sistemas antigos, conhecidos também como sistemas legados, os quais não são mais atualizados para inclusão de informação, não foram concebidos com a preocupação de garantir a segurança a si mesmo e as informações as quais manipulam, o que dificulta, ou torna não vantajoso, a implantação dos princípios pretendidos, impossibilitando que a segurança por meios técnicos seja deficiente.

A partir das diversas definições dadas para a segurança da informação, pode-se concluir que o seu gerenciamento exige uma visão bastante abrangente e integrada de vários domínios de conhecimento, englobando aspectos de gestão de riscos, de tecnologias da informação, de processos de negócios, de recursos humanos, de segurança física e patrimonial, de auditoria, de controle interno e também de requisitos legais e jurídicos. Ramos (2006), define que uma visão lógica sobre a segurança da informação, é aquela que compreende todo esse universo, entretanto, cita que “a maioria das organizações possui diferentes áreas para controlar os diferentes aspectos relacionados segurança da informação” (RAMOS, 2006, p. 26).

Para que a segurança da informação esteja adequada para uma organização, deve ser levado em consideração o bom senso financeiro, considerando as interações entre alguns agentes principais e certos fatores. Ramos (2006) também relaciona, que os principais agentes e fatores são: o valor da implantação, o nível de ameaça, o grau de vulnerabilidade, o impacto da ameaça e o risco a ser considerado.

O valor pode ser avaliado através de propriedades abstratas como, a imagem da organização ou valores a serem investidos. Ainda segundo Ramos (2006), é considerado como ativo, tudo aquilo que tenha valor e que necessita de proteção de alguma maneira, portanto é considerado que as proteções são; práticas, procedimentos ou mecanismos, utilizados para proteger os ativos contra ameaças, reduzindo ou eliminando as vulnerabilidades, ou até mesmo limitar o impacto associado ao incidente. Já a ameaça é tudo o que tem potencial para comprometer os objetivos da organização, de maneira a causar algum tipo de dano aos ativos, estando associada à ausência de mecanismos de proteção ou a falhas em mecanismos existentes para proteção. O impacto é mensurado, pelo tamanho do prejuízo que a confirmação de uma determinada ameaça poderá causar. Já o risco é

considerado como uma medida, que indica a probabilidade de uma determinada ameaça se concretizar, combinada aos seus impactos.

Ao citar que “a interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de controlar o acesso. Sendo que muitos sistemas de informação não foram projetados para serem seguros” (ARAÚJO 2009 p.41), reforça a necessidade de implantação de mecanismos de proteção da informação, além da tecnologia, por incorporar as características de segurança desde os princípios dos projetos. Desta maneira é possível a criação de produtos e serviços com uma quantidade menor de vulnerabilidades.

2.3 Modelo de Maturidade

2.3.1 Visão Geral

Os modelos de maturidade foram incialmente desenvolvidos para avaliar e definir métricas para se obter conhecimento, principalmente por tratar de um bem intangível, depois começaram a ser explorados em outras áreas como segurança da informação e gestão de conhecimento.

A definição do modelo de maturidade é muito amplo e ambíguo, existem muitas definições. Para Leal (2008) os modelos de maturidade são mecanismos capazes de quantificar numericamente a maturidade. Os modelos ajudam na elaboração de processos, indicando as melhores práticas, e auxiliam através de métricas e estágios para que as organizações se desenvolvam de forma constante. O modelo de maturidade descrito por Kerzner (2017), é referenciado como sendo um conjunto de procedimentos e processos, que aumenta a probabilidade de sucesso, baseados na premissa de repetição e estabelecimento de estágios a serem implementados. Prado e Oliveira (2018) afirmam que existe uma relação entre a maturidade e indicadores de desempenho. Alencar (2019) compartilha de pensamento, que quanto maior a maturidade maior a possibilidade de sucesso total ou maior percentual de execução de escopo previsto, com menor atraso e menor custo. Além disso, quanto maior a maturidade, maior será a percepção pela diretoria da organização do valor da área em questão, agregando outro nível de valor à organização (PRADO; OLIVEIRA, 2018).

Almeida Neto (2015) corrobora de mesmo pensamento, o qual definem que o modelo de maturidade pode ser estabelecido por um grupo de atributos que descritos estabelecem a

melhor maneira de se obter resultados esperados para a gestão de processos, onde o objetivo principal desta maturidade, é de obter o grau de refinamento e institucionalização da gestão associada. Baseado nessas definições, um modelo de maturidade pode ser entendido como uma estrutura conceitual, composta por processos bem definidos, por meio do qual uma organização desenvolve-se com objetivo de alcançar um estágio futuro seguro.

Para Mayer e Fagundes (2008), citam que modelo de maturidade representa um guia para a organização, de forma que possibilite buscar excelência em procedimentos e processos, identificando qual nível a organização está e baseado no plano que deve seguir, tendo como objetivo evoluir para um nível sempre acima do atual. Fato corroborado por Nery Júnior, Moura e Texeira Filho (2018), ao inserir que a função do modelo de maturidade é avaliar e identificar em qual nível de maturidade a organização se encontra e depois aplicar o plano de crescimento para se chegar a excelência.

O modelo de maturidade também pode ser descrito, como um conjunto de características, atributos, indicadores ou padrões que representam uma determinada disciplina. O conteúdo do modelo tipicamente exemplifica as melhores práticas e pode incorporar padrões ou outros códigos de prática da disciplina (REA-GUAMAN et al., 2017).

Um nível de maturidade pode ser definido como uma etapa evolucionária essencial na melhoria de processos. Cada nível tem papel de estabiliza uma parte importante dos processos organizacionais. Sendo assim a partir do diagnóstico de um nível, pode ser medida de maturidade de uma organização, tornando possível prever seu desempenho futuro dentro de área determinada Almeida Neto et al. (2015b). Cordeiro (2017) contribui, acrescentando que de acordo com as métricas do modelo utilizado, é possível identificar de forma mais simples quais processos precisam ser restruturados para que se possa alcançar os níveis desejados.

Esse pensamento e semelhante e exposto por Gomes et al. (2016) que acredita que um modelo de maturidade que tem por objetivo auxiliar na melhoria contínua, por meio de processos, para que possam ser implementadas as melhores práticas. Prado et al. (2016) afirmam que via um modelo de maturidade aplicado corretamente na área de TIC, geram pontos de melhoria que são melhor compreendidos e explicados; bem como facilita a visualização do alinhamento aos objetivos estratégicos da organização, baseados na dependência da organização à área de TIC mostrando as virtudes como também os pontos de fraquezas dentro da área, podendo até refletir em pontos fortes e fracos da própria organização como um todo. Vale ressaltar que, para esta dissertação, será adotado o termo

modelo de maturidade para referenciar modelos de estágios (englobando maturidade e/ou capacidade), assim como ocorreu em Almeida Neto (2015).

Segundo Alencar (2019), depois de identificar os processos e controles críticos, o uso de um modelo de maturidade permite a identificação de lacunas que representam risco, devendo mostrá-las para equipe de gestão. Com base nesta análise, planos de ação podem ser avaliados e desenvolvidos para a melhoria dos processos e controles considerados deficientes até o nível de desenvolvimento retificado por Rigon et al. (2014).

Para aferir a área e traçar um caminho para se alcançar o nível desejado pela organização, como mencionado, os modelos normalmente trabalham de duas formas: a representação contínua e a representação por estágios (SILVA et al., 2016).

> "Na representação contínua, uma organização pode optar por melhorar o desempenho de uma única área de processo que esteja relacionada a um determinado problema ou pode trabalhar em diversas áreas independentes que estejam alinhadas aos objetivos de negócio da organização. Do contrário da representação contínua, a representação por estágios oferece um caminho sistemático, estruturado e uniforme, baseado em um conjunto de áreas de processos associados em níveis de maturidade. Quando uma organização atinge um nível de maturidade, considera-se que seus processos alcançaram uma determinada capacidade, ou seja, possuem mecanismos que garantem a repetição sucessiva de bons resultados. A melhoria contínua dos processos da organização é obtida por meio de passos evolutivos entre os cinco níveis de maturidade dos modelos, definidos e numerados" (SILVA et al., 2016, p. 127).

Ressaltam a importância de um modelo de maturidade e avaliação para a área de segurança da informação Rigon (2011) ao afirmar que ter uma PSI implantada na organização não garante a total segurança da informação, sendo necessário medir o nível de maturidade da segurança através de um método de medição e um conjunto de controles que tratem a segurança da informação de forma abrangente. Desta forma, avaliando o estado atual da segurança, os gestores poderão tomar decisões precisas para melhorar os processos e controles internos da organização. Um modelo de maturidade em segurança, abrange implementação de recursos que auxiliem na conservação da segurança da informação, podendo definir quais recursos de segurança podem ser implementados dentro da organização (RIGON; 2013).

Um modelo de maturidade de segurança deve fornecer também um guia para um programa de segurança completo, definido a ordem em que os elementos de segurança devem ser implementados, incentivando o uso de padrões de melhores práticas e fornecendo um meio para comparar programas de segurança, como aborda o The Open Group (2017). Fato corroborado por Silva e Barros (2017) ao afirmar que um modelo de maturidade deve ter objetivo de auxiliar as organizações na avaliação da segurança da informação. Para a

avaliação, o modelo de maturidade deverá apontar o estágio atual, bem como deixa claro o caminho para se chegar aos níveis mais avançados.

A necessidade das organizações implementarem a gestão de risco de forma consistente e sistematizada, torna-se inevitável segundo Silva (2007). Porém, são poucos os estudos na área, como pode ser percebido em Mayer e Fagundes (2008) que afirmavam, em 2008, não se ter um modelo de maturidade voltado à Gestão de Riscos em Segurança da Informação que aferisse ou avalie o nível de maturidade desses processos dentro das organizações, conforme os requisitos de um Sistema de Gestão de Segurança da Informação que seja aplicável a organizações de diferentes portes e segmentos de mercado. Fato que aos poucos vem sido mitigado com publicações na área em períodos mais recentes, como afirma Alencar (2019).

Entre as pesquisas relacionadas ao uso de modelos, com a finalidade de aferir a maturidade da segurança da informação no ambiente corporativo pode-se destacar a classificação dos modelos de feita de forma específicas para a área de segurança, realizada por Rigon et al. (2014) onde foi dividido em cinco grupos os principais modelos utilizados no mercado sendo eles: Orientados a Processo: COBIT e ITIL; Orientados a Controle: ISO/IEC 27.001; Orientados a Produtos: representada pela ISO/IEC 15.408; Orientados a Gerenciamento de Risco: como OCTAVE e ISO 27.005; e, por fim, Orientados a Melhores Práticas: como ISO/IEC 27.002. Sendo o ITIL e o COBIT os mais citados em trabalhos relacionados.

2.3.2 Normas de Segurança da Informação

As Normas de segurança da informação foram criadas inicialmente para permitirem a redução de custos nas organizações e prover uma forma de realizar avaliações dentro do âmbito organizacional. Estas normas de segurança devem fornecer medidas comuns nas avaliações, servindo na realização das avaliações definindo critérios e orientações.
BARKER e NELSON (1988) explicam:

> “As normas de segurança também permitem a compatibilidade entre os produtos dos fornecedores. Compatibilidade que serve como uma conveniência para os clientes e aumenta a concorrência, que eventualmente diminui o custo dos produtos. A menos que a segurança seja barata e conveniente, ela será usada apenas para aplicativos muito sensíveis e muitas aplicações permanecerão desprotegidas. Normas para a segurança da informação não são fáceis de estabelecer. Os requisitos do usuário são diversos; De fato, os requisitos de um usuário podem entrar em conflito com os de outra pessoa”.

No final dos anos 80, acreditavam que não iria demorar para que as organizações aderissem na utilização de normas de segurança com objetivo de reduzir custos e aumentar a qualidade de seus produtos além disso os autores consideraram também a hipótese de uma maior complexidade na aplicação das normas de segurança no futuro, devido ao aumento da diversidade e surgimento de novas comunidades comerciais com a necessidade de novos sistemas cada vez mais específico, gerando assim uma carência de segurança associados aos sistemas e políticas que devem ser utilizada. Na concepção de Pfleeger (1997), as normas para investimento em segurança da informação devem ter como base três segmentos: pessoas, tecnologia e processos. Uma combinação entre treinamento, procedimentos e tecnologias é defendido por Laudon e Laudon (2007), necessários, para proteger sistemas de informação contra acesso não autorizado, uso indevido, destruição ou adulteração de ativos. Visto que não adianta apenas investimentos em tecnologias se não for feito o mesmo investimento com pessoas que operam a tecnologia, principalmente pela complexidade dos ambientes de *data center*, retratado por Ono (2014).

Historicamente, o segmento que tem recebido maior atenção e maior investimento é segmento da tecnologia da informação e comunicação, mas Marciano (2006), ressalta que a tecnologia é capaz de apresentar parte da solução a esse problema, porém não é capaz de resolvê-lo em sua totalidade. Com base nesse sentimento alguns órgãos buscam padronizar e criar normas de segurança para os processos envolvendo a segurança da informação.

As normas de segurança da informação são publicadas geralmente sob responsabilidade de órgãos onde membros que participam são amplamente respeitados por sua experiência em segurança da informação. Essas normas podem ser adotadas por equipes técnicas, organizações privadas ou de terceiro setor e órgãos públicos é o que define (BAYUK, 2010).

Segundo (BAYUK, 2010) as normas de segurança nos processos organizacionais ou avaliações de segurança, incorporaram muitas organizações que auditam sistemas, produtos e serviços, podendo caracterizar, se a segurança da informação está em conformidade com as normas ou não. Boa parte das normas de segurança foram criadas ou estabelecidas por partes que têm grande interesse em segurança da informação, podendo ser visto como exemplo, a ISO/IEC 27002 (ISO/IEC 27002, 2013) e NIST(NIST, 2014).

A perda de informações em ambientes empresariais, pode ocasionar em desvantagem competitiva e na pior das situações, causar à falência da organização. Acredita-se que o uso de normas de segurança pode auxiliar a reduzir custos, perda de informações e dar suporte a

gestão da segurança nas organizações, através de implementação de metodologias provenientes destas normas (HOLIK et al.,2015). De certa forma, a adoção de normas de segurança depende de abordagens que facilitem o consenso industrial e não qualquer tentativa de justificativa acadêmica. (BAYUK, 2010). O uso destas normas de segurança depende da legitimidade de seu uso nas organizações, além de ser analisado de modo significado a eficiência e o desempenho econômico

Para Madan (2010) o interesse na utilização de normas de segurança é diminuir as falhas e suas consequências uma vez que várias técnicas e métodos surgiram nas ultimas duas décadas para realização de ataques. Apesar de um crescente uso em normas pela indústria para garantir os processos de TI. Acredita-se que com isso que o uso de normas de segurança possam apoiar processos de monitoramento dos controles técnicos contra ataques dentro das organizações.

Os conceitos encontrados na literatura, baseia-se na utilização de normas de segurança da informação acreditando ser primordial para agregar valor a sistemas, processos e serviços dentro das organizações. Uma vez que permite dar embasamento em avaliações periódicas, onde a alta direção e até mesmo engenheiros de sistemas, podem adotar as melhores decisões com base em métricas propostas por essas normas, apresentada normalmente por relatórios.

No contexto deste trabalho, foram escolhidas três conjuntos de normas de segurança da informação, que embasaram a estratégia Primasia a qual será aplicada neste estudo. A seguir são apresentadas uma simplificação das três normas: a ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27.005, onde serão explanados os conceitos principais, famílias e os controles de segurança. Em seguida será definido o modelo de maturidade COBIT com descrição dos níveis de maturidade.

2.3.3 ISO/IEC 27001 - Código de Prática para Controles de Segurança da Informação

A norma ABNT NBR ISO/IEC 27.001:2013, é um modelo internacional para a gestão da segurança da informação, sua versão atual foi publicada em 2013, é baseada na norma BS 7799 (British Standard), que foi considerada como a primeira de normas de segurança da informação. A mesma surgiu na década de 90 por uma iniciativa da instituição inglesa para padronizar os processos de segurança da informação e melhorar a qualidade dos dados.

A principal função da norma ABNT NBR ISO/IEC 27.001:2013, é apontar os requisitos básicos para a implantação de um Sistema de Gestão de Segurança da Informação (SGSI),

bem como todo o controle e gerenciamento (ABNT, 2013a). Segundo Alencar (2019) essa norma é considerada como a principal norma, que uma organização deve utilizar como base, para obter a certificação empresarial em gestão da segurança da informação. Além disso a norma ABNT NBR ISO/IEC 27.001:2013 é considerada como a única norma internacional que pode ser auditável e que define os requisitos para um SGSI.

A estrutura da norma foi definida por onze seções, são elas:

- 0 Introdução;
- 1 Escopo;
- 2 Referências normativas;
- 3 Termos e definições;
- 4 Contexto da organização;
- 5 Liderança;
- 6 Planejamento;
- 7 Apoio;
- 8 Operação;
- 9 Avaliação do desempenho;
- 10 Melhoria.

Alencar (2019) descreve que o sistema de gerenciamento para sistema de informação é proposto por um modelo baseado em estabelecer, monitorar, rever, manter e melhorar um sistema de gestão da segurança da informação. Sendo considerado como um código de práticas para segurança da informação. A sua declaração está estruturada em seções, onde cada seção tem uma série de controles que podem ser implementados, dependendo do tamanho e necessidade de cada organização. O Anexo A, da norma, detalha 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles que podem ser implementados (ABNT, 2013a).

As 14 seções apontadas no Anexo A da norma são (ABNT, 2013a):

a) Política de Segurança da Informação;

b) Organizando a Segurança da informação;

c) Segurança em Recursos Humanos;

d) Gestão de ativos;

e) Controle de Acesso;

f) Criptografia;

g) Segurança Física e do Ambiente;
h) Segurança nas Operações;
i) Segurança nas Comunicações;
j) Aquisição, Desenvolvimento e Manutenção de Sistemas;
k) Relacionamento na Cadeia de Suprimento;
l) Gestão de Incidentes de Segurança da Informação;
m) Aspectos da Segurança da Informação na Gestão da Continuidade do Negócio;
n) Conformidade.

Esta norma internacional foi preparada para promover um modelo para estabelecer, implantar, operar, monitorar, rever, manter e melhorar o sistema de gestão de segurança da informação, podendo ser usada visando avaliação da conformidade por partes interessadas internas e externas comentam Fernandes e De Abreu (2014) . Conforme descrito por norma ABNT (2013a) os requisitos definidos nesta norma são genéricos sendo pretendido que sejam aplicáveis a todas as organizações, independentemente de tipo, natureza e tamanho. A possibilidade de exclusão de algum de seus controles precisa ser criteriosa e justificada, e a confirmação de aceitação de que os riscos associados, inerentes à retirada, foram aceitos por membros responsáveis pelo gerenciamento precisando ser fornecida aceitação.

Segundo Alencar (2019), a organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gerenciamento de sistema de informação documentado dentro do contexto das atividades de negócio globais da organização e os riscos que ela enfrenta. Sobre esse assunto, Fontes (2012) elaborou uma base de dados com informações referentes a política de segurança da informação, analisando o que as empresas definem em sua PSI. O resultado da análise realizada em estudo por Fontes (2012), apresentou a realidade das organizações naquele período, o autor descreve como as organização enxergavam a segurança da informação e como a mesma estava sendo tratada internamente, o estudo aponta para uma incorreta ou incompleta aplicação da norma por parte das organizações.

Para Beckers et al. (2013) a ISO/IEC 27.001 é visível para as empresas que não está clara as normas que implantam, propondo uma análise das implantações para entender o motivo, tornando mais legível a norma e propõe a construção de uma hierarquia dos processos da ISO/IEC.

2.3.4 ISO/IEC 27002 - Código de Prática para Controles de Segurança da Informação

A norma estabelece procedimentos e diretrizes para iniciar, implementar, manter e melhorar a gestão de segurança numa organização. Provendo recomendações gerais para apoiar a segurança da informação e pode servir como guia prático para o desenvolvimento de procedimentos de segurança da informação e eficientes práticas para ajudar a dar confiança nas atividades das organizações (ISO/IEC 27002, 2013).

De forma abrangente é proposto, um modelo para criação e operação de um sistema de gestão de segurança da informação. O mesmo incorpora características atribuídas por especialistas de diversas áreas do mundo que chegaram a um consenso, gerando assim um modelo internacional. Além disso, a norma oferece uma ampla variedade de controles que não foram contemplados na ISO/IEC 27001. Esses controles abrangem desde conhecimentos técnicos e funcionais, incluindo novos conceitos antes não utilizados relacionados a padrões éticos e lógicos, além de políticas, procedimentos e processos.

Esta norma surge de embasamento da família de normas ISO/IEC 27000. A criação desta família tem como objetivo ajudar as organizações de todos os tipos e tamanhos para implementar e operar um sistema de gestão de segurança da informação. A norma consiste de 15 seções (ISO/IEC 27000, 2014). As referências das famílias dos controles de segurança da norma ISO/IEC 27002 estão listadas no quadro 2 a seguir. A publicação dessa norma foi inicialmente publicada no Brasil como ISO/IEC 17.799, em setembro de 2001, e atualizada e renomeada posteriormente para ISO/IEC 27.002, em 2005. No ano de 2013 foi atualizada para a versão atual, nomeada como: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação (ABNT, 2013b). Esta norma contempla cinco seções explicativas, são elas:

- 0 Introdução;
- 1 Escopo;
- 2 Referências normativas;
- 3 Termos e definições;
- 4 Estrutura desta Norma.

Quadro 2 – Referência das famílias dos controles da norma ISO/IEC 27002

Controles de Segurança
A.5 - Políticas de segurança da informação
A.6 - Organização da segurança da informação
A.7 - Segurança em recursos humanos
A.8 - Gestão de ativos
A.9 - Controle de acesso
A.10 – Criptografia
A.11 - Segurança física e do ambiente
A.12 - Segurança nas operações
A.13 - Segurança nas comunicações
A.14 - Aquisição, desenvolvimento e manutenção de sistemas
A.15 - Relacionamento na cadeia de suprimento
A.16 - Gestão de incidentes de segurança da informação
A.17 - Aspectos da segurança da informação na gestão da continuidade do negócio
A.18 - Conformidade

Fonte: ISO/IEC 27002 (2013)

A norma continua com mais quatorze seções, seguindo a mesma divisão do Anexo A da ISO/IEC 27.001 (ABNT, 2013a), 14 seções de controles de segurança da informação, 35 objetivos de controles e 114 controles que podem ser implementados, sendo um detalhamento da sua implementação (ABNT, 2013b). Tais normas (ISO/IEC 27.001 e 27.002) são tidas como os principais documentos de referência para elaboração de um SGSI, sendo a escolha de Silva Neto, Alencar e Queiroz (2015), bem como de Fontes (2012) ao pesquisar um padrão mínimo para elaboração e implantação de uma PSI.

A norma a ISO/IEC 27.002 Pode ser entendida como um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação. Sendo recomendável que a norma seja utilizada em conjunto com a ISO/IEC 27.001. Alencar (2019) descreve que a norma citada, também pode ser consultada de forma independente com fins de adoção das boas práticas. A identificação de quais controles devem ser implementados requer planejamento e atenção cuidadosa em nível de detalhes. Tendo, como um das contribuições principais desse modelo, a prevenção contra perdas

financeiras que a organização pode ter no caso de ocorrências de incidentes de segurança da informação.

Um sistema de gestão da segurança da informação bem-sucedido requer apoio de todos os funcionários da organização. Isto pode também exigir a participação de acionistas, fornecedores ou outras partes externas. Orientações de especialistas externos podem também ser necessárias (ALENCAR, 2011). Conforme ABNT (2013b) enfoca, os ativos são foco de ameaças, tanto acidentais como deliberadas, enquanto que os processos corporativos, sistemas, redes e pessoas têm vulnerabilidades existentes. Mudanças nos processos e sistemas do negócio ou outras mudanças externas (bem como novas leis e regulamentações), podem criar novos riscos de segurança da informação, conforme descreve a ABNT (2013b).

De certa forma, a segurança da informação também garante à direção e outras partes interessadas que os ativos da organização estejam razoavelmente seguros e protegidos contra danos.

Um ponto interessante da norma ISO/IEC 27.002 ABNT (2013b), atualmente em vigor, é a sua alteração de visão ao tratamento das pessoas (ALENCAR, 2008). Na atualização que foi realizada de 2005, Alencar (2019) esclarece que foi alterada a compreensão do aspecto humano ao modificar sua antiga seção 6.2.1 “Educação e treinamento em segurança da informação”, entre outras alterações que foram realizadas e divulgada na primeira edição (ISO/IEC 17799 de 2001), para a seção 8.2.2 “Conscientização, educação e treinamento em segurança da informação”, divulgada na atualização da norma em 2005 (ISO/IEC 27.002 de 2005), nomenclatura e concepção que permanece na versão 2013 (ABNT, 2013b), atual.

2.3.5. ISO/IEC 27005 – Gestão de Riscos em Segurança da Informação

A ISO/IEC 27.005 foi publicada no ano de 2008, o seu principal foco é a utilização de técnicas na Gestão de Riscos em Segurança da Informação (GRSI). Esta norma permite um suporte à organização para que faça a gestão de risco baseado em técnicas que associem combinações de probabilidade e consequência de determinados eventos indesejados causar perdas (ABNT, 2011). Em 2011, foi publicada uma revisão da norma que substitui a edição anterior, esta que ficaria conhecida como ABNT NBR ISO/IEC 27.005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos da Segurança da Informação. A norma desenvolvida tem como princípio ajudar na implementação dos processos de segurança da informação, através do fornecimento de diretrizes para o processo de GRSI

(GHAZOUANI et al., 2014). Kozen (2013) cita que existem varias metodologias e normas que direcionam para um bom desenvolvimento de uma gestão de risco, onde cada uma fornece um conjunto de diretrizes distintas para o gerenciamento dos riscos e nos vários modelos de referência para gestão dos riscos que visam nortear as implementações necessárias. Considerando como as primordiais, está a norma ISO/IEC 27.005:2011.

A ISO/IEC 27.005 é a norma que fornece diretrizes e descreve um processo genérico para a organização na gestão de seus riscos de segurança da informação (PONTES, 2009). Segundo a presente norma (ABNT, 2011), os controles em segurança da informação incluem qualquer processo, política, procedimento, diretriz, prática ou estrutura organizacional, que podem ser de natureza administrativa, técnica, gerencial ou legal, que modificam o risco da segurança da informação. Os processos descritos nesta norma formam uma base para construção de metodologias para gestão de riscos, que direciona o que a organização deve fazer, mas não detalha suficientemente como executar as atividades, dificultando na organização ou em algum setor a sua implementação (KONZEN, 2013).

Para Ghazouani (2014) A ABNT NBR ISO 27.005 torna-se aplicável a todos os tipos de organizações, indiferente do porte financeiro, que pretendem gerir os riscos, que possam comprometer qualquer uma das áreas ou princípios inerentes à segurança da informação da organização, sejam elas privadas ou públicas. O risco de segurança da informação pode ser entendido como a possibilidade da ameaça causar problema explorando vulnerabilidades ao bem empresarial.

2.3.6. COBIT

Segundo Ono (2014) O COBIT é um modelo baseado nos domínios de gestão de TI e em modelos de processos, onde os domínios são áreas ou disciplinas de TI compostas por um conjunto de processos que objetivam a finalidade de negócio e os processos são relacionados com o Planejamento, Implantação, Operação e Monitoração. Os processos são controlados pelos indicadores de performance e de objetivos.

De acordo com Prado et al. (2016), o modelo de maturidade padrão do COBIT foi derivado do Capability Maturity Model for Software (SW-CMM) e estabelece para cada processo de TIC níveis de maturidade para que a organização passe a ser medida, avaliada e comparada.

O COBIT está estruturado em 4 domínios, possuem 34 processos que possuem 1 objetivo de negócio para cada processo e 318 objetivos de controle e gestão no total como detalha ONO (2014).

A seguir são apresentados os domínios do COBIT 4.1

- *Planning & Organization (PO)* – Planejamento e Organização
  Este domínio compreende o modelo de estratégia e tática do uso da informação e tecnologia para atingir os objetivos ou metas da organização.
- *Acquisition & Implementation (AI)* – Aquisição e Implementação
  Tem o objetivo a identificar, desenvolvimento ou aquisição, a implementação e integração das soluções de TI.
- *Delivery & Support (DS)* – Entrega e Apoio
  Entrega dos serviços de TI, incluindo o gerenciamento da segurança, continuidade, dados, gestão de facilidades de TI e serviços de suporte a usuários, o que corresponde à operação de TI.
- *Monitoring & Evaluation (ME)* – Monitoração e Avaliação
  Domínio que realiza o gerenciamento de performance, monitoração dos controles internos e compliance e governança.

Os níveis de maturidade do COBIT 4.1, destinam-se a descrever possíveis estados dos processos de TI (STAMBUL; RAZALI, 2011), produzindo um perfil de maturidade de uma determinada organização ISACA (2012a). A definição de cada nível, de acordo com ITGI (2007) e ISACA (2012a), pode ser vista no quadro 3.

Para tratar a maturidade, o COBIT define um conjunto de indicadores que são obtidos pelo consenso de especialistas, porém os mesmo são mais focados nos controles de atividades do que em sua execução. Esses controles auxiliam para otimizar o investimento em TIC, garantir a prestação de serviços fornecendo uma medida para julgar e permitir a comparação (RIGON et al., 2014). Sendo definido o papel da organização em analisar e apontar o grau de maturidade que a empresa se encontra e o grau de maturidade que deseja alcançar, de acordo com a estratégia de TIC organizacional.

Quadro 3 – Níveis de Maturidade Conforme o COBIT

Nível	Nome	Descrição
0	Inexistente	Falta completa de qualquer processo identificável. Não existindo a consciência da necessidade de controles. A organização nem sequer reconhece que existe um problema a ser tratado.
1	Inicial	Há evidências de que a organização tenha reconhecido a existência de problemas que deveriam ser tratados. Existem processos, porém ad hoc. Normalmente são aplicados isoladamente ou tratados a cada caso. De forma geral, o gerenciamento ainda é desorganizado.
2	Repetível	Os processos seguem procedimentos similares e são seguidos por diferentes pessoas que executam a mesma tarefa, normalmente ações que estavam no Nível 1 e deram certo ou foram bem aceitas. Não existe treinamento formal ou comunicação dos procedimentos padrões, sendo a responsabilidade ainda individual. Existe um alto grau de confiança no conhecimento dos indivíduos, sendo provável a ocorrência de erros.
3	Definido	Neste nível os procedimentos já estão padronizados e documentados, bem como comunicados e treinados. Em qualquer etapa é possível acontecer erros ou desvios, mas, a partir deste estágio, os erros não são vistos com frequência. Seguir esses processos é obrigatório. No entanto, é improvável que os desvio sejam detectados. Os procedimentos não são sofisticados, mas existe formalização das práticas existentes;
4	Gerenciado	Após a melhoria da execução (nível 3), é possível monitorar e medir a conformidade com os procedimentos, bem como agir nos processos que aparentemente não funcionam corretamente. Os processos estão sobre aperfeiçoamento constante e fornecem boas práticas. Ferramenta de automação é usada de forma limitada e fragmentada.
5	Otimizado	Os processos estão refinados ao nível das melhores práticas, baseados em resultados de aperfeiçoamento contínuo e modelagem de maturidade com outras organizações. A TIC é usada de forma integrada para automatizar fluxos de trabalho, fornecendo ferramentas para aperfeiçoar a qualidade e eficiência, e fazendo com que a empresa, quando necessário, se adapte rapidamente.

Fonte : ITGI (2007) e ISACA (2012a)

Almeida Neto (2015) explicam:

> "Existem casos onde os marcadores de auto avaliação, os quais refletem onde a organização se encontra segundo sua maturidade e onde ela tem intenção de chegar, ficam separados por um "gap" que reflete o esforço necessário para atingir esta meta estratégica. Visando apoiar que esta meta possa ser alcançada, este "gap" acaba sendo descrito de maneira mais detalhada para posteriormente servir de insumo para uma análise mais apurada. Esta análise resulta no planejamento de projetos que possibilitem que a organização atinja suas metas estratégicas para segurança e controle da TIC" (ALMEIDA NETO, 2015, p. 57).

Prado et al. (2016) ainda comentam que o COBIT, para medir um processo, utiliza dois tipos de indicadores:

- *Outcome measures* - Medições de resultados

  O que indica se um processo de TI atingiu os objetivos de negócios, Essa medição também é conhecida como *lag indicators;*
- *Performance indicators* - Indicadores de desempenho

> Esse indicadores indicam o quanto os processos de TIC estão sendo bem executados no atendimento aos objetivos do negócio. Esses indicadores são conhecido como *lead indicators*.

Segundo Alencar (2019), no COBIT 5, é baseado na ISO/IEC 15.504, não existindo mais um modelo de maturidade específico. O mesmo trabalha com uma abordagem da avaliação da capacidade de processo ISACA (2012a). Este modelo fornece meios para medir o desempenho dos processos de governança e gestão especificados no modelo de referência do COBIT 5 (ALMEIDA NETO, 2015).

Os atributos de maturidade do COBIT 4.1 e os atributos de capacidade de processo do COBIT 5 não são idênticos. Eles sobrepõem-se e mapeiam até certa medida (ISACA, 2012a). As organizações que utilizam a abordagem dos atributos do modelo de maturidade do COBIT 4.1 podem reutilizar os atuais dados da sua avaliação e reclassificá-los segundo as avaliações de atributos do COBIT 5 (ISACA, 2012a).

2.4 Visão Geral Sobre *Data center*

Segundo Moraes (2018) O *data center* pode ser definido como um departamento dentro da organizações que além de abrigar, mantém sistemas, servidores, *mainframe* e bancos de dados.

Anteriormente os sistemas eram estruturados de forma centralizada. Lima (2017) define que o objetivo de um *data center* é fornecer conexões centralizadas, utilizando poderosos recursos de computação para implantação de variados serviços.

Cada vez mais as organizações estão implantando suas aplicações em *data centers* por causa da confiabilidade, disponibilidade e baixo custo. (LI, 2014) (NIEKERK; JACOBS, 2015). *Data centers* dentro das organizações podem fornecer uma variedade de serviços, tanto para acesso local ou remoto. Muitos servidores podem armazenar ou processar informações confidenciais.

Normalmente em *data centers* é mais fácil encontrar servidores de serviços web, de banco de dados e de arquivos, porém outros servidores como de e-mail, virtualização podem ser encontrados nas organizações (SCARFONE; JANSEN; TRACY, 2008).

Data centers possuem algumas características essenciais (LI, 2014) que serão descritas a seguir:

- Acesso sob demanda – Os usuários especificam os requisitos (número de CPU´s necessárias e o armazenamento) que são automaticamente fornecidos pelo *data center*;
- Serviço medido - Os requisitos de serviço indicados devem ser mensuráveis para que os consumidores possam ser cobrados pelo uso de recursos.
- Acesso à rede - Um portal ou plataforma deve ser fornecido aos usuários para que eles possam enviar e gerenciar seus trabalhos.
- Agrupamento de Recursos - Os recursos no *data center* podem ser compartilhados por consumidores com acordos de nível de serviço (ACL´s) diferentes.
- Virtualização - A topologia do *data center* não deve importar ao usuário. As aplicações são facilmente migradas entre plataformas de hardware à medida que as demandas e as alterações de uso ocorrem. Isso acontece automaticamente.
- Confiabilidade - Existem múltiplas cópias redundantes de conteúdo armazenado.
- Manutenção - Esta é tratada por uma equipe de TI profissional e dedicada.

Desta forma, fica evidente que devido ao grande número de características os seguintes elementos lógicos precisam de proteção: uso adequado de protocolos de comunicação, quais serviços/aplicações serão utilizados. Além disso, elementos físicos também precisam de proteção: rede, acesso físico e os componentes físicos (NIEKERK; JACOBS, 2015).

2.5 Segurança em *Data center*

Os conceitos fundamentais sobre segurança de *data center*, são divididos entre segurança física e segurança lógica segundo Lima (2017). Todas as informações valiosas de quase todas as organizações em sua grande maioria estão armazenadas em *data centers*, seja ele presencial ou em tecnologia de armazenamento em nuvens. Desta forma é imprescindível que os dados e servidores sejam protegidos de pessoas com intenção maliciosa. Impedir acesso não autorizado é extremamente importante (JAYASWAL, 2006), (GREENBERG et al., 2009), (SHIEH et al., 2011).

A segurança lógica de *data center* precisa ter o objetivo de dificultar qualquer intruso de conseguir acesso não autorizado. Porém esta segurança não está relacionada apenas aos servidores, mas também a outros *hosts* de acesso, como por exemplo terminais que têm acesso remoto ao servidor. Além disso, outras medidas são recomendadas:

- Desabilitação de serviços desnecessários que utilizem portas de comunicação (menos de 1024);
- Construir mais de uma camada de autenticação, e permitir que apenas alguns usuários tenham acessos a essas camadas;
- Os usuários devem se autenticar num servidor de *login* central, e assim esta máquina estará com acesso direto aos consoles da rede.

Alguns pontos são essenciais na segurança lógica do *data center*, já que um *data center* é composto por uma variedade de dispositivos, sendo divido por três modalidades de interação com seus clientes segundo Lima (2017). A primeira modalidade definida por Lima (2017) é denominada de Provedor de "*Co-location*" ("*Co-location Services Provider* ou CSP), onde todos os recursos de tempo de execução e tempo de serviços, ambos de propriedade de um cliente são alocados nas instalações local do *data center*. Nessa modalidade o *data center* torna-se um fornecedor de recursos na forma de espaço físico em um conjunto de racks e energia elétrica para um conjunto de servidores, que recebem a denominação de serviços basais e tudo pertence ao cliente. A segunda modalidade e denominada de provedor de serviços gerenciados ("*Managed Services Provider* ou MSP") , nessa modalidade todo os serviços basais são oferecidos pelo provedor, sendo os recursos de serviços a única propriedade do cliente. A terceira modalidade é denominada por provedor de serviços de aplicações ("Application Services Provider" ou ASP), onde todos os recursos pertencem ao *data center* sendo o cliente apenas um consumidor de recurso de serviço. Para todas as modalidades a segurança da informação é recurso primordial, porém nesse trabalho iremos abordar

Servidores dentro das organizações podem fornecer uma variedade de serviços, tanto para acesso local ou remoto. Muitos servidores podem armazenar ou processar informações confidenciais (SCARFONE; JANSEN; TRACY, 2008). Normalmente podemos encontrar servidores de serviços de internet, banco de dados e servidores de arquivos. Servidores são frequentemente alvos de ataque por causa da importância dos seus dados. Alguns exemplos de ameaças a servidores podem ser identificadas:

- Entidades mal-intencionadas podem explorar *bugs* de software no servidor ou seu sistema operacional;
- Ataques de Negação de Serviço (*DoS* ou *DDoS*), impedindo os usuários de acessarem seus serviços;
- Acesso de pessoas não autorizadas a informações sensíveis;

- Algum indivíduo pode obter acesso não autorizado a outros recursos da rede através de uma vulnerabilidade do servidor;

Quando se trata de segurança em servidores existem alguns princípios que ajudam a resolver problemas de segurança:

- Simplicidade – Os sistemas de informação devem ser o mais simples possível. Complexidade sem necessidade pode ser um agravante na segurança;
- Falha na segurança – Caso ocorra uma falha, ela tem que ocorrer de forma mínima, sem que haja perda nos controles e configurações de segurança;
- Utilização de mediadores – Uso de permissões a sistemas de arquivos, *proxies*, *firewalls* e *gateways*;
- *Open Design* – A segurança em servidores não pode ser dependente de configurações sigilosas.
- Separação dos privilégios das funções – Na medida do possível, devem-se separar as funções.
- Menor privilégio – Determinar direitos mínimos para execução de tarefas/processos pelos usuários ou sistemas;
- Aceitabilidade psicológica – Os usuários devem entender a necessidade de segurança por meio de treinamento e educação;
- Defesa de profundidade – As organizações devem entender que um único mecanismo de segurança em geral é insuficiente;
- Fator de trabalho – As organizações devem entender qual o esforço para um invasor quebrar a segurança, a realização de análise de risco do ambiente pode ser uma saída;
- Registros – Registro e *logs* devem ser mantidos, para que em caso de comprometimento segurança a organização tenha evidências do ataque, falha ou omissão disponíveis.

Várias organizações dependem de regulamentações e regras que são estabelecidas por órgãos especializados, como por exemplo: *IEEE e AMA.* Desta forma, isso também é válido para a segurança da informação (KRÁTKÝ et al., 2016) (FULLER et al., 2013).

2.6 Estratégia Primasia – Controles e Níveis de Maturidade

A aplicação prática deste trabalho, está embasada na utilização da estratégia Primasia - Priorização e Maturidade em Segurança da Informação Adaptável, que será descrita neste capítulo. Alencar (2019) define a estratégia com um conjunto de regras descritas que deve funcionar de forma cíclica indiferente do arcabouço que a fundamente, sendo modular e adaptável ao ambiente.

A mesma consiste, inicialmente, na classificação de 114 controles da ISO/IEC 27.001 e 27002, que serão transformados em estágios. A estratégia utiliza níveis de maturidade baseados no COBIT inserindo um nível. Numa uma segunda fase, os controles são classificados em estágios e a divisão realizada por percentual conforme apresentado por Alencar (2019). Para Alencar (2019) o que diferencia a estratégia do demais modelos, está na utilização de estágios e níveis de maturidades. Nos estágios estão classificados os controles por quartis, de acordo com a importância dada a eles pelas Organizações. E a organização só será avaliada no segundo quartil ao atender o nível mínimo dos controles do estágio anterior. Ainda segundo Alencar (2019),Nesta nova configuração, os controles mais importantes serão inseridos de forma prioritária.

Baseado nas informações coletadas nos estágios é calculado a média das notas de cada controle e ordenando-os. O primeiro quartil representa os 25% dos controles considerados mais importantes, enquanto o último quartil, representa os 25% dos controles com menor nível de importância. Cada quartil é categorizado como “Estágio”. Em uma situação ideal, os controles estarão distribuídos, conforme mostrado no quadro 4.

Quadro 4 – Estratificação dos Controles de Acordo com sua Importância

Média do Controle	Primeiro Quartil (maiores médias)	Segundo Quartil	Terceiro Quartil	Quarto Quartil (menores médias)
Estágio	Básico	Essencial	Intermediário	Avançado
Controles	32	27	28	27

Fonte : Adaptada de Alencar (2019, p. 151)

Ressalta-se, que os controles apontados no primeiro estágio, Básico, são considerados os elementos para a concepção de um SGSI ou PSI simplificados (ALENCAR, 2019).

Alencar (2019) também ressalta que a divisão dos quartis pode não ser tão exata. Pois, após a classificação dos controles, uma análise dos controles pré-requisitos é realizada, e caso o controle pré-requisito não esteja no mesmo estágio ou em um estágio anterior do

que o controle que o tem como pré-requisito, o controle pré-requisito é inserido no referido estágio.

Um quartil também pode ter as quantidades de controles aumentadas caso exista empate nas notas dos últimos controles, sendo todos incorporados ao quartil. Por exemplo, se os controles das posições 27, 28, 29 e 30 tiverem a mesma média, todos serão incorporados ao primeiro quartil, tendo neste caso o primeiro quartil 32 controles conforme descrito no quadro 4.

Para evitar que tenha-se, um excesso de controles em um mesmo nível, no primeiro quartil é limitada em três a quantidade de controles empatados nas últimas posições a ser incorporado. Caso tenha mais do que três controles empatados, deve-se utilizar o máximo possível de casas decimais para o desempate. Segundo Alencar (2019), caso ainda persista, deverá ser seguida a ordem numérica dos controles da ISO/IEC, inserindo, desta forma, os controles com a numeração mais baixa primeiro. Com essa regra implantada, caso aconteça a hipótese dos controles das posições 27 até 45 estarem exatamente com a mesma média de nota, será ordenado pela numeração do controle e selecionado os 3 empatados. Como o primeiro quartil tem 29 controles como referência (Quadro 3), seria inserido mais 3, totalizando assim a quantidade máxima de 32 controles.

Cada estágio é composto pelos seis níveis de maturidade do COBIT (Quadro 2), descrito a seguir na Figura 2. Sendo verificado o nível de cada controle aplicável a organização no estágio em questão conhecimento compartilhado por Alencar (2019).

Existem duas formas para aferir a maturidade para à estratégia Primasia. A primeira, é feita, após o levantamento e ordenação dos controles mais importantes, análise e, se necessário, inclusão dos controles pré-requisitos, entendimento dos quatro estágios e de seus cinco níveis, devendo ser visto o nível mínimo para se alcançar e estar apto a passar de estágio. Fato que é alcançado quando todos os controles aplicáveis do estágio atual atingirem, ao menos, o nível 3 (processo estabelecido), como linha de base para que os controles atinjam e, com isso, a organização mude de estágio. Na segunda forma é realizar uma análise de risco de segurança da informação na organização, como sugere a ISO/IEC 27005, e categorizado o nível mínimo de cada controle de acordo com a probabilidade e impacto do risco inerente ao referido controle.

Figura 2 – Estágios e Níveis de Maturidade

Fonte : Adaptada de Alencar, 2019, p.152

Para Alencar (2019), a probabilidade e o impacto serão categorizados como baixo, médio ou alto. Recebendo, respectivamente, o peso 1, 2 ou 3. Uma matriz é formada e o valor mínimo de maturidade a ser alcançado é definido através da soma da nota da probabilidade e do impacto, conforme Figura 3. Uma exceção é quando se atinge uma probabilidade e impacto altos, recebendo a nota 6 (3+3). Ciente que o modelo proposto aborda até o nível de Maturidade 5 (otimizado), os controles categorizados com nota 6 deverão atingir o Nível 5 (otimizado) e, por sua criticidade, serão tratados, dentro de seu estágio, de forma prioritária pela organização. Nesta proposta , o estágio inicial é o Essencial 1 e o último é o Completo 5.

Figura 3 – Nível de Maturidade Mínima de Acordo com o Impacto e Probabilidade

Probabilidade	Baixo (1)	Médio (2)	Alto (3)
Alta (3)	4 - Gerenciado	5 - Otimizado	6 - Otimizado
Média (2)	3 – Definido	4 - Gerenciado	5 - Otimizado
Baixa (1)	2 - Repetível	3 – Definido	4 - Gerenciado

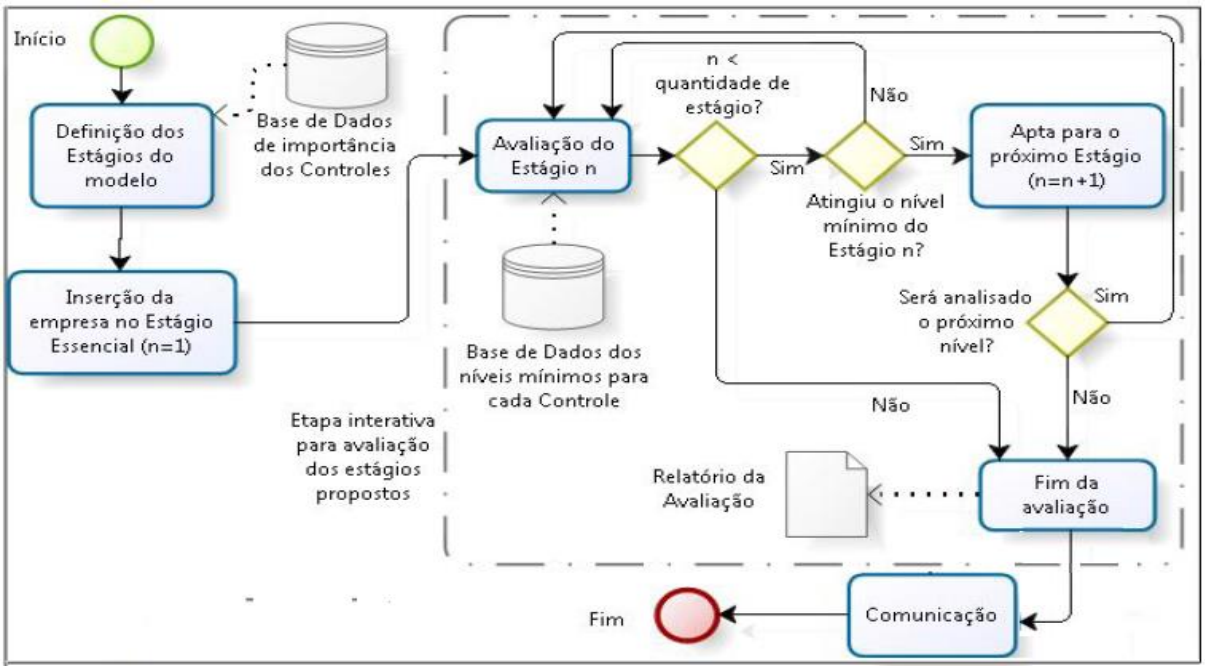
Impacto

Fonte : Alencar (2019, p.153)

Desta forma, os controles nos quais ausências geram riscos com maior probabilidade e maior impacto deverão ser tratados de forma diferenciada, com um nível de maturidade superior (ALENCAR, 2019). Os controles não aplicáveis deverão ser devidamente justificados no relatório a ser apresentado no final da avaliação e terão como nível mínimo o 0 (inexistente) não sendo contabilizados para Primasia. A fase de aplicação da estratégia consiste em analisar e aplicar cada controle ordenado nos estágios até o estágio pretendido, conforme representa Alencar (2019) aqui referenciado no trabalho por Figura 4.

A estratégia Primasia pode ser aplicada de duas formas, denominadas de “Modelo de Maturidade Comparável” e de “Aplicação Independente”. É necessário dividir essas formas de aplicação diante das duas possibilidades de se escolher o nível mínimo de cada controle o qual, direciona o esforço necessário para se alcançar o próximo estágio. As duas formas de aplicações são detalhadas a seguir.

Figura 4 – Fase de Aplicação da Estratégia Primasia



Fonte: Alencar (2019, p.154)

2.6.1 Modelo de Maturidade Comparável

Para ser possível a medição da maturidade e comparação entre as organizações mensuradas torna-se necessário um modelo padrão, de forma a se comparar questões iguais Alencar (2019). Os modelos de maturidade em segurança da informação, como já mencionados durante o trabalho, utilizam, por exemplo, os controles da ISO/IEC 27.001 ou 27.002 normalmente, com a média dos valores medidos. Tendo todos os controles o mesmo peso.

Como um diferencial da estratégia Primasia, o modelo de maturidade proposto trabalha com estágios e níveis de maturidades. Nos estágios estão classificados os controles por quartis, de acordo com a importância dada a eles pelas organizações. A organização só será avaliada no segundo quartil ao atender o nível mínimo dos controles do estágio anterior. Neste modelo de configuração da estratégia Primasia, os controles mais importantes serão

inseridos de forma prioritária. O modelo de maturidade proposto tem seus estágios e níveis apresentados na Figura 2.

Alencar (2019) compartilha de conhecimento que com a estratégia Primasia no modelo proposto, para se passar de um estágio (Básico, Essencial, Intermediário ou Avançado) para o seguinte só é possível após atingir o nível de maturidade mínimo de 3 (nível definido) para todos os controles, sendo este o parâmetro da base de dados dos níveis mínimo para cada controle, ou seja, se a empresa é categorizada como "Avançada Nível 2", significa que a média dos controles do grupo Avançado obteve o nível de maturidade 2 (Repetível) e que todos os controles aplicáveis do estágio Essencial e do Intermediário foram mensurados, no mínimo, como nível 3 (Definido). Sendo um diferencial do comparado a outro modelo de maturidade.

2.6.2 Modelo de Aplicação Independente

De acordo com Alencar (2019), a aplicação independente da estratégia visa o atendimento das organizações que estão em busca da implantação da segurança da informação e necessitam de uma estratégia que se adeque à sua organização, não necessitando, neste momento, utilizar o padrão de melhores práticas apontados no modelo de maturidade comparável (Seção 2.6.1). Esta ação consiste em aplicar a estratégia já mencionada (Figuras 2, 3 e 4). Porém a base de dados de importância dos controles (Figura 4), deve ser realizada de uma analise de aplicação do mesmo *survey* (questões de importância de cada controle) dentro da própria organização com definições feitas por *stakeholders.* Com essa implementação a base de dados dos níveis mínimos para cada controle (Figura 4), será montada conforme avaliação de risco referente a cada controle matriz definidos por Alencar (2019) apresentada na Figura 3.

Na forma de Aplicação Independente ainda Segundo Alencar (2019), temos a aplicação da mesma estratégia, porém adaptada ao ambiente e necessidades da organização. Fato este que segue a linha de pensamento da governança ágil, em especial seus meta-valores que apontam (LUNA et al., 2016):

- Comportamento e prática do que processos e procedimentos;
- Alcançar a sustentabilidade e a competitividade do que ser auditada para estar em conformidade;

- Transparência e envolvimento das pessoas com a empresa do que monitoramento e

controle;

- Sentir, adaptar e responder do que seguir um plano.

Neste modelo de estratégia as empresas estão moldando o processo ao seu negócio e não o contrário, para ser comparada com outras, buscando atingir seus objetivos, priorizar suas ações em segurança da informação Alencar (2019). A aplicação de estratégia Primasia de forma independente, pode promover definições básicas para o tratamento dos controles, tendo parâmetros para definição dos investimento e funcionando com um alinhamento da segurança da informação ao negócio, podendo ser visto como governança da segurança da informação, que apoia a governança de TIC que, por fim, incorpora à governança corporativa conforme detalhado por Alencar (2019).

Vale apena salientar, que Alencar (2019) ressalta, que o modo de aplicação não é totalmente comparável entre organizações para classificá-las. Uma vez que os controles selecionados em cada estágio, a quantidade de controles em cada estágio, como também o nível mínimo por controle podem ser diferentes. Porém, a nota e análise de cada controle de cada organização pode ser inserida em um modelo padrão o qual o autor se retrata como modelo de maturidade comparável, descrito neste trabalho na Seção 2.6.1. Fazendo com que exista a possibilidade de comparação entre os modelos de forma desejada sem muitos esforços.

2.6.3 Ganhos com Aplicações da Estratégia Primasia

Pensando na estratégia como uma ferramenta corporativa, Alencar (2019) cita que novas características podem ser adicionadas auxiliando, ainda mais, as empresas e profissionais na aplicação da segurança da informação. Algumas opções foram apontadas por Alencar et al. (2018b) e são detalhadas a seguir.

2.6.3.1 Banco de Melhores Práticas em Segurança da Informação

Em um pensamento mais amplo Alencar (2019), afirma que o modelo proposto de levantamento de dados pode servir como insumos para outras finalidades. Entre elas como uma base de melhores práticas para a segurança da informação, como diagramado na Figura 4. Com uma base de dados com amostras significativas, é possível verificar a indicação de

controles da ISO/IEC 27.001 e 27.002 selecionados como mais importante para o tipo de organizações específica.

Alencar (2019) corrobora com utilização da Primasia para trazer a inserção de requisitos legais, contratuais ou regulamentares para compor e ser aferido e analisado dentro da área de segurança da informação (Figura 4). Tal solução pode ser útil para apontar os controles mais utilizados (melhores práticas) por nicho, região ou características para que organizações sigam como referência. Seja por não ter um profissional para apoiar e melhor definir as áreas e controles a serem tratados dentro da organização ou, caso exista, para comparar o modelo da empresa com o que está sendo utilizado no mercado.

2.6.3.2 Sistema de Recomendações

Após as organizações responderem o questionário inicial com os dados do negócio (Apêndice A), o sistema poderá verificar o banco de respostas para empresas semelhantes e recomendar a aplicação de um conjunto de controle específicos para formação do Banco de Dados Personalizado (Figura 4) para a organização em questão.

Alencar (2019) Acredita que com passar da utilização da Primasia, as recomendações servirão como guia para aqueles que não tem uma análise mais aprofundada na área de segurança da informação e, consequentemente, não conseguem definir corretamente os controles a implantar, bem como, no caso de organizações, que já têm um nível de conhecimento, confrontar com o que é mais utilizado de forma a avaliar os controles já selecionados ou levantar o debate para inserção ou exclusão de algum controle.

O Alencar (2019) descreve ainda que o sistema de recomendações também pode ser ativado por indicação de especialistas na área de segurança da informação que poderão atuar na implantação da estratégia ou em uma ferramenta que a execute. O mesmo cita o como exemplo, ao se ter algum normativo ou lei específicos para um grupo que a organização em questão se enquadra, poderá ser indicado algum controle para o tratamento ou atendimento da norma ou lei. Além dessa possibilidade Alencar (2019) descreve uma outra situação onde exista a possibilidade de algum ataque que esteja se espalhando. Dá mesma forma o sistema, guiado por especialista, poderá recomendar algum controle na tentativa de mitigar as possíveis ações ou reduzir vulnerabilidades.

2.7 Trabalhos Correlatos

Este seção apresenta a revisão de três trabalhos relacionados com está dissertação. No processo de extração dos trabalhos, foi utilizada a o mecanismo de busca manual para identificar os trabalhos que mais se aproximavam com escopo e objetivos específicos desta pesquisa. E após leitura destes documentos foram selecionados documentos que foram referenciados neste trabalho.

Na primeira parte foram realizadas pesquisas na internet utilizando navegador como ferramenta, baseado em sites com mecanismo de busca, dentre os mecanismos de busca, o que trouxe o maior número de resultados foi selecionado como mecanismo de busca. Nesse sentido o Google foi escolhido como o mecanismo de busca, sendo apenas considerados trabalhos entre os anos de 2005 e 2019. Para realização da busca, foram utilizadas as palavras chaves: “Modelos de Maturidade”, “Segurança da informação” e “*Data centers”,* aplicados a teses, dissertações e artigos, A seleção dos documentos seguiu os seguintes passos:

1. Após o uso da *string* de busca, esta pesquisa inicialmente encontrou setecentos e três resultados Com os resultados, inicialmente foram muito alto, foi aplicado novos filtros com documentos publicados a partir de 2005, reduzindo para cinquenta e sete resultado;

2. Foram lidos os títulos dos cinquenta e sete trabalho. Após a leitura restaram vinte trabalhos de títulos correlatos onde foram analisados os resumos e conclusões;

3. Após a leitura dos resumos e conclusões restaram seis trabalhos onde foram analisados os escopos de pesquisa de cada um;

4. Após a leitura na íntegra dos seis trabalhos, apenas três trabalhos foram selecionados por possuir associação direta com o tema em pesquisa.

5. Os três trabalhos foram lidos levaram a o estudo a realizar nova busca baseado em referencias dos trabalhos citados. Os mesmo não foram identificados por busca anterior por serem trabalhos publicados fora do Brasil. Foi levado em consideração as referencia que possuíam relacionamento direto como tema de estudo e foi obtido com isso mais quatro trabalhos correlacionados com as pesquisas.

Baseados no trabalhos pesquisados foram selecionados três estudos que foram identificados por correlação direta como o tema deste trabalho. Os mesmo serão apresentado a seguir como trabalhos correlatos para o aprimoramento desta dissertação.

O Primero estudo é o de Lima (2017), o qual expõe a desenvolvimento de uma metodologia para avaliar maturidade associado a segurança da informação em *data center*s. O mesmo investiga parâmetros de segurança para determinar a conformidade dos *data center*s baseados em normas internacionais de segurança.

O trabalho propões três procedimentos de avaliação para capturar o nível de maturidade sendo dois procedimentos criado pelo autor com uma nova perspectiva para uma melhor analise. Definindo assim duas novas perspectivas de segurança em ambientes de *data center*s. Destacando a primeira perspectiva, Lima (2017) explora uma análise ponderada dos controles de segurança, presentes em um número maior de normas de segurança. Para a segunda perspectiva foi apresentado uma análise contextual sensível ao nível de importância que a organização atribui a cada controle de segurança. Baseado na metodologia proposta Lima (2017) é estimado que engenheiros de segurança podem identificar problemas de segurança e caracterizar a organização para o nível de maturidade da segurança e sugerir novas políticas para melhorar as configurações de segurança dos *data center*s.

O ponto forte do trabalho de Lima (2017) é que ele desenvolveu uma metodologia que também utiliza baseados em norma ISO/IEC 27002 e normas NIST SP 800-53 sendo pioneiro em estudo publicações acadêmica referente ao estudo no Brasil, levando-se em consideração a metodologia de busca aplicado neste trabalho. O ponto de melhoria que poderia ter sido levado em consideração seria ter acrescentado as normas ISO/IEC 27001 e ISO/IEC 27005.

A principal diferença entre o estudo realizado por Lima (2017) e por este trabalho, está no foco de aplicação deste trabalho. Lima (2017) utilizou quatro dimensões de estudo para seu trabalho focar na segurança dos servidores em *data center*. Lima (2017) separou o seu trabalho em quatro dimensões de estudo. Sendo que foram identificada para correlação neste trabalho apenas as dimensões: *Server Business Compliance e Server Security Preserving*, desconsiderando as dimensões: *Server Operating System Security* e *Server Application Security*, ambas aplicadas apenas a servidores. Esse estudo foca no ambiente de *data center* como um todo e não apenas em servidores.

O segundo estudo do autor Ono (2014) apresenta estudo sobre indicadores de desempenho em *data center*. O trabalho referencia os benefícios que oferece a seus clientes

a aplicação de indicadores de desempenho e de performance para medir, avaliar e otimizar os resultados da administração das instalações de TI aplicados aos *data center*s, destacando as ferramentas importantes para tomadas de decisões gerenciais baseadas em fatos e números, afim de evitar desta forma as análises subjetivas e que não demonstrem os benefícios e resultados de uma boa administração.

No decorrer do estudo Ono (2014) apresenta os principais indicadores voltados para administração do ambiente de *data center* considerando o modelo COBIT 4.1. Neste sentido foi descrito os controles internos COBIT que foram aplicados aos *data center*, aprimorando o gerenciamento de riscos e a prevenção que foi explicitado. A utilização do modelo COBIT 4.1 está diretamente relacionada ao foco de estudo deste trabalho, uma vez que a estratégia Primasia utiliza deste insumos. O resultado obtido por Ono (2014), apresenta apenas os indicadores, enfatizando as KPIs que melhor adequam ao ambiente de *data center*. Não foi aplicado a um caso real não podendo assim medir a implantação dos indicadores. O trabalho apenas relaciona os processos do COBIT. No entanto, um ponto importante avaliado é extração de evidências de tais controles. Outro ponto a ser considerado, é que Ono (2014) defende a padronização de controles de forma necessária, destacando o conveniente dos indicadores de maneira a convergirem para os resultados no atendimento da determinação da eficiência e dos objetivos definidos.

O terceiro trabalho relacionado abordou um estudo que gerou um modelo de maturidade desenvolvido por Muthukrishnan e Palaniappan (2016), chamado *Security Metrics Maturity Model for Operational Security* onde foram criadas identificações de elementos de qualidade de segurança para determinar métricas para um ambiente de segurança operacional. A avaliação dessas métricas foram definidas e realizada a partir das análises quantitativa e qualitativa com base em dois níveis de avaliação denominadas *Quantitative Matured Metrics* (QtMM) e *Qualitatives Matured Metrics*

A escolha da aplicação da estratégia Primasia está associada a uma evolução de modelos de maturidade existente com diferença proposta por Alencar (2019) de Propor não apenas um modelo para mensuração, mas, também, um guia para implantação da segurança da informação através da priorização dos controles. Sendo levado em consideração a possibilidade de aplicar controles de acordo com a importância apontada pelas organizações, através de uma visão modular que permite utilizar os diversos arcabouços existentes, adequando a necessidade de cada organização ou setor da mesma, facilitando a implantação.

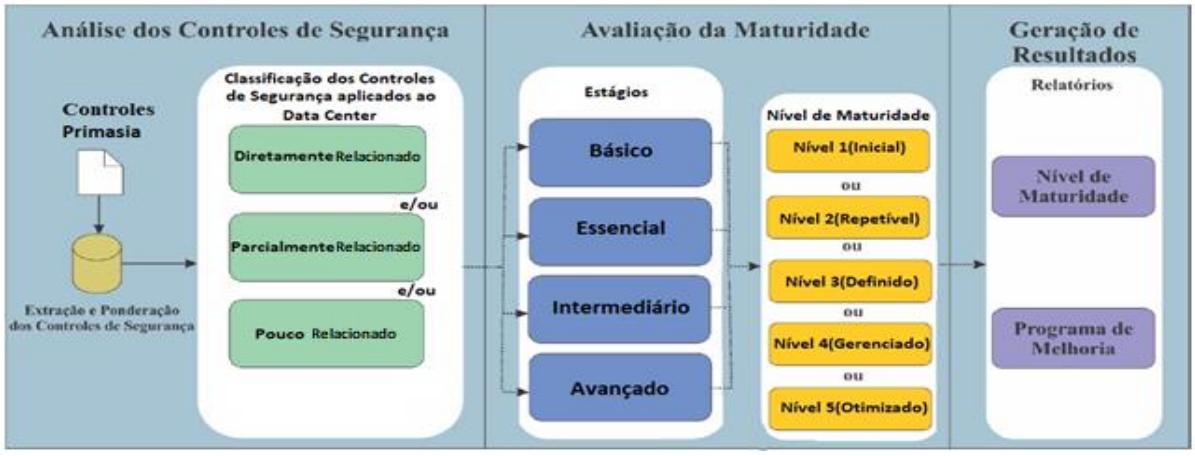
3 ADEQUAÇÃO DA ESTRATÉGIA PRIMASIA PARA AMBIENTE DE *DATA CENTER* DE FORMA INDEPENDENTE.

Este capítulo apresenta a implementação prática da estratégia Primasia, que visa avaliar o nível de maturidade de segurança da informação e priorizar as ações de segurança da informação. Neste estudo a estratégia será aplicada em organizações que utilizam *data centers* visando aferir o estado de segurança das informações. Inicialmente, tem-se uma visão geral das atividades e componentes para facilitar a compreensão da estratégia como um todo. Em seguida, são apresentados os detalhes de cada atividade e como realizar a avaliação usando esta estratégia. Por fim, são discutidos o uso e a importância desta estratégia.

3.1. Visão Geral

O objetivo principal do estudo proposto neste trabalho é avaliar o nível de segurança da informação aplicados ao ambiente de *data center* das organizações, independente do sistema operacional ou de políticas de segurança existente na utilizado no *data center*, aplicando de forma prática a estratégia Primasia. A implementação da estratégia permite a avaliação e melhoria da maturidade das configurações de segurança em ambientes de *data center*. Também possível avaliar as políticas de segurança existentes em normas voltadas para os processos que de utilização destes ambientes a fim de fornecer diretrizes para avaliar a maturidade de segurança das organizações. A seguir (Figura 5), apresenta uma visão geral da aplicação da estratégia descrição de cada atividade.

Figura 5 –Visão de Aplicação da Estratégia Primasia para ambiente de *Data center*s



Fonte : Elaborado pelo Autor

1. **Análise dos Controles de Segurança**: É baseada na seleção de um conjunto de controles de segurança para apoiar a gestão da segurança da informação no ambiente de *data center*. Esta atividade é composta pela aplicação de formulário a um grupo de especialista para definir o nível de priorização dos controles que serão aplicados para o ambiente de *data center*. Os controles serão os mesmo estabelecidos pela estratégia Primasia (ALENAR, 2019), contendo assim o formulário com representação dos 114 controles de segurança que foram extraídos a partir das normas de segurança da informação *ISO/IEC 27001 e 27002*. Após a coleta das informações, as mesma serão analisadas e classificadas em três níveis, que foi proposto para o formulário, sendo eles definidos como: Diretamente Relacionado – DIR , Parcialmente Relacionado - PAR e Pouco Relacionado – POR. Para o levantamento das informações foram utilizados os questionários expostos no Anexo B e Apêndice A.
2. **Avaliação de Maturidade**: Esta atividade será a considerada como segunda etapa do estudo. Será realizada após definição de uma nova classificação da estratégia Primasia aplicada de forma independente, diretamente aplicada ao ambiente de *data center*. Essa nova classificação será embasada, na classificação dos especialistas, associada com a classificação de controle do Primasia, finalizada por identificação do nível de maturidade do COBIT 4.1. A estratégia segue apenas os controles de segurança definidos e considera o nível de importância baseado nos estágios que se encontram os controles, enquadrando o nível de maturidade classificado pelo COBIT para assim definir a o nível de maturidade.
3. **Geração de Resultados:** Esta atividade final da estratégia, reporta o Estágio e Nível de Maturidade em que se encontram as organizações que foram aplicada a estratégia. Também será possível identificar melhorias na política de segurança adequada para atender os requisitos encontrados, incluindo um conjunto de recomendações de melhorias (*Programa de Melhoria*), informando os pontos fortes e fracos de segurança da informação da organização no ambiente de *data center*, com objetivo de auxiliar o monitoramento dos níveis de segurança da informação na organização.

3.2. Análise dos Controles de Segurança

As próximas seções apresentarão a análise dos controles de segurança da informação adaptados para implementação da estratégia Primasia para aplicação em ambientes de *data*

center. Para melhor entendimento foi dividido por seção: classificação dos controles da estratégia Priamasia, os quais servirão de insumo essencial para o andamento do estudo, e classificação dos controles adptado para utilização em ambiente de *data center*.

3.2.1 Classificação dos controles da Estratégia Primasia

Durante o processo de revisão da literatura, foram constatados a utilização de 114 controles definidos pela estratégia Primasia. O Quadro 5 apresenta a classificação dos controles utilizados pela estratégia, a fim de possibilitar definição do nível de maturidade. A utilização do Quadro 5 foi essencial para conseguir realizar a classificação de um novo quadro descrito na próxima seção.

Quadro 5 – Controles Separado por Estágio - Primasia

Estágio	Quantidade de Controles	Controles
Básico	32	A.5.1.1, A.6.1.1, A.6.1.5, A.6.2.2, A.7.1.1, A.7.2.1, A.8.1.2, A.8.1.3 A.8.2.1, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.3, A.9.2.4, A.9.2.5, A.9.4.2, A.9.4.4, A.11.1.5, A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.12.5.1, A.12.6.2, A.13.1.3, A.15.1.3, A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4 e A.18.1.5
Essencial	27	A.5.1.2, A.6.1.2, A.6.2.1, A.7.2.2, A.8.1.1, A.8.3.1, A.9.2.6, A.9.4.3, A.11.1.3, A.11.2.2, A.11.2.3, A.12.1.3, A.12.1.4, A.12.2.1, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.1, A.14.2.6, A.15.1.1, A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.7, A.17.1.1 e A.18.2.2
Intermediário	28	A.7.2.3, A.8.1.4, A.8.2.2, A.9.3.1, A.9.4.1, A.9.4.5, A.11.1.1, A.11.1.2, A.11.2.1, A.11.2.9, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.6.1, A.12.7.1, A.13.1.2, A.13.2.4, A.14.1.2, A.14.1.3, A.14.2.5, A.14.2.9, A.15.1.2, A.15.2.1 A.16.1.3, A.17.2.1, A.18.2.1 e A.18.2.3
Avançado	27	A.6.1.3, A.6.1.4, A.7.1.2, A.7.3.1, A.8.3.2, A.8.3.3, A.9.2.2, A.10.1.1, A.10.1.2, A.11.1.4, A.11.1.6, A.11.2.8, A.12.4.2, A.12.4.3, A.12.4.4, A.13.2.2, A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.7, A.14.2.8, A.14.3.1, 15.2.2, A.16.1.6, A.17.1.2 e A.17.1.3

Fonte : Alencar (2019, p. 172)

3.2.2. Definição de controles adaptado para utilização em ambiente de *Data center*

O modelo dinâmico consiste em estratificar os controles de acordo com a importância dada pelas empresas (ALENCAR 2019). Visando aprofundamento para melhoria do estudo, foi realizado a classificação dos controles utilizados na estratégia Primasia, que será implementado na prática baseado na forma de aplicação independente descrito anteriormente na seção 2.6.2. A escolha da aplicação independente foi embasada pela possibilidade de utilização da estratégia, adequando a necessidade do ambiente de *data*

center com definição de importância dos controles realizada por especialista, com objetivo de se obter resultado mais coerente por meio da aplicação prática da estratégia, contextualizada na segurança da informação em *Data center*.

3.2.2.1 Especificação dos Controles para área de *Data center*

Inicialmente foi enviado o questionário a oito especialistas da área de segurança da informação em *Data centers,* dos oito enviados, três tiverem problemas pessoais e não puderam responder em tempo hábil o questionário. Foi utilizado um formulário (Anexo A) para verificar a experiência e formação de possíveis especialistas, para participação na presente pesquisa. Mesma metodologia realizada por Alencar (2019). O resultado é exibido no Quadro 6.

Quadro 6 – Qualificação dos Especialistas em Segurança da Informação

	Esp.1	Esp.2	Esp.3	Esp.4	Esp.5
Experiência com TIC em (Anos)	12	15	30	20	15
Experiência com segurança (Anos)	12	10	1	8	10
Trabalha em empresa de segurança	Não	Não	Não	Não	Não
Maior cargo assumido	Gerente TI	Gerente TI	Gerente TI	Gerente TI	Gerente TI
Maior titulação	Especialista	Especialista	Especialista	Mestrado	Doutor
Titulação em Andamento	-	-	-	Doutorado	-
Titulação em Área de segurança	-	-	-	-	Sim
Têm experiência com Maturidade	Sim	Sim	Sim	Sim	Sim
Quantidade de Publicações Acadêmicas	1-3	1-3	1-3	4-7	Mais que 7
Quantas delas em segurança	1-3	1-3	1-3	1-3	Mais que 7
Experiência no ensino de TIC	Não	Não	Sim	Sim	Sim
Experiência ensino em segurança	Não	Não	Não	Sim	Sim
Tempo de experiência ensino em TIC em (Anos)	0	0	10	10	10
Quanto tempo em segurança(Anos)	0	0	0	5	8

Com o perfil de especialista atendido, foi solicitado aos especialista que classificassem os 114 controles utilizados na estratégia Primasia, agora focando-os nas necessidades, riscos

e problemas de um *data center*. Um controle de segurança pode ser uma política, prática ou alienações definidas para atingir um propósito específico (LIMA, 2017).

3.2.2.2 Classificação dos controles adaptado para utilização em *Data center*

A separação em três níveis foi realizada, objetivando a implementação de estrutura de peso a ser utilizado na aplicação independente da estratégia Primasia, ficando assim estruturados os blocos de níveis de classificação: “Diretamente Relacionado (DIR)”, utilizado quando o controle aplicado estiver totalmente relacionado ao contexto de segurança da informação associado aos servidores no ambiente de *data center*. O segundo bloco foi denominado de “Parcialmente Relacionado (PAR)”, o qual foi utilizado na classificação dos controles, quando existir algum contexto que ponha em risco a segurança da informação dentro do ambiente de *data center*. O terceiro bloco foi denominado de “Pouco Relacionado (POR)” servindo para classificar os controles, quando não afetarem diretamente a segurança da informação em ambiente de *data centers*.

Os blocos criados para a classificação da estratégia, foram pensados para uma melhor classificação da maturidade aplicadas, as configurações de segurança da informação em ambientes de *data center*. Conseguindo assim um melhor direcionamento das políticas de segurança para um foco mais específico. Espera-se, com essa definição, melhorar a classificação da maturidade possibilitando uma visão focada em *data centers* das configurações que devem ser aplicadas, prevenindo e melhorando os processos aplicados a este contexto.

Foram analisados os questionários (Apêndice A) respondidos pelos 5 especialistas conforme representação exibida no Apêndice B. O método utilizado para classificar o controle será estabelecido pela soma das notas do controle dada por cada especialistas, sendo nota 1 para os controles Poucos Relacionados, nota 2 para os controles Parcialmente Relacionados e nota 3 para controles classificados com Diretamente Relacionados. Desta forma cada controle poderá atingir as notas entre 5 e 15. A nota mínima seria quando todos os 5 especialistas categorizar o controle com pouco relacionado (1+1+1+1+1 = 5 pontos). A nota máxima, 15 pontos, seria quando todos os especialistas categorizassem o controle como Diretamente Relacionado (3+3+3+3+3 = 15 pontos).

A divisão da classificação da avaliação dos controles foi dividida em três blocos iguais conforme apresentados no Quadro 7. Os blocos foram definidos pela constante, subtraindo o valor da soma dais maiores notas pelo valor da soma das menores notas, dividido pela quantidade de classificação de importância. Sendo o calculo representado por "(15 - 5) Mod 3 = 3.33333". Essa constante foi somada ao menor valor de cada grupo de importância.

Quadro 7 – Avaliação dos Controles

Nota do Controle	**Classificação Final**
Entre 5 e 8,333	Pouco Relacionado - POR
Entre 8,34 e 11,666	Parcialmente Relacionado - PAR
Entre 11,67 e 15	Diretamente Relacionado- DIR

Fonte : Elaborado pelo Autor

Para a adaptação do modelo Primasia utilizando aplicação de forma independente, a ser aplicado para área de *data center*, foi realizada uma ponderação da distribuição dos controles propostos por Alencar (2019), de acordo com a importância de priorização dos controles para a área de *data center*, proposto pelos especialistas. Para realizar a ponderação será utilizado a forma exposta no Quadro 4, como a classificação definida por Alencar (2019) dos estágios do Primasia. Além disso será necessário a divisão dos controles, conforme Quadro 5, contendo a classificação dos controles relacionados a importância para área de *data center*. Após realização de associação dos controles da estratégia Primasia, levando em consideração a classificação da importância, foi atribuído uma nova classificação dos controles da estratégia Primasia por nível de importância representados no Quadro 8. Resumindo a classificação final dos especialista a aos controles da estratégia Primasia.

Quadro 8 – Avaliação dos controles dos especialistas

Classificação	**Quantidade Controles**	**Código dos Controles**
Pouco Relacionado - POR	4	8.1.2, 8.1.4, 11.2.9, 14.2.9,

Parcialmente Relacionado - PAR	33	6.1.3, 6.1.4, 6.2.1, 7.2.2, 7.3.1, 8.2.1, 9.4.5, 11.2.5, 11.2.8, 12.1.1, 13.2.4, 14.1.2, 14.2.1, 14.2.2, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.3.1, 15.1.3, 15.2.1, 16.1.4, 16.1.5, 16.1.6, 16.1.7, 17.1.2, 18.1.1, 18.1.2, 18.1.3, 18.1.4, 18.2.1, 18.2.2
Diretamente Relacionado - DIR Diretamente Relacionado - DIR	77	5.1.1, 5.1.2, 6.1.1, 6.1.2, 6.1.5, 6.2.2, 7.1.1, 7.1.2, 7.2.1, 7.2.3, 8.1.1, 8.1.3, 8.2.2, 8.2.3, 8.3.1, 8.3.2, 8.3.3, 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.3.1, 9.4.1, 9.4.2, 9.4.3, 9.4.4, 10.1.1, 10.1.2, 11.1.1, 11.1.2, 11.1.3, 11.1.4, 11.1.5, 11.1.6, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.2.6, 11.2.7, 12.1.2, 12.1.3, 12.1.4, 12.2.1, 12.3.1, 12.4.1, 12.4.2, 12.4.3, 12.4.4, 12.5.1, 12.6.1, 12.6.2, 12.7.1, 13.1.1, 13.1.2, 13.1.3, 13.2.1, 13.2.2, 13.2.3, 14.1.1, 14.1.3, 14.2.3, 15.1.1, 15.1.2, 15.2.2, 16.1.1, 16.1.2, 16.1.3, 17.1.1, 17.1.3, 17.2.1, 18.1.5, 18.2.3

Fonte: Elaborado pelo Autor

Os parâmetros utilizado no presente trabalho, para criação de uma nova classificação utilizada para aplicação da estratégia Primasia foram definidos como:

1) Os controles Diretamente Relacionados – DIR, seriam deslocados para um estágio inferior, mais importante, até chegarem ao mínimo de estágio que é o estágio 1 (Básico), e necessitariam um nível de maturidade maior para serem atingidos. Sendo assim definido um nível a mais, passando a ter o nível mínimo 4. Visto que 3 é o nível mínimo estabelecido pela estratégia Primasia.

2) Os controles Parcialmente Relacionados – PAR, da mesma maneira que o Diretamente Relacionado - DIR, necessitariam um nível de maturidade maior para serem atingidos. Sendo assim, será definido da mesma forma um nível a mais, passando a ter o nível

mínimo 4, porém continuam classificados no mesmo estágio proposto por Alencar (2019).

3) Os controles Pouco Relacionados – POR, não sofreriam diferença na classificação proposta por Alencar (2019). Mantendo-se assim no mesmo estágio e nível que o classificam pela estratégia Primasia, conforme representação do Quadro 6.

O modelo de definição de classificação por pontuação também é defendido por Muthukrishnan e Palaniappan (2016), uma vez que além da avaliação estar relacionada com aspectos quantitativos, a utilização de uma pontuação para definir a escala de maturidade torna mais confiável a análise. Como exemplo da classificação proposta por esse trabalho tem-se:

Exemplo 1) Um controle que estivesse no estágio 3 (Intermediário), em Alencar (2019) e fosse categorizado como Diretamente Relacionado – DIR :

1.1) Iria para um estágio inferior, considerado mais importante e aplicado primeiro.

1.2) Seu nível mínimo de maturidade seria acrescido de + 1 (um ponto), justificando a classificação dos especialistas

Resultado: Sairia do estágio 3 (Intermediário) com nível mínimo 3 para Estágio 2 (Essencial) com nível mínimo 4.

Exemplo 2) Um controle que estivesse no estágio 1 (Básico) em Alencar (2019) e fosse categorizado como Diretamente Relacionado – DIR:

1.1) Iria para um estágio inferior, considerado mais importante e aplicado primeiro. Neste caso como o mesmo já está no mínimo estabelecido pela estratégia Primasia, nada seria feito com a classificação do estágio, mantendo-se no mesmo estágio proposto por Alencar (2019).

1.2) Seu nível mínimo de maturidade seria acrescido de + 1 (um ponto), justificando a classificação dos especialistas

Resultado: Permaneceria no estágio 1 (Básico), porém o nível de maturidade do estágio seria estabelecido para o nível mínimo 4, aumentado assim nível de maturidade a ser alcançada.

Exemplo 3) Um controle que estivesse no estágio 3 (Intermediário) em Alencar (2019) e fosse categorizado como Parcialmente Relacionado – PAR:

1.1) Não seria aplicado.
1.2) Seu nível mínimo de maturidade seria acrescido de + 1 (um ponto), justificando a classificação dos especialistas.

Resultado: Permaneceria no Estágio 3 (Intermediário), porém o nível de maturidade do estágio seria estabelecido para o nível mínimo 4, aumentado assim nível de maturidade a ser alcançada.

Exemplo 4) Qualquer controle enquadrado nos estágios: Estágio 1 (Básico), Estágio 2 (Essencial), Estágio 3 (Intermediário) ou Estágio 4 (Avançado), definidos por Alencar (2019), e fosse categorizado como Pouco Relacionados – POR:

1.3) Continuariam com mesmo estágio e nível de classificação proposta por Alencar (2019).

Resultado: Permaneceria no estágio e nível de maturidade estabelecidos pelo quadro 6, proposto por Alencar (2019).

Após a aplicação dos parâmetros definidos, adaptado para utilização da estratégia Primasia aplicado à segurança da informação em ambiente de *data center*, surge a nova classificação, com mais um nível de maturidade, representada no Quadro 9, estabelecida pela aplicação da estratégia Primasia utilizada de forma independente.

Quadro 9 – Controles separado por estágio com aplicação independente da estratégia Primasia

Estágio	Quantidade de Controles	Identificação dos Controles	Nível de Maturidade Mínimo
Básico	51	5.1.1, 5.1.2, 6.1.1, 6.1.2, 6.1.5, 6.2.2, 7.1.1, 7.2.1, 8.1.1, 8.1.3, 8.2.1, 8.2.3, 8.3.1, 9.1.1, 9.1.2, 9.2.1, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.2, 9.4.3, 9.4.4,11.1.3, 11.1.5, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 12.1.3, 12.1.4, 12.2.1, 12.5.1, 12.6.2, 13.1.1, 13.1.3, 13.2.1, 13.2.3, 14.1.1, 15.1.1, 15.1.3, 16.1.1, 16.1.2, 17.1.1, 18.1.1, 18.1.2, 18.1.3, 18.1.4, 18.1.5,	4
	1	8.1.2	3
Essencial	26	6.2.1, 7.2.2, 7.2.3, 8.2.2, 9.3.1, 9.4.1, 11.1.1, 11.1.2, 11.2.1, 12.1.1, 12.1.2, 12.3.1, 12.4.1, 12.6.1, 12.7.1, 13.1.2, 14.1.3, 14.2.6, 15.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.7, 17.2.1, 18.2.2, 18.2.3	4
Intermediário	22	7.1.2, 8.3.2, 8.3.3, 9.2.2, 9.4.5, 10.1.1, 10.1.2, 11.1.4, 11.1.6, 11.2.8, 12.4.2, 12.4.3, 12.4.4, 13.2.2, 13.2.4, 14.1.2, 14.2.3, 14.2.5, 15.2.1, 15.2.2, 17.1.3, 18.2.1	4
	3	8.1.4, 11.2.9, 14.2.9	3
Avançado	11	6.1.3, 6.1.4, 7.3.1, 14.2.1, 14.2.2, 14.2.4, 14.2.7, 14.2.8, 14.3.1, 16.1.6, 17.1.2	4
			3

Fonte: Autor

O Quadro 9 apresenta a nova classificação da estratégia Primasia o qual pode ser visto a quebra dos estágios em dois níveis, no lugar de um proposto pela estratégia Primasia inicialmente. Os valores de priorização 4 foram definidos para os controles que foram priorizados como diretamente e parcialmente relacionados a segurança da informação em ambiente de *data center*. Para o nível inferior dos estágios foram definidos controles considerados como pouco relacionados a segurança da informação em ambientes de *data center*s, definindo-o com o valor 3 que é o mínimo exigido pela estratégia Primasia para os níveis de Maturidade de controles e estágios.

3.3 Avaliação da Maturidade

Para estratégia Primasia foram definidos 4 estágios: Básico, Essencial, Intermediário e Avançado (ALENAR, 2019). O primeiro estágio denominado como Básico, revela os

controles mais importantes, a ser implantados numa organização, também foi definido o nível mínimo com valor 3 pela estratégia, para que a organização possa mudar de estágio. O segundo estágio, Essencial, garante que todo os controles do básicos foram implementados e estão como nível mínimo com valor 3 atendido. O próximo estágio Intermediário atende os dois estágios anteriores obrigando que todos os controles tenha sido atendido também com o nível mínimo de valor 3, por fim, após atender os três estágios anteriores, consegue-se atingir o nível avançado. Neste estágios estão os controles com menor índice de importância de acordo com as estratégia Primasia, porém, para alcança-los, a organização deverá ter passado por todos os outros estágios anteriores, que contemplam os controles mais importantes.

Para que a organização possa mudar de estágio, além do nível mínimo médio do estágio, se faz necessário atender o nível mínimo em cada controle, de acordo com os níveis de maturidade do COBIT apresentado no Quadro 2 deste documento. Sendo verificado assim o nível de cada controle aplicável à empresa no estágio em questão. Ao chegar no último estágio com todos os níveis de maturidade do COBIT atendido, a organização terá atendido a todos os aspectos considerados pela estratégia.

3.4. Geração de Resultados

Por fim, esta atividade tem como objetivo gerar relatórios que possam ser compreendidos tanto pelo responsável técnico como pela alta direção da organização. Como resultados, esta atividade é composta por dois componentes: o nível de maturidade e programas de melhoria.

O nível de maturidade servirá para a empresa perceber o seu estágio atual, bem como, periodicamente reanalisar a maturidade e verificar a diferença para o estágio anterior. Também pode ser útil para realizar comparativos gerais, alinhamento estratégico, etc. Possíveis exemplos de sua utilização são:

- Ao aplicar alguma nova política ou ferramenta, recalcular a maturidade e verificar se houve mudança.
- Definir um período fixo (por exemplo, seis meses) para recalcular a maturidade e fazer um acompanhamento da empresa.
- Verificar se os recursos estão sendo empenhados para o cumprimento, prioritariamente, dos controles mais críticos (níveis mais baixos da estratégia).

- Possibilidade de comparação, através do nível de maturidade, da presente empresa como outras. Em especial no caso de concorrentes, fusão e etc.
- Simular as mudanças que uma nova ferramenta ou tecnologia poderá proporcionar e calcular a maturidade de forma a verificar se tal ferramenta ou tecnologia gera as mudanças de maturidade esperada. Tal ação pode servir como um dos critérios para compra.
- Verificar que controles estão sendo aplicados e, consequentemente, priorizar as ações de segurança aos controles mais críticos (dos estágios iniciais).

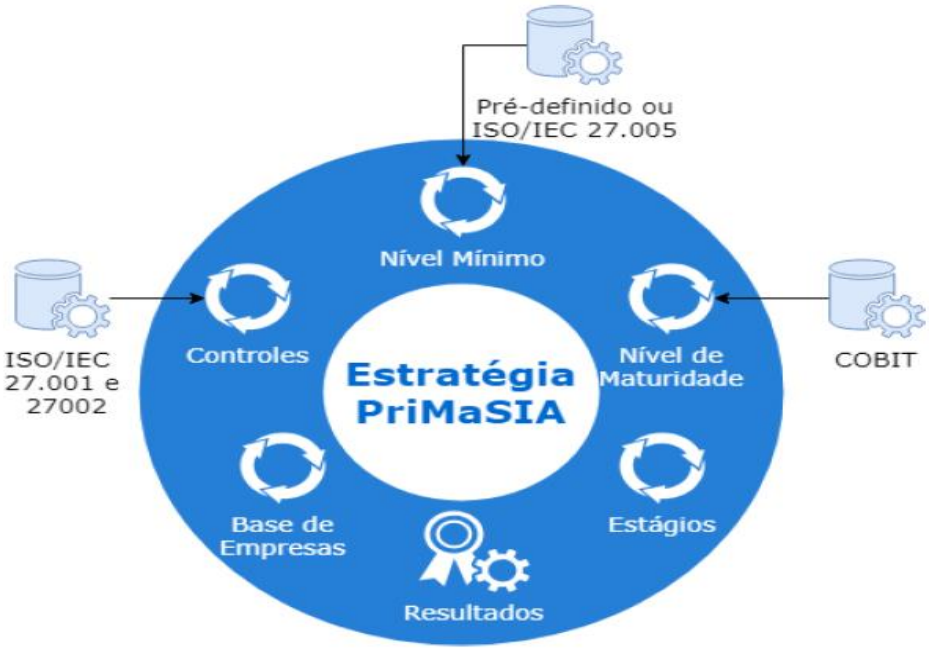
Tais utilizações serão retratadas em relatório como possíveis melhorias para a empresa e na tomada de decisão, como forma de auxiliar a área de TIC e a direção da empresa.

4 APLICAÇÃO PRÁTICA DA ESTRATÉGIA PRIMASIA

O presente capítulo pretende realizar a aplicação prática da estratégia Primasia de forma independente, conforme detalha Alencar (2019). Foram utilizados, inicialmente, os controles padrões descritos por Alencar (2019), com as alterações propostas na presente pesquisa, criou-se novas priorizações de controles e em seguida alcançada uma nova classificação de controles descrito no Capítulo 3. Neste contexto foi criada a definição de níveis mínimos por controle deste estudo, focando-os na análise da segurança da informação nos ambientes de *data centers*, *conforme* proposta deste estudo.

Foi realizada a aplicação da estratégia Primasia através de pesquisa em dois casos reais, visando garantir melhor confiabilidade da adaptação proposta por esta estratégia através do questionário exposto no Anexo B. Em suma, a estratégia Primasia tem suas regras descritas e deve funcionar de forma cíclica indiferente do arcabouço que a fundamente, sendo modular e adaptável ao ambiente (ALENCAR, 2019). A Figura 6 representa a estratégia Primasia ilustrada de forma modular cíclica.

Figura 6 – Estratégia Primasia

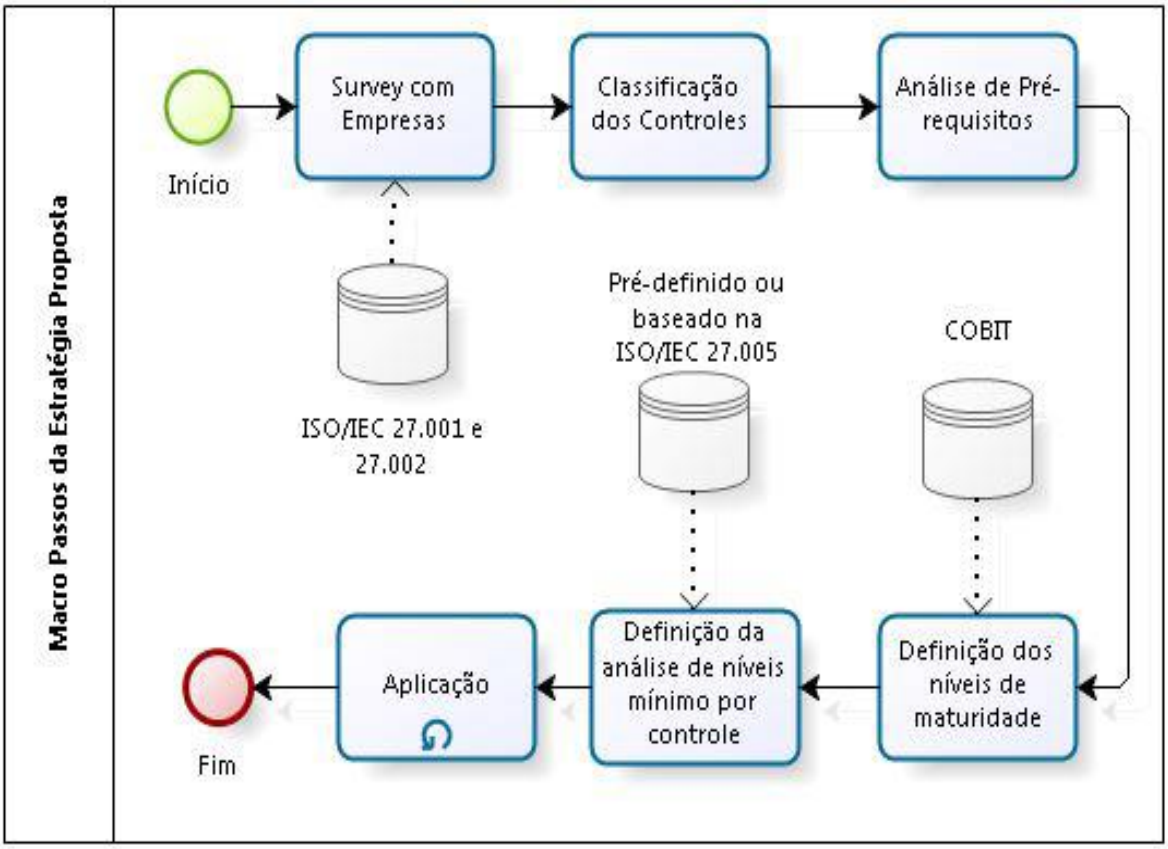


Fonte: Alencar (2019, p.170)

Na aplicação da estratégia foram utilizados os arcabouços padrões (COBIT, ISO/IEC 27.001, 27.002 e 27.005), proposto inicialmente por Alencar (2019), os quais são vistos

como insumos padrões para a estratégia proposta. Neste aspecto, a estratégia permite que os arcabouços podem ser trocados ou atualizados sem prejuízo à estratégia. Se a organização já possuir uma tabela de níveis de maturidade implantada, pode ser utilizada no lugar dos níveis do COBIT. Ou a base de dados da ISO/IEC 27.001 e 27.002 pode ser trocada por um conjunto de controles do NIST, de qualquer outro arcabouço ou junção deles, segundo descreve Alencar (2019), permitindo, com isso, a aplicação da estratégia de forma independente. A Figura 7 apresenta o diagrama de macro passos da estratégia Primasia com seus arcabouços padrões.

Figura 7 – Macro Passos da Estratégia Primasia



Fonte: Alencar (2019, p.171)

Na primeira aplicação em caso real descrito na Seção 4.1 são apresentados os passos práticos de aplicação em uma organização privada que tem como foco o comércio de varejo. A segunda aplicação em caso real, a ser apresentada na Seção 4.2, faz uma avaliação de um organização também privada do segmento de varejo. Ambas organizações possuem um *data center* próprio e são empresa brasileiras que estão localizadas no estado de Pernambuco. O

que diferencia as organizações no aspecto geral é o tamanho do ambiente a ser gerenciado e o tempo de implantação do ambiente de *data center*.

4.1 Primeira Aplicação em Caso Real

A fim de comprovar a definição do nível de maturidade foi realizada a aplicação prática da estratégia Primasia em uma organização privada brasileira, onde neste estudo será apresentada com Organização X.

A Organização X tem mais de 50 anos no mercado, atuando no segmento comercial. Tem sua sede em Recife, Pernambuco, e filial em mais cinco capitais do Nordeste. Seus produtos são comercializados em todo território nacional. A empresa possui mais de 500 colaboradores e tem uma equipe de TIC com mais de 30 pessoas. Em contato com a organização X, foi aplicado o formulário de pesquisa ISO/IEC 27001 e 27002 proposto por Alencar (2019) para classificação dos controles baseados no nível de maturidade do COBIT (Anexo B), utilizando a estrutura atual da organização, a fim de priorizar suas ações em segurança da informação, bem como promover definições básicas para o tratamento dos controles, tendo parâmetros para definições dos investimento e funcionando com um alinhamento da segurança da informação ao negócio.

O questionário propostos (Anexo B) foi aplicado com os gestores da área de Tecnologia da Informação e Comunicação da Organização X, obtendo a resposta de três gestores.

Levando-se em consideração à priorização de cada controle obtido através das três respostas do questionário, ficou definido através de reuniões com gestores, que os controles que divergiram fossem solucionados com o comitê gestor próprio da organização, o qual definiu um único nível para cada controle proposto pelo questionário, através da aplicação da regra de média de nota, calculado por somas das notas do controle divergente, dividido pela quantidade de gestores, utilizando o princípio de arredondamento da parte inteira para casa decimais maiores que 5 (cinco). Pode ser citado como exemplo para organização X o controle 14.1.1, que obteve nota 4 atribuída pelo primeiro gestor, nota 5 atribuída pelo segundo gestor e nota 5 definida pelo terceiro gestor. Foi somada as notas e divida pela quantidade de gestores, sendo, neste exemplo, obtida a média 4.66 obtida através do cálculo (4+5+5) /3. Com a aplicação da regra de arredondamento, o controle passou a ser considerado com nota 5 para a organização.

Após a definição de todos os 114 controles, foi realizada a aplicação da estratégia considerando inicialmente o nível básico. A organização deveria obter nível mínimo 4,

conforme a definição estabelecida no Quadro 9 deste estudo, onde foi definida a regra para classificação dos níveis de maturidade propostas para os controles priorizados para a segurança da informação em ambiente de *data center*.

O nível de maturidade do estágio básico da empresa X, foi embasado por 33 controles com nível 5 (Otimizado), 17 controles com nível 4 (Gerenciado) e 2 controles nível 3 (Definido). Totalizando o nível básico de maturidade neste estágio de: (33 x 5) + (17 x 4) + (2 x 3) finalizando com o cálculo (165 + 68 + 6)/52, que resulta na nota de estágio básico de 4,59. Mesmo ficando acima da média do nível mínimo exigido para o nível de maturidade de estágio básico, a empresa não pode passar para o nível essencial até corrigir os controles reprovados que não atingirem o nível mínimo de maturidade por controle proposto através do Quadro 9.

A organização X não atendeu todos os critérios mínimos de controles básicos, não estando apta para o próximo estágio. A mesma falhou, não atingindo o nível mínimo nos controles: "11.1.3 – Convém que seja protegida e aplicada segurança física para escritórios, salas e instalações" alcançando o nível 3 (Definido) e a matriz de risco tinha apontado como critério mínimo o nível 4 (Gerenciado) e no controle "15.1.3 – Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação" o mesmo alcançou o nível 3 (Definido) e a matriz de risco tinha apontado como critério mínimo o nível 4 (Gerenciado). O Quadro 10 apresenta de forma resumida a analise do estágio básico, para efeito de classificação de nível de maturidade.

Quadro 10 – Resumo do Estágio Básico Aplicado

Estágio: Básico	Quantidade de Controles
Aprovados	50
Reprovados	2
Estágio: Básico	**Controles Analisados**
Controles Aprovados	Nível 4 5.1.1, 5.1.2, 6.1.1, 6.1.2, 6.1.5, 6.2.2, 7.1.1, 7.2.1, 8.1.1, 8.1.3, 8.2.1, 8.2.3, 8.3.1, 9.1.1, 9.1.2, 9.2.1, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.4.2, 9.4.3, 9.4.4, 11.1.5, 11.2.2, 11.2.3, 11.2.4, 11.2.5, 11.2.6, 11.2.7, 12.1.3, 12.1.4, 12.2.1, 12.5.1, 12.6.2, 13.1.1, 13.1.3, 13.2.1, 13.2.3, 14.1.1, 15.1.1, 16.1.1, 16.1.2, 17.1.1, 18.1.1, 18.1.2, 18.1.3, 18.1.4, 18.1.5 Nível 3 8.1.2
Controles Reprovados	11.1.3, 15.1.3 Ambos obtiveram **Nível de Maturidade de Controle = 3**, sendo o **Mínimo exigido para nível = 4**. Resultado : **Impede a mudança de Nível de Básico para o Essencial.**
Nível de Maturidade do Estágio Básico	**4.59**

Fonte: Autor

Sendo um estudo prático, foi realizado a classificação dos demais estágios a fim de identificar para organização se a mesma priorizou outros controles definidos em estágio mais avançado.

No estágio Essencial, a análise resultou em dois controles que falharam. Foram eles: “8.2.2 – Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização”, e o controle “11.1.2 – Convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis”.

A classificação destes controles ficaram no nível 3 (Definido), sendo que o mínimo para avançar para o próximo estágio para esses controles também seria o nível 4 (Gerenciado). A média de maturidade para esse estágio Essencial, foi de 4,23, embasado por 10 controles com nível 5 (Otimizado), 17 controles com nível 4 (Gerenciado) e 3 controles com nível 3 (Definido).

O Quadro 11 apresenta o resumo com os controles reprovados e aprovados, bem como média do Nível de Maturidade do estágio Essencial. O estudo demonstra que a organização priorizou 24 controles Essenciais, porém deixou 2 controles do estágio básico, que são mais relevantes no estado de reprovado, demonstrando falta de gestão na priorização de controles mais críticos.

Quadro 11 – Resumo do Estágio Essencial Aplicado

Estágio: Essencial	**Quantidade de Controles**
Aprovados	24
Reprovados	2
Estágio: Essencial	**Controles Analisados**
Controles Aprovados	Nível 4 6.2.1, 7.2.2, 7.2.3, 9.3.1, 9.4.1, 11.1.1, 11.2.1, 12.1.1, 12.1.2, 12.3.1, 12.4.1, 12.6.1, 12.7.1, 13.1.2, 14.1.3, 14.2.6, 15.1.2, 16.1.3, 16.1.4, 16.1.5, 16.1.7, 17.2.1, 18.2.2, 18.2.3 Nível 3 Não existe controles neste Estágio com esse nível
Controles Reprovados	8.2.2, 11.1.2 Ambos controles obtiveram **Nível Maturidade de Controle = 3,** sendo o **Mínimo exigido para nível = 4.** **Resultado : Impede a mudança de Nível de Essencial para Intermediário.**
Nível de Maturidade do Estágio Essencial	**4.23**

Fonte: Autor

A aplicação do estágio de Intermediário realizado na organização X falhou nos seguintes controles: “10.1.2 - Convém que uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas, seja desenvolvida e implementada ao longo de todo o seu ciclo de vida”, “11.1.4 - Convém que sejam projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes”, “14.1.2 - Convém que as Informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e modificações”. “15.2.1 - Convém que a Organização monitore, analise criticamente e audite intervalos regulares, a entrega dos serviços executados pelos fornecedores. A classificação final destes controles que falharam foi concebida da seguinte forma. O controle 11.1.4, ficou no nível 3 (Definido), e demais no nível 2 (Repetível), permanecendo o nível mínimo para avançar para o próximo estágio com valor 4 (Gerenciado). A média de maturidade para esse estágio Intermediário, foi de 3,73, composta por 4 controles com nível 5 (Otimizado), 17 controles com nível 4 (Gerenciado) e 1 controle com nível 3 (Definido) e 3 controles no nível 2 (Repetível). O Quadro 12 apresenta o resumo da aplicação da estratégia Primasia para o estágio Intermediário.

Quadro 12 – Resumo do Estágio Intermediários Aplicado

Estágio: Intermediário	Quantidade de Controles
Aprovados	21
Reprovados	4
Estágio: Essencial	**Controles Analisados**
Controles Aprovados	Nível 4 7.1.2, 8.3.2, 8.3.3, 9.2.2, 9.4.5, 10.1.1,, 11.1.6, 11.2.8, 12.4.2, 12.4.3, 12.4.4, 13.2.2, 13.2.4, 14.2.3, 14.2.5, 15.2.2, 17.1.3, 18.2.1 Nível 3 8.1.4, 11.2.9, 14.2.9
Controles Reprovados	10.1.2 , 11.1.4 , 14.1.2 , 15.2.1 O controle 11.1.4 obteve **Nível Maturidade de Controle = 3,** sendo o **Mínimo exigido para nível = 4**. Demais Controles (10.1.2, 14.1.2, 15.2.1) apresentaram **Nível Maturidade de Controle = 2,** sendo o **Mínimo exigido para nível = 4**. Resultado : **Impede a mudança de Nível de Intermediário para Avançado; Média de Estágio menor que o mínimo = 4**
Nível de Maturidade do Estágio Intermediário	**3.73**

Fonte: Autor

O último estágio aplicado a organização X foi o Avançado. O mesmo está associado a 11 controles com nível 4, porém a organização falhou em dois controles com nível abaixo de 4 sendo estes controles:

- "14.2.4 – Convém que Modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas".
- "14.2.8 – Convém que Testes de funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas".

Ambos os controles foram aferidos no nível 3 (Gerenciado), porém o mínimo seria o nível 4. A média para o estágio ficou em 3,9, tendo os controles classificados da seguinte forma: 2 controles foram definidos com nível 3 (Definido), 8 controles definidos com nível 4 (Gerenciado) e apenas 1 controles ficou o nível 5 (Otimizado). O Quadro 13 apresenta o resumo do estágio Avançado Aplicado.

Quadro 13 – Resumo do Estágio Avançado Aplicado

Estágio: Intermediário	Quantidade de Controles
Aprovados	9
Reprovados	2
Estágio: Essencial	**Controles Analisados**
Controles Aprovados	Nível 4 6.1.3, 6.1.4, 7.3.1, 14.2.1, 14.2.2,, 14.2.7, 14.3.1, 16.1.6, 17.1.2 Nível 3 Não Implementa o Nível 3 para o Estágio
Controles Reprovados	14.2.4 14.2.8 Ambos controles obtiveram **Nível Maturidade de Controle = 3,** sendo o **Mínimo exigido para nível = 4**. Resultado : **Impede a permanência no nível Avançado;**
Nível de Maturidade do Estágio Intermediário	**3.90**

Fonte: Autor

Apesar da organização conseguir obter um média geral de 4,11, o estágio enquadrado foi o Básico, com nota 4,59. Visto que, em todos os níveis houveram falhas em mais de um controle o que compromete a melhoria de seu nível de maturidade. Para melhor apresentação dos resultados, foi idealizado um resumo dos estágios de maturidade analisados para empresa "X" exibindo a quantidade de controles aprovados bem como

informar quantidade e classificar os que foram reprovados. No resumo é apontado a média de cada estágio. O Quadro 14 contempla as médias por estágio de maturidade.

Quadro 14 – Média de Maturidade Organização X por Estágio

Estágios:	Básico Qtd Controles	Essencial Qtd Controles	Intermediário Qtd Controles	Avançado Qtd Controles
Aprovados	50	24	21	9
Reprovados	2	2	4	2
Controles Reprovados	11.1.3, 15.1.3	8.2.2, 11.1.2	10.1.2 , 11.1.4 14.1.2 , 15.2.1	14.2.4 14.2.8
Nível de Maturidade por Estágio	4.59	4.23	3.73	3.90

Fonte: Autor

O Resultado final da aplicação da estratégia Primasia para organização “X”, mostra que a mesma, foi enquadrada com nível de maturidade básico, por ter dois controles reprovados nesse nível. Apesar da classificação do nível de maturidade básico ter sido de 4.59, acima da média de 4.00, a estratégia Primasia definem que todos os controle devem ser aprovados por da média estabelecida a qual foi definida no capítulo 3 deste estudo. A organização “X” precisa corrigir oito(controles) para chegar ao nível intermediário.

No total foram identificados 8 controles que precisam de acompanhamento para que a organização possa resolver, e assim ser re-enquadrada do estágio básico para o estágio Intermediário. O quadro 15 exibe a quantidade de controles por estágios. Sendo o estágio Básico de maturidade obtida através da aplicação da estratégia Primasia organização “X”.

Quadro 15 – Média de Maturidade Organização “X” final

Quantidades	Estágios
2	Básico
2	Essencial
4	Intermediário
2	Avançado

Fonte: Autor

4.2 Segunda Aplicação em Caso Real

A fim de comprovar a definição do nível de maturidade, foi realizada a aplicação prática da estratégia Primasia em uma segunda organização de origem brasileira, onde neste estudo será apresentada com Organização Y.

A Organização Y tem mais de 15 anos no mercado, atuando no segmento comercial, tem sua sede em Recife, Pernambuco, e filial em mais 4 capitais do Nordeste. Seus produtos são da área automotiva sendo comercializado apenas nas lojas físicas ou por televendas. A empresa possui mais de 120 colaboradores e tem uma equipe de TIC 5 pessoas. Em contato com a organização Y, foi aplicado o formulário de pesquisa ISO/IEC 27001 e 27002, proposto por Alencar (2019) para classificação dos controles baseados no nível de maturidade do COBIT (Anexo B), utilizando a estrutura atual da organização, o questionário foi respondido por dois diretores da organização e um gestor da área de Tecnologia da informação. Foi solicitado, da mesma forma que na empresa X, que os controles que divergissem fossem solucionados internamente pela organização. De posse do questionário respondido foi aplicada a estratégia para mensurar o estágio e nível de maturidade da organização em questão.

A aplicação da estratégia foi realizada considerando o estágio mais importante, o estágio básico, conforme preconiza Alencar (2019). Foi constatado que a organização Y não atendeu todos os critérios mínimos de controles básicos, não estando apta para o próximo estágio. A organização Y falhou, não atingindo o nível mínimo em 25 controles dos 52 aplicados. Para facilitar a leitura foi confeccionado o Quadro 16 com todos os controles reprovados e seus respectivos níveis apresentados.

Quadro 16 – Controles Reprovados Estágio Básico Organização Y

Controle	**Descrição do Controle**	**Nível Maturidade Atingido**
6.1.1	Todas as Responsabilidades pela segurança da informação sejam definidas e atribuídas	2
6.1.5	Todas Segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto.	2
8.2.1	Informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.	2
8.2.3	Procedimentos para o tratamento dos ativos sejam desenvolvidos e	3

	implementados de acordo com o esquema de classificação da informação.	
8.3.1	Procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.	3
9.1.1	Política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.	3
9.1.2	Usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.	2
9.2.3	Concessão e uso de direitos de acesso privilegiado sejam restritos e controlados.	3
9.2.5	Proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.	3
9.2.6	Direitos de acesso dos funcionários sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após mudança de atividades.	3
11.1.5	Projetado e aplicado procedimentos para o trabalho em áreas seguras.	2
11.2.4	Equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.	2
11.2.5	Equipamentos, informações ou software não sejam retirados do local sem autorização prévia.	2
12.1.3	Utilização dos recursos seja monitorada e ajustada e as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido	3
12.2.1	Implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, adequado programa de conscientização do usuário.	3
12.6.2	Estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.	2
13.1.1	Redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.	2
13.1.3	Grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.	3
13.2.1	Procedimentos e controles de transferências formais, sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos recursos de comunicação.	3
13.2.3	Informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.	2
14.1.1	Requisitos relacionados com segurança da informação sejam	3

	incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas.	
18.1.1	Requisitos legislativos estatutários, regulamentares e contratuais, e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados	2
18.1.2	Procedimentos sejam implementados para garantir a conformidade com os requisitos legislativos, e contratuais relacionados com direitos de propriedade intelectual	3
18.1.4	Privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.	3
18.1.5	Controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.	3

Fonte: Autor

Devido a quantidade de controles com falhas, a organização não conseguiu obter um média geral de 4,00, o estágio enquadrado Básico obteve média 3,23.

Através da aplicação da estratégia para o estágio Essencial foi possível identificar falha em dez controles que será apresentado no Quadro 17 a seguir:

Quadro 17 – Controles Reprovados Estágio Essencial Organização Y

Controle	**Descrição do Controle**	**Nível Maturidade Atingido**
9.3.1	Usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.	3
9.4.1	Acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.	3
11.1.2	Áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.	2
12.1.2	Mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.	2
12.3.1	Cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente. Conforme a política de segurança.	2
12.4.1	Registros (log) das atividades do usuário, exceções, falhas e	3

	eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente.	
13.1.2	Mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, sejam identificados e incluídos em acordo de serviços de rede.	3
16.1.3	Funcionários e partes externas que usam os sistemas e serviços de informação, sejam instruídos a registrar e notificar quaisquer fragilidades de segurança da informação.	3
18.2.2	Gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas.	2
18.2.3	Sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação.	2

Fonte: Autor

Devido a quantidade de controles com falha, a organização não conseguiu obter um média geral de 4,00 sendo enquadrado no estágio Essencial com média 3,48.

O estágio Intermediário também não conseguiu atender todos controles definidos. Foi identificado seis controles que não conseguiram atingir o nível mínimo exigido pela matriz da estratégia.

Os controles que precisam ser revistos na organização foram representados pelo Quadro 18 apresentando a seguir.

Quadro 18 – Controles Reprovados Estágio Intermediário Organização Y

Controle	**Descrição do Controle**	**Nível Maturidade Atingido**
8.3.2	Mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.	2
10.1.2	Política sobre o uso, proteção e ciclo de vida das chaves criptográficas, seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.	3
11.1.6	Pontos de acesso, que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação.	2
11.2.8	Usuários assegurem que os equipamentos não monitorados	2

	tenham proteção adequada.	
15.1.2	Sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar, ou prover componentes de infraestrutura.	2
17.1.3	Organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos, para garantir que são válidos e eficazes.	3

Fonte: Autor

O último estágio avaliado foi estágio Avançado. Nesse estágio foram reprovados três controles que foram representados pelo Quadro 19 Foi constatado que onze controles passaram na avaliação o que mostra que a organização priorizou de forma errada esse controles, ficando em estágios anteriores outros controles com falha.

Quadro 19 – Controles Reprovados Estágio Avançado Organização Y

Controle	**Descrição do Controle**	**Nível Maturidade Atingido**
6.1.3	Contatos apropriados com autoridades relevantes sejam mantidos. (fiscais, polícia, bombeiros...)	2
14.2.1	Regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.	2
15.2.1	Organização monitore, analise criticamente e audite a intervalos regulares, a entrega dos serviços executados pelos fornecedores..	2
17.1.3	Organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos, para garantir que são válidos e eficazes.	3

Fonte: Autor

O Quadro 20 demonstra a classificação final da média de maturidade por estágio obtido pela organização Y. O Nível de maturidade da Organização Y após aplicação da estratégia ficou classificado como: Básico com média de 3,23.

Quadro 20 – Média de Maturidade organização Y

Estágio de Maturidade	Média de Maturidade
Básico	3,23
Essencial	3,48
Intermediário	3,32
Avançado	3,23

Fonte: Autor

Em comparação com a Empresa X percebe-se um nível bem abaixo da Empresa Y. Mesmo ambas sendo categorizadas no Estágio Básico, a Empresa X ficou em Básico 4,59, enquanto a Empresa Y alcançou o Básico 3,23. Além disto, percebeu-se que a Empresa X tem um número maior de controles com maior maturidade em todos os estágios, o que demonstra uma maior preocupação e aplicação dos controles de segurança da informação.

Em ambos os casos, empresas X e Y, verificou-se o dispêndio de recursos para o atendimento de um conjunto de controles que não são os mais importantes para a empresa. Ou seja, recursos estão sendo direcionados para a área de segurança da informação, mas não estão sendo aplicados nos controles mais críticos, demonstrando uma falta de alinhamento da estratégia e desejos corporativos com as ações em nível tático e gerencial.

Em suma, a estratégia Primasia foca em duas áreas críticas: priorização e aferição da maturidade. Ficando claro, neste trabalho, a importância desses dois pilares. Foi possível verificar a falta de priorização em ações para atendimento dos controles mais críticos, bem como foi possível mensurar a maturidade, mostrando os pontos fortes e falhos de cada empresa, e tendo um parâmetro de comparação entre as organizações.

5 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Esta seção apresenta as considerações finais da pesquisa e como seus objetivos foram alcançados. Por fim, ciente que todo trabalho é passível de melhorias e continuações, uma lista, não exaustiva, de trabalhos futuro é apresentada.

5.1 Considerações Finais

O trabalho apresentado realizou a aplicação da estratégia Primasia de forma independente (ALENCAR, 2019), para avaliar a maturidade das organizações e priorização da segurança da informação aplicada ao ambiente de *data center*, independente de estrutura de hardware, software ou sistemas operacional, sendo considerado o contexto da segurança da informação de forma mais abrangente, não focados apenas no servidores, mas em todos os processo ou serviços que estão envolvidos em manter a segurança da informação no ambiente de *data center*.

Como insumo para aplicação da estratégia para área definida, foi realizada uma pesquisa bibliográfica envolvendo assuntos associados a normas e modelos de maturidade, foco do objeto de estudo, levando-se em consideração pesquisas em áreas acadêmicas, documentos do meio corporativo e normativos que contribuíram com melhor percepção do aprendizado, atendendo assim o primeiro objetivo específico (realizar levantamento bibliográfico sobre normas e modelos de maturidades associados a segurança da informação, que permitem a utilização em ambiente de *data center*, a fim de melhor compreender o assunto a ser estudado).

Na pesquisa bibliográfica foram encontrados vários documentos, porém apenas três trabalhos puderam ser considerados como correlatos direto à presente pesquisa, cujo a principal fonte foi o trabalho de Alencar (2019), trabalho que esta pesquisa desmembrou. As referências, revisões da literatura e mapeamento sistemático trazido por Alencar (2019) foram analisados e complementado pelo presente autor através de sua pesquisa bibliográfica. O primeiro estudo é de Lima (2017), o qual expõe a desenvolvimento de uma metodologia para avaliar a maturidade associada a segurança da informação em *data centers*, usando controles da ISO/IEC 27002. A principal diferença nos estudos está relacionada ao foco estimado da pesquisa. No trabalho Lima (2017) o foco foi dado no âmbito da segurança da informação em servidores. O presente trabalho realizou a analise da segurança da informação no ambiente de *data center* como um todo.

No segundo estudo (ONO, 2014), apresenta indicadores de desempenho em *data center*. O trabalho apresenta os benefícios que oferece a seus clientes a aplicação de indicadores de desempenho e de performance para medir, avaliar e otimizar os resultados da administração das instalações de TI aplicados aos *data center*s. No decorrer do estudo, Ono (2014) apresenta os principais indicadores voltados para administração do ambiente de *data center* considerando o modelo COBIT 4.1, que também foi utilizado pela estratégia Primasia para evidenciar os níveis que estão os estágios definido pela maturidade alcançada. Porém, no estudo de Ono (2014), não foi realizada nenhuma aplicação real dos indicadores.

O último trabalho propõem a criação de um modelo de maturidade desenvolvido por Muthukrishnan e Palaniappan (2016), chamado *Security Metrics Maturity Model for Operational Security* onde foram criadas identificações de elementos de qualidade de segurança para determinar métricas para um ambiente de segurança operacional. A avaliação dessas métricas foram definidas e realizada a partir das análises quantitativa e qualitativa com base em dois níveis de avaliação denominadas *Quantitative Matured Metrics* (QtMM) e *Qualitatives Matured Metrics*, sendo as empresa responsável por definir métricas para priorização.

A escolha da aplicação da estratégia Primasia está associada a uma evolução de modelos de maturidade existente proposta por Alencar (2019), tendo a diferença de não apenas propor um modelo para mensuração, mas, também, um guia para implantação da segurança da informação através da priorização dos controles. Sendo levado em consideração a possibilidade de aplicar controles de acordo com a importância apontada pelas organizações, através de uma visão modular que permite utilizar os diversos modelos existentes, adequando a necessidade de cada organização ou setor da mesma, facilitando a implantação. Diferente de outras estratégias e modelos citados, que trabalham com uma visão fixa, não se adaptando ao ambiente das empresas. Tal justificativa, inclusive, é um dos pontos embasados por Alencar (2019) como diferencial e justificativa em sua tese doutoral.

O segundo objetivo específico do trabalho era: Apresentar suporte teórico consolidando uma visão de como a avaliação da maturidade pode auxiliar no gerenciamento da informação. Acredita-se que o mesmo foi cumprido ao apresentar o entendimento e avaliação das políticas e controles de segurança existentes em normas internacionais, as quais são voltadas a fornecer diretrizes e referenciar boas práticas no que tange a garantia da segurança das informação nas organizações. Desta forma o trabalho contribui com visão pautada de diversos ângulos, descrevendo as principais normas internacionais citadas em trabalhos correlatos atendendo ao referido objetivo específico.

Uma grande contribuição foi dada com a adaptação da estratégia Primasia, focando-a na avaliação da segurança da informação em ambientes de *Data centers* (terceiro objetivo específico). Acredita-se que o objetivo tenha sido alcançado através da nova classificação dos controles realizada, baseado na importância definida a cada controle, levando em consideração o principal aspecto da segurança da informação no ambiente de *Data center*. As possibilidades de adaptação e aplicações independentes foram vislumbradas por Alencar (2019) na definição da estratégia Primasia, porém não tinham sido, de fato, implementadas e, muito menos, aplicadas em ambientes reais. Seguindo as possibilidades propostas por Alencar (2019) e obedecendo aos princípios da Estratégia Primasia, o presente trabalho avança no estado da arte comprovando que a possibilidade proposta em Alencar (2019) é viável, bem como demonstrando-a em dois casos reais.

Outra contribuição relevante foi obtida com a avaliação dos relacionamentos entre os controles da ISO/IEC 27001 e 27002, além de uma priorização dos mesmos e criação de um novo nível de classificação dos controles, ponderado com maior peso os controles que foram considerados como diretamente e parcialmente relacionados ao âmbito da segurança da informação em ambiente de *Data centers.* Tal ação, citada no quarto objetivo específico, foi essencial para o entendimento do ambiente e trabalhou em conjunto com o objetivo anterior, para que se tenha a estratégia Primasia propícia para a análise dos ambientes desejado, neste caso, de *Data centers.*

O quinto objetivo específico proposto era: Gerar subsídios que permitam acompanhamento de estágios de classificação da organização, baseada em controles que foram priorizados com a aplicação da estratégia, a fim de definir o nível de maturidade da organização, considerando os aspectos relacionados à segurança da informação aplicados em ambiente de *data center*. Percebe-se que as ações realizadas vão traçando um caminho para o desenvolvimento da solução e, consequentemente, passando pelos objetivos. Desta forma, ao correlacionar os controles da área de segurança da informação com a área de *Data centers* e especificar a estratégia Primasia têm-se subsídios e uma ferramenta para acompanhamento e gestão da organização, na área especificada, e, desta forma, cumprido o objetivo em questão. Salienta-se que que, com esses insumos criados, foram gerados subsídios que permitiram o acompanhamento de estágios de classificação da organização, baseada em controles que foram priorizados com a aplicação da estratégia, a fim de definir o nível de maturidade da organização.

Por fim, ao aplicar a estratégia Primasia em duas organizações, foi possível mensurar o nível de maturidade das organizações aplicado ao ambiente de *data centers*. No primeiro

estudo, os resultados permitem demonstrar que a organização precisa melhorar em dois aspectos de nível básicos para evoluir para um estágios de maturidade superior. Seguindo com estudo, dos demais estágios, houve decréscimos na escala de maturidade o que comprova que a organização priorizou alguns controles de estágios superior e deixou controles de estágios inferior sem atender. A estratégia foi eficiente em não só calcular o nível de maturidade, como em apontar os pontos de melhorias para a organização a qual foi aplicada, priorizando os controles e indicando áreas de carência e investimento de recursos.

No segundo estudo de aplicação prática real, a estratégia obteve novamente resultados diferentes na escala de maturidade quando observado os estágios. A estratégia permitiu identificar varias falhas nas configurações de segurança no estágio básico. Tais informações foram úteis para propor políticas para melhorar os parâmetros de segurança no ambiente de *data center*. Os demais estágios apresentaram também decréscimos na escala de maturidade o que comprova que a organização precisa investir em melhorias em seus controles básicos de segurança, e melhor priorizar os controles dos demais estágios. Após toda a avaliação foram identificados os impactos dos controles no negócio, levando as respectivas organizações a refletirem sobre suas atividades que entraram em conflito com as recomendações das normas internacionais de segurança. Portanto, as duas organizações começaram a analisar possíveis mudanças de melhorias aplicadas ao modelos de negócio. Com a aplicação prática em ambientes reais da estratégia foi alcançado o último objetivo proposto neste estudo.

Os cinco objetivos específicos propostos podem ser entendidos como etapas para se alcançar o objetivo geral do trabalho: “Analisar o nível de maturidade dos ambientes de *data center*s corporativos no que tange à segurança da informação”. Com a completude do atendimento dos objetivos específicos, acredita-se que o objetivo geral também foi alcançado com sucesso.

Por fim, entende-se que o uso da estratégia é viável de ser aplicada em qualquer tamanho de ambiente *data center* o qual a organização esteja inserida, desta maneira segundo Alencar (2019), as organizações estão moldando o processo de maturidade ao seu negócio e não o contrário. Buscando obter uma melhoria na área de segurança da informação e não a aplicação de um modelo ou normativo formal para estar em conformidade. Servindo, como mostrado nos dois casos reais aplicados no presente trabalho, que a estratégia é viável e eficiente para a mensuração da maturidade e para a priorização dos controles de segurança da informação.

5.2 Trabalhos Futuros

Para dar continuidade a este trabalho, são apresentadas as seguintes sugestões de trabalhos futuros.

- Estender esse trabalho a um ambiente de *data centers* que ofereçam serviços em *cloud*. Foi avaliado neste trabalho dois estudos de aplicação de caso real relevantes, mas que tinham o *data centers* próprios. A análise envolvendo cenários mais complexos poderá gerar resultados diferentes mostrando outros pontos não abordados por este trabalho. Principalmente a importância da adoção de medidas de segurança neste tipo arquitetura em nuvem, o que poderá proporcionar novos riscos.
- Realizar estudos em número maior de organizações de pequeno a grande porte, público e privado a fim de analisar existência de correlação entre o nível de maturidade aplicado ao ambiente de *data center* relacionado aos recursos disponibilizados para investimentos em segurança da informação, avaliando assim a preocupação da organização com a segurança da informação.
- Agregar na adaptação da estratégia Primasia aplicado à ambiente de *data center* outras normas internacionais de segurança que venha melhorar a definição do nível de maturidade, focando em alguns dispositivos específicos como, por exemplo, servidores de banco de dados. Como exemplo de normas e documentos a serem analisados a inclusão, tem-se: *Shared Assessments Agreed Upon Procedures* (AUP) e *Open Web Application Security Project* (OWASP);
- Aplicar a estratégia em outros setores da tecnologia da informação que lidam com interface de manipulação de informações. Esta estratégia avaliou apenas segurança da informação em ambiente de *data center.* Acredita-se que seja possível aplicar a estratégia para área que lidem diretamente com informações estratégicas como, *Bussines Inteligence, Data Warehouse, Data Science.*

Por fim, ressalta-se que a presente estudo buscou evoluir a temática nos aspectos acadêmicos e profissionais, sendo os trabalhos futuros supracitados possíveis ações que permitam alcançar melhorias na aplicação da estratégia. Porém a segurança da informação ainda necessita de muitas ações e pesquisas para suprir demandas que irão surgir uma vez que a informação sempre estará como princípio de sobrevivência numa sociedade cada vez mais conectada.

REFERÊNCIAS

ABNT. *NBR ISO/IEC 17799 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação*. Rio de Janeiro - RJ, Brasil: ABNT, 2006. 120 p.

ABNT. *NBR ISO/IEC 27005 - Tecnologia da informação - Técnicas de segurança -Gestão de riscos de segurança da informação*. Rio de Janeiro - RJ, Brasil: ABNT, 2011.87 p.

ABNT. *NBR ISO/IEC 27001 - Tecnologia da informação — Técnicas de segurança - Sistemas de gestão da segurança da informação — Requisitos*. Rio de Janeiro - RJ, Brasil: ABNT, 2013a. 32 – 80 p.

ABNT. *NBR ISO/IEC 27002 - Tecnologia da Informação-Técnicas de Segurança -Código de Prática para controles de segurança da informação*. Rio de Janeiro - RJ, Brasil: ABNT, 2013b. 112-120 p.

ALBUQUERQUE JUNIOR, A. E.; SANTOS, E. M. *Adoção de Medidas de Segurança da Informação: Um Modelo de Análise para Institutos de Pesquisa Públicos*. Revista Brasileira de Administração Científica,, v. 5, n. 2, p. 46-59, 2014.

ALENCAR, G. D. *Primasia: Uma Estratégia para Priorização e Avaliação da Maturidade da Segurança da Informação Adaptável ao Ambiente Corporativo*. 182 p. Tese (Doutorado em Gestão da Tecnologia da Informação) - Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2019.

ALENCAR, G. D. *Estratégias para Mitigação de Ameaças Internas*. 137 p. Dissertação (Mestrado em Ciência da Computação) - Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2011.

ALMEIDA NETO, H. R. *Um Modelo de Maturidade para Governança Ágil em Tecnologia da Informação e Comunicação*. 322 p. Tese (Tese de Doutorado) — Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2015.

ALMEIDA NETO, H. R. D. de; MAGALHÃES, E. M. C. de; MOURA, H. P. de; TEXEIRA FILHO, J. G. d. A.; CAPPELLI, C.; MARTINS, L. M. F. *Avaliação de um Modelo de Maturidade para Governança Ágil em Tecnologia da Informação e Comunicação*. *iSys* – Revista Brasileira de Sistemas de Informação, v. 8, n. 4, p. 44–79, 2015b.

ARAÚJO, W. J. *A Segurança do Conhecimento nas Práticas da Gestão da Segurança da Informação e da Gestão do Conhecimento*. 280 p. Tese (Doutorado em Ciência da Informação) — Universidade de Brasília, Brasília - DF, Brasil, 2009.

BARKER, L. K.; NELSON, L. D. *Security Standards- Government and Commercial*. AT&T Technical Journal, v. 67, n. 3, p. 9–18, 1988.

BAYUK, J. L. *The Utility of Security Standards. Proceedings - International Carnahan Conference on Security Technology*, p. 1–6, 2010.

BENZ, K. H. *Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI: estudos de caso em instituições financeiras*. 200 p. Dissertação (Mestrado em Administração) - Escola de Administração, Universidade Federal do Rio Grande do Sul, Porto Alegre - RS, Brasil, 2008.

CASTELLS, M. *A Sociedade em Rede*. 10ª. ed. [S.l.]: Paz e Terra, 2009. 630 p. ISBN 9788577530366.

CHATZIPOULIDIS, A.; MAVRIDIS, I. *An Ict Security Management Framework. Securityand Cryptography* (SECRYPT), Proceedings of the 2010 International Conference on. Anais, 2010.

CORDEIRO, E. S. d. P. *Fatores críticos de sucesso para o aprimoramento da maturidade da gestão da segurança da informação das instituições federais de ensino superior*. 199 p. Dissertação (Mestrado em Ciência da Computação) - Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2017.

COOK, C.; HEATH, F.; THOMPSON, R. L. A meta-analysis of response rates in Web-or Internet-based surveys. Educational and Psychological Measurement, Durham, v. 60, n. 6, p. 821-836, Dec. 2000.

CÔRTE, K. *Segurança da Informação Baseada no Valor da informação e nos pilares Tecnologia, Pessoas e Processo.* Tese (Doutorado em Ciência da Informação) -Faculdade de Ciência da Informação da Universidade de Brasília, Brasília - DF, Brasil, 2014.

CONDON, E.U. *Science and security. The American Biology Teacher*, v. 10, n.4, pp. 107-108, apr. 1948.

DA SILVA, C. A. *Gestão da segurança da informação: um olhar a partir da Ciência da Informação*. 99 p. Dissertação (Mestrado em Ciência da Informação) - Pontifícia Universidade Católica de Campinas, Campinas - SP, Brasil, 2009.

DINIZ, I. J. D.; MEDEIROS, M. F.; VERAS, M. *Governança de TI: a visão dos concluintes de Administração e Ciências da Computação. Revista* Brasileira de Administração Científica, v. 3, n. 2, p. 7–24, 2012.

ECO, U. *Como se faz uma tese em ciências humanas.* Tradução de Ana Falcão Bastos e Luís Leitão. 13. ed. Queluz de Baixo, Editorial Presença, 2007.

FERREIRA, F. N. F. *Segurança da informação*. Rio de Janeiro: Editora Ciência Moderna Ltda., 2003. 162p.

FERREIRA, F. N. F.; ARAUJO, M. T. *Política de Segurança da Informação: Guia Prático para Elaboração e Implementação*. 2ª. ed. Rio de Janeiro - RJ, Brasil: Ciência Moderna, 2009. 224 p.

FONTES, E. L. G. *Segurança da Informação: O Usuário Faz a Diferença*. São Paulo -SP, Brasil: Editora Saraiva (Edição Digital), 2012.

FULLER, J. et al. *Fedora 18 Security Guide - A Guide to Securing Fedora Linux*. 2013.

GHAZOUANI, M.; MEDROMI, H.; SAYOUTI, A.; BENHADOU, S. *An integrated use of iso27005, melhoria and multi-agents system in order to design a comprehensive information security risk management tool*. *International Journal of Applied Information Systems – IJAIS*, Foundation of Computer Science FCS - Citeseer, New York, EUA, v. 7, n. 2, p. 10–15, 2014. ISSN 2249-0868.

GOMES, L. D.; GOULART JÚNIOR, C. R.; SIMEÃO, J. L. C.; SOUSA, T. d. J. R. de; SANTANA, A. C. Best Practices in Governance of Information and Tecnology Management. In: *13th International Conference on Information Systems & Technology Management - CONTECSI*. [s.n.], 2016. p. 837–857. ISBN 978-8599693124.

GREENBERG, A. et al. VL2: *A Scalable and Flexible Data center Network*. ACM SIGCOMM Conference on Data Communication, p. 51–62, 2009.

HOLIK, F. et al. *Methods of Deploying Security Standards in a Business Environment*. Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA, p. 411–414, 2015.

IBGE. *Estatísticas do cadastro central de empresas: 2016*. Rio de Janeiro - RJ, Brasil: Instituto Brasileiro de Geografia e Estatística - IBGE, 2018. 101 p. Coordenação de Metodologia das Estatísticas de Empresas, Cadastros e Classificações. ISBN 978-85-240-4461-8.

ISACA. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows - IL, EUA: ISACA - Information Systems Audit and Control Association, 2012a. 98 p.

ISACA. *COBIT 5 for Information Security*. Rolling Meadows - IL, EUA: ISACA - Information Systems Audit and Control Association, 2012b.

ITGI. *COBIT 4.1: Framework, Control Objectives, Management Guidelines and Maturity Model*. Rolling Meadows - IL, EUA: ITGI - IT Governance Institute, 2007. 2012 p.

JAYASWAL, K. *Administering Data centers: Servers, Storage, and Voice over IP*. 2006.

JANKE, N. *Pesquisa-ação-participativa: compartilhando conhecimentos*. 2005. 128f. Dissertação (Mestrado em Educação para Ciências) – Universidade Estadual Paulista, Faculdade de Ciências, Bauru, 2005.

JOIA, L.; NETO, *A. Government-to-government enterprises in brazil: Key success factors drawn from two case studies*. In: *17ª Bled eCommerce Conference eGlobal (BLED 2004)*. [S.l.: s.n.], 2004. p. 1–13.

KERZNER, H. *Gestão de Projetos: As Melhores Práticas*. 3. ed. [S.l.]: Bookman Editora (edição digital), 2017. 796 p.

KITCHENHAM, B. et al. *Systematic literature reviews in software engineering-A tertiary study*. Information and Software Technology, v. 52, n. 8, p. 792–805, 2010.

KRÁTKÝ, R. et al. Red Hat Enterprise Linux 6.8 Security Guide. 2016.

KONZEN, M. P. *Gestão de Riscos de Segurança da Informação Baseada na Norma ISO/IEC 27005 Usando Padrões de Segurança*. 119 p. Dissertação (Mestrado em Engenharia de Produção) - Centro de Tecnologia, Universidade Federal de Santa Maria, Santa Maria – RS, Brasil, 2013.

LANDWEHR, C. E. *Computer security. International Journal of Information Security*, Springer, v. 1, n. 1, p. 3–13, 2001.

LAUDON, K. C.; LAUDON, J. P. *Sistemas de informacao gerenciais*. São Paulo: Pearson Prentice Hall, 2007.

LAUREANO, M. A. P.; MORAES, P. E. S. *Segurança como estratégia de gestão da informação*. *Revista Economia & Tecnologia*, v. 8, n. 3, p. 38–44, 2005.

LESSING, M. M. *Best practices show the way to information security maturity*. In: *6th National Conference on Process Establishment, Assessment and Improvement in Information Technology - ImproveIT*. [S.l.: s.n.], 2008. p. 1–9.

LEAL, L. Q. (2008). *Maturidade em gerenciamento de projetos: uma visão analítica*. Engenharia de Software Magazine, n. 8. edição especial. Dez. 2008

LI, Y. *Network-Aware Job Placement in Datacenter Environments*. Department of Computer Science - University of Calbary, 2014.

LIMA, M. V. d. M. *Uma metodologia para avaliar a maturidade das configurações de segurança em ambientes de data center: uma estrutura sistemática com multiperspectiva*. 134 p. Dissertação - (Mestrado em Ciência da Computação) Centro de Informática, Universidade Federal de Pernambuco, Recife - PE, Brasil, 2017.

MADAN, S.; MADAN, S. *Security standards perspective to fortify web database applications from code injection attacks*. ISMS 2010 - UKSim/AMSS 1st International Conference on Intelligent Systems, Modelling and Simulation, p. 226–230, 2010.

MARCIANO, J. L.; LIMA-MARQUES, M. *O enfoque social da segurança da informação*. *Ciência da Informação*, v. 35, n. 3, p. 89–98, 2006. ISSN 0100-1965.

MAYER, J.; FAGUNDES, L. L. Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação. In: *VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSEG*. São Leopoldo - RS, Brasil: [s.n.], 2008. p. 347–356.

MENDONÇA, M. C. S. *A Percepção Gerencial sobre o Modelo de Gestão da Segurança da Informação de uma Empresa Pública de TIC: Perspectiva de Evolução para um Modelo de Governança*. 171 p. Dissertação (Mestrado em Gestão do Conhecimento e da Tecnologia da Informação) - Pró-Reitoria de Pós-Graduação Stricto Sensu em Gestão do Conhecimento e da Tecnologia da Informação, Universidade Católica de Brasília, Brasília - DF, Brasil, 2007.

MUTHUKRISHNAN, S. M.; PALANIAPPAN, S. *Security metrics maturity model for operational security*. ISCAIE 2016 - 2016 IEEE Symposium on Computer Applications and Industrial Electronics, p. 60–126, 2016.

NOBRE, A. C. d. S. *Fatores que Influenciam a Aceitação de Práticas Avançadas de Gestão de Segurança da Informação: Um Estudo com Gestores Públicos Estaduais no Brasil*. 171 p. Dissertação (Mestrado em Administração) - Universidade Federal do Rio Grande do Norte, Natal - RN, Brasil, 2009.

NERY JÚNIOR, E. d. J.; MOURA, H. P.; TEXEIRA FILHO, J. G. A. *Modelos de Maturidade em Gerenciamento de Projetos: Fatores Influenciadores para uma Melhor Escolha*. Curitiba - PR, Brasil: Editora Appris, 2018. 129 p. ISBN 978-85-473-0893-3.

NIEKERK, V. B.; JACOBS, P. *Toward a Secure Data center Mode*l. ISACA Journal, v. 3, n. 1, p. 1–10, 2015.

NIST. NIST SP 800-53A, R4: *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*. NIST Special Publication 800-53A, Revision 4, n. December 2014, p. 1–487, 2014b.

ONO, M. Y; *Indicadores de desempenho em Data center*. 67 p. Monografia (MBA em Gerenciamento de Facilidades) – Universidade de São Paulo. São Paulo- SP, Brasil, 2014.

SHIEH, A. et al. *Sharing the Data center Network*. Nsdi, 2011.

STAMBUL, M. A. M.; RAZALI, R. *An assessment model of information security implementation levels*. In: IEEE. *International Conference on Electrical Engineering and Informatics (ICEEI)*. Bandung, Indonesia, 2011. p. 1–6.

SOUZA, R.; VOSS, C. *Quality Management: Universal or Context Dependent? Production and Operations Management*, v. 10, n. 4, p. 383-404, 2001.

PALMA, F. *As normas da família ISO 27000 - Gestão da Segurança da Informação*. 2016. Acesso em: 30 jan. 2019. Disponível em <http://www.portalgsti.com.br/2013/12/ISO-27000.html>.

PELTIER, Thomas R., *Information security risk analysis*. Boca Raton: Auerbach Publications, 2001.

PFLEEGER, C. P.; PFLEEGER, S. L.; MARGULIES, J. *Security in Computing*. 5ª. ed.Upper Saddle River - NJ, Brasil: Editora Prentice Hall (Edição Digital), 2015.

PINHEIRO, P. P.; SLEIMAN, C. M. *Tudo o que você precisa saber sobre direito digital no dia-a-dia*. São Paulo: Saraiva, 2009. 58p.

PRADO, D. *A Importância da Evolução da Maturidade em Gerenciamento de Projetos*. 2018. Acesso em: 07 jun. 2018. Disponível em: <http://www.maturityresearch.com/novosite/biblio/importancia-da-evolucao.pdf>.

PRADO, E. P. V.; MANCINI, M.; BARATA, A. M.; SUN, V. IT Governance in HEALTHCARE INDUSTRY ORGANIZATIONS : *A Case Study of COBIT Implementation*. In: *XII Brazilian Symposium on Information Systems*. Florianópolis - SC: [s.n.], 2016. p. 1–8.

PRADO, D.; OLIVEIRA, W. *Maturidade em Gerenciamento de Projetos - Brasil. Relatório Pesquisa 2017: Relatório Geral - Parte A: Indicadores*. 2018. Acesso em: 07 Dez. 2018. Disponível em:<http://www.maturityresearch.com/novosite/2017/download/RelatorioMaturidade2017-Global-Parte-A-Indicadores-V2.pdf>.

PRASAD, T. K.; SHETH, A. P. *Semantics-Empowered Approaches to Data center Processing for Physical-Cyber-Social Applications* p. 68–75. Presented at the 2013 AAAI Fall Symposium Series.

PROENÇA, D.; BORBINHA, J. *Information security management systems - a maturity model based on* ISO/IEC 27001. In: ABRAMOWICZ, W.; PASCHKE, A. (Ed.). *International Conference on Business Information Systems*. [S.l.], 2018. p. 102–114. ISBN 978-3-319-93931-5.

RAMOS, A. *Security Officer - 1: guia oficial para formação de gestores em segurança da informação*. Porto Alegre: Zouk, 2006. 460p. Módulo Security Solutions.

RAMOS, I. Q. *Contribuição da Ciência da Informação para Criação de um Plano deSegurança da Informação*. 117 p. Dissertação (Mestrado em Ciência da Informação) -Centro de Ciências Sociais Aplicadas, Pontifícia Universidade Católica de Campinas, Campinas - SP, Brasil, 2007.

RELEASE, P. *Cisco cybersecurity report: csos reveal true cost of Breaches*. Disponível em: <http://www.datacenterjournal.com/cisco-cybersecurity-reportcsos-reveal-true-cost-breaches/>.

REA-GUAMAN, Á. M.; SÁNCHEZ-GARCÍA, I. D.; SAN FELIU, T.; CALVOMANZANO, J. A. *Modelos de madurez en ciberseguridad: una revisión sistemática*. In: *12th Iberian Conference on Information Systems and Technologies*. Lisboa, Portugal: [s.n.], 2017. p. 284–289. Disponível em: <http://oa.upm.es/48746/>.

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

SALEH, M. F. *Information security maturity model*. *International Journal of Computer Science and Security (IJCSS)*, Citeseer, v. 5, n. 3, p. 316–337, 2011b.

SCARFONE, K.; JANSEN, W.; TRACY, M. *Guide to General Server Security Recommendations of the National Institute of Standards and Technology*. Special Publication 800-123, 2008.

SHIREY, R. *RFC 4949 – Internet Security Glossary, Version 2. The Internet Society*. 2007. Acesso em: 07 set. 2018. Disponível em: <http://www.ietf.org/rfc/rfc4949.txt>.

SILVA NETO, G. M.; ALENCAR, G. D.; QUEIROZ, A. A. L. *Proposta de Modelo de Segurança Simplificado para Pequenas e Médias Empresas*. In: *XI Brazillian Symposium on Information Systems - SBSI*. [S.l.: s.n.], 2015. p. 299–306.

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, oct 2017. ISSN 1548-0992 Disponível em: <http://ieeexplore.ieee.org/document/8071246/>.

SÊMOLA, M. *Gestão da Segurança da Informação: Uma visão executiva*. 2ª. ed. Rio de Janeiro - RJ, Brasil: Editora Elsevier Academic (Edição Digital), 2013. 172 p. ISBN 9788535271782.

THIOLLENT, M. *Metodologia da pesquisa-ação.* 10 ed. São Paulo: Cortez: Autores Associados, 2000.

THE OPEN GROUP. *Open Information Security Management Maturity Model (O-ISM3).* Zaltbommel, Holanda: Editora Van Haren Publishing, 2011. 152 p.

THE OPEN GROUP. *Open Information Security Management Maturity Model (O ISM3), Version 2.0*. Berkshire, Inglaterra: Editora Van Haren Publishing, 2017. 130 p.

TIPTON, H. F.; NOZAKI, M. K. *Information Security Management Handbook*. Boca Raton - FL, EUA: Auerbach Publications, 2016. Volume 6. ISBN 978-1138199750.

VASCONCELLOS, H.S.R. *A pesquisa-ação em projetos de educação ambiental*. In: PEDRINI, A.G.(org.) Educação ambiental*:* reflexões e práticas contemporâneas. Rio de Janeiro: Vozes, 1997. 3ª ed.

ZHANG, J. *A model of human factors that affect organizational information security effectiveness*. Mississippi, USA:University of Mississippi, 2006.

ZAPATER, M.; SUZUKI, R. *Segurança da Informação – Um diferencial na competitividade das corporações*. *Promon Businnes & Technology Review*. Rio de Janeiro, 2005.

APÊNDICE A – Formulário de Pesquisa:

Classificação entre os Controles ISO/IEC 27001 e 27002 utilizados na estratégia Primasia para analise em *Data center*

Formulário de Pesquisa:
Classificação entre os Controles ISO/IEC 27001 e 27002 utilizados na estratégia Primasia para analise em *Data center* – Versão 1

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o seu nome, da empresa ou indícios que os caracterizem diretamente.

INTRODUÇÃO

Regras e Recomendações Gerais:
Com base na análise deste pesquisador foram apontados 114 controles, utilizados na estratégia Primasia o quais sendo classificados para uma melhor analise de maturidade aplicados a segurança de informação em *data center*.

No que tange os controles da ISO/IEC 27001 e 27002, exposto abaixo, marque, (DIR) - "Diretamente Relacionado ", quando o controle aplicado estiver totalmente relacionado ao contexto de segurança da informação associado aos servidores no ambiente de *data center.* Marque (PAR) - "Parcialmente Relacionado" quando existir algum contexto que ponha em risco a segurança da informação dentro do ambiente de *data center* ou marque (POR) - "Pouco Relacionado" quando não afetarem diretamente a segurança da informação em ambiente de *data center*.

1.(5.1.1) Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

2.(5.1.2) Convém que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

3. (6.1.1) Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

4.(6.1.2) Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.
(o solicitante e o aprovador são pessoas distintas)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

5.(6.1.3) Convém que contatos apropriados com autoridades relevantes sejam mantidos.
(fiscais, polícia, bombeiros...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

6.(6.1.4) Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

7.(6.1.5) Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

8.(6.2.1) Convém que uma política e medidas que apoiam a segurança da informação seja adotada para gerenciar os riscos decorrentes do uso de dispositivos móveis.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

9.(6.2.2) Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

10.(7.1.1) Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

11.(7.1.2) Convém que as obrigações contratuais com funcionários e partes externas, declarem as suas responsabilidades e a da organização para a segurança da informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

12.(7.2.1) Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

13.(7.2.2) Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

14.(7.2.3) Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

15.(7.3.1) Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação, sejam definidas, comunicadas aos funcionários ou partes externas e sejam cumpridas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

16.(8.1.1) Convém que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

17.(8.1.2) Convém que os ativos mantidos no inventário tenham um proprietário.
(Notebooks, PC's, Roteadores...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

18.(8.1.3) Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação, sejam identificadas, documentadas e implementadas. (Notebooks, PC's, Roteadores...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

19.(8.1.4) Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.
(Notebooks, PC's, Roteadores...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

20.(8.2.1) Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.
(Notebooks, PC's, Roteadores...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

21.(8.2.2) Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

22.(8.2.3) Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotada pela organização.
(informação confidencial, restrita ou pública...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado
23.(8.3.1) Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.
(Modens, Roteadores, Switchs...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

24.(8.3.2) Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

25.(8.3.3) Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

26.(9.1.1) Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

27.(9.1.2) Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

28.(9.2.1) Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição de direitos de acesso.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

29.(9.2.2) Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

30.(9.2.3) Convém que a concessão e uso de direitos de acesso privilegiado sejam restritos e controlados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

31.(9.2.4) Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

32.(9.2.5) Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

33.(9.2.6) Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

34.(9.3.1) Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

35.(9.4.1) Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

36.(9.4.2) Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (log-on).
(incluindo autoridades e lideranças...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

37.(9.4.3) Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

38.(9.4.4) Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações sejam restrito e estritamente controlado.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

39.(9.4.5) Convém que o acesso ao código-fonte de programa seja restrito.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

40.(10.1.1) Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

41.(10.1.2) Convém que uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas, seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

42.(11.1.1) Convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

43.(11.1.2) Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

44.(11.1.3) Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

45.(11.1.4) Convém que sejam projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

46.(11.1.5) Convém que seja projetado e aplicado procedimentos para o trabalho em áreas seguras.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

47.(11.1.6) Convém que pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

48.(11.2.1) Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

49.(11.2.2) Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

50.(11.2.3) Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos.
(ambientes protegidos de raios, inundações...)
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

51.(11.2.4) Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

52.(11.2.5) Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

53.(11.2.6) Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

54.(11.2.7) Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança, antes do descarte ou do seu uso.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

55.(11.2.8) Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

56.(11.2.9) Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

57.(12.1.1) Convém que os procedimentos de operação sejam documentados e disponibilizados a todos os usuários que necessitem deles.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

58.(12.1.2) Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

59.(12.1.3) Convém que a utilização dos recursos seja monitorada e ajustada e as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

60.(12.1.4) Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

61.(12.2.1) Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

62.(12.3.1) Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

63.(12.4.1) Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

64.(12.4.2) Convém que as informações dos registros de eventos (log) e seus recursos sejam protegidas contra acesso não autorizado e adulteração.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

65.(12.4.3) Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

66.(12.4.4) Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

67.(12.5.1) Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

68.(12.6.1) Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

69.(12.6.2) Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

70.(12.7.1) Convém que os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

71.(13.1.1) Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

72.(13.1.2) Convém que mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

73.(13.1.3) Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

74.(13.2.1) Convém que políticas, procedimentos e controles de transferências formais, sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

75.(13.2.2) Convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e partes externas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

76.(13.2.3) Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

77.(13.2.4) Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

78.(14.1.1) Convém que os requisitos relacionados com segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

79.(14.1.2) Convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

80.(14.1.3) Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

81.(14.2.1) Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

82.(14.2.2) Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

83.(14.2.3) Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

84.(14.2.4) Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

85.(14.2.5) Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

86.(14.2.6) Convém que as organizações estabeleçam e protejam adequadamente ambientes de desenvolvimento seguros para os esforços de desenvolvimento e integração de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

87.(14.2.7) Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

88.(14.2.8) Convém que os testes de funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

89.(14.2.9) Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

90.(14.3.1) Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

91.(15.1.1) Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

92.(15.1.2) Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar, ou prover componentes de infraestrutura de TI para as informações da organização.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

93.(15.1.3) Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

94.(15.2.1) Convém que a organização monitore, analise criticamente e audite a intervalos regulares, a entrega dos serviços executados pelos fornecedores.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

95.(15.2.2) Convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação de riscos.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

96.(16.1.1) Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

97.(16.1.2) Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

98.(16.1.3) Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização, sejam instruídos a registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

99.(16.1.4) Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

100.(16.1.5) Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

101.(16.1.6) Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

102.(16.1.7) Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

103.(17.1.1) Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

104.(17.1.2) Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

105.(17.1.3) Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

106.(17.2.1) Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

107.(18.1.1) Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

108.(18.1.2) Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

109.(18.1.3) Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

110.(18.1.4) Convém que a privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

111.(18.1.5) Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

112.(18.2.1) Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

113.(18.2.2) Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

114.(18.2.3) Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.
[ ] DIR - Diretamente Relacionado [ ] PAR- Parcialmente Relacionado [ ] POR - Pouco Relacionado

APÊNDICE B – Classificação de Controles por Especialistas:

Classificação entre os Controles ISO/IEC 27001 e 27002 utilizados na estratégia Primasia para analise em *Data center*.

Controle	Especialista1	Especialista2	Especialista3	Especialista4	Especialista5	Nota Final
5.1.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
5.1.2	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
6.1.1	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	13
6.1.2	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	13
6.1.3	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(x)	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	9
6.1.4	DIR( )PAR(X) POR( )	DIR( )PAR(x) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	9
6.1.5	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	12
6.2.1	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	11
6.2.2	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
7.1.1	DIR(X)PAR( ) POR( )	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	12
7.1.2	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	14
7.2.1	DIR(X)PAR( ) POR( )	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
7.2.2	DIR(X)PAR( ) POR( )	DIR( )PAR(x) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	11
7.2.3	DIR(X)PAR( ) POR( )	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	12
7.3.1	DIR(X)PAR( ) POR( )	DIR( )PAR(x) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	11
8.1.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	12

8.1.2	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	8
8.1.3	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
8.1.4	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	8
8.2.1	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	11
8.2.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	13
8.2.3	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
8.3.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
8.3.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
8.3.3	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
9.1.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
9.1.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
9.2.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
9.2.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
9.2.3	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
9.2.4	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
9.2.5	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
9.2.6	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
9.3.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	12
9.4.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
9.4.2	DIR(X)PAR( )	DIR(X)PAR( )	DIR(X)PAR( )	DIR(X)PAR( )	DIR(X)PAR( )	15

	POR( )	POR( )	POR( )	POR( )	POR( )	
9.4.3	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
9.4.4	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
9.4.5	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	11
10.1.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
10.1.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
11.1.1	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
11.1.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
11.1.3	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	13
11.1.4	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
11.1.5	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	13
11.1.6	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
11.2.1	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	13
11.2.2	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
11.2.3	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
11.2.4	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
11.2.5	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	11
11.2.6	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	13
11.2.7	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
11.2.8	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	10
11.2.9	DIR( )PAR( )	DIR( )PAR( )	DIR( )PAR( )	DIR( )PAR( )	DIR( )PAR( )	5

	POR(X)	POR(X)	POR(X)	POR(X)	POR(X)	
12.1.1	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	10
12.1.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	13
12.1.3	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
12.1.4	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
12.2.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
12.3.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
12.4.1	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
12.4.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	14
12.4.3	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
12.4.4	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	13
12.5.1	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
12.6.1	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	13
12.6.2	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	12
12.7.1	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
13.1.1	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
13.1.2	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	14
13.1.3	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	13
13.2.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
13.2.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	15
13.2.3	DIR(X)PAR( )	DIR(X)PAR( )	DIR( )PAR(X)	DIR( )PAR(X)	DIR( )PAR(X)	12

	POR( )	POR( )	POR( )	POR( )	POR( )	
13.2.4	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	11
14.1.1	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	12
14.1.2	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	11
14.1.3	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	13
14.2.1	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	10
14.2.2	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	9
14.2.3	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
14.2.4	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	11
14.2.5	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	11
14.2.6	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	10
14.2.7	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	9
14.2.8	DIR(x)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	10
14.2.9	DIR(x)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	8
14.3.1	DIR(x)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	9
15.1.1	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	12
15.1.2	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
15.1.3	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	9
15.2.1	DIR(x)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	9
15.2.2	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	12
16.1.1	DIR(x)PAR( )	DIR(X)PAR( )	DIR( )PAR(X)	DIR( )PAR(X)	DIR( )PAR(X)	12

	POR( )	POR( )	POR( )	POR( )	POR( )	
16.1.2	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	12
16.1.3	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	12
16.1.4	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	10
16.1.5	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	9
16.1.6	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	11
16.1.7	DIR(x)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR( ) POR(X)	10
17.1.1	DIR(x)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	12
17.1.2	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	DIR( )PAR(X) POR( )	11
17.1.3	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	12
17.2.1	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	DIR(X)PAR( ) POR( )	14
18.1.1	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	10
18.1.2	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	10
18.1.3	DIR( )PAR( ) POR(x)	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	11
18.1.4	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	11
18.1.5	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	12
18.2.1	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	11
18.2.2	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR( ) POR(X)	11
18.2.3	DIR( )PAR(x) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	DIR(X)PAR( ) POR( )	DIR( )PAR(X) POR( )	12

ANEXO A – Formulário de Pesquisa: Dados dos Especialistas

O questionário é o mesmo utilizado e avaliado por Alencar (2019).

Dados do Especialista

O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o seu nome, da empresa ou indícios que os caracterizem diretamente. Para uma padronização das respostas, solicitamos que todos os tempos sejam inseridos em anos. Bem como informamos que tudo que o questionário trata como Segurança, deve ser entendido como Segurança da Informação.

DADOS DO ESPECIALISTA

Cargo: _____

Tempo no Cargo (anos): _____

Maior cargo assumido na área de segurança ou correlata: _____

Tempo no Cargo: _____

Tempo de experiência profissional com TIC: _____

Deste tempo, quanto foi com Segurança: _____

Maior titulação: ( ) Especialização ( ) Mestrado ( )Doutorado.

Titulação em Andamento: ( ) Mestrando ( ) Doutorando

Alguma titulação foi em segurança (curso ou trabalho de conclusão)? ( ) Sim ( ) Não.

Em caso positivo, qual(is): ( ) Especialização ( ) Mestrado ( ) Doutorado.

Área da titulação em segurança: _____

Tem experiência com Maturidade? ( ) Sim ( ) Não.

Quantidade de Publicações Acadêmicas: ( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7

Quantidade destas publicações acadêmicas que são em Segurança:

( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7

Certificações na área de TIC: ( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7

Quantidade destas certificações são na área de Segurança:

( ) 0 ( ) 1-3 ( ) 4-7 ( ) Mais que 7

Tem experiência de ensino na área de TIC? ( ) Sim ( ) Não.

Em caso positivo,

Tipo: ( )Palestrante ( )Professor ( )Coordenador ( )Outros:_____

Nível: ( )Graduação ( )Especialização ( )Mestrado/Doutorado ( )Cursos/Palestras na área Profissional ( ) Outros: _____

Tempo de Experiência com ensino: _____

Alguma destas experiências de ensino é na área de Segurança? ( ) Sim ( ) Não.

Em caso positivo:

Tipo: ( )Palestrante ( )Professor ( )Coordenador ( )Outros: _____

Nível: ( )Graduação ( )Especialização ( )Mestrado/Doutorado ( )Cursos/Palestras na área Profissional ( ) Outros: _____

Tempo de Experiência com ensino em Segurança: _____

O senhor(a) tem interesse em receber informações sobre o resultado final desta pesquisa?

( ) Sim ( ) Não. Em caso positivo, e-mail: _____

ANEXO B – Formulário de Pesquisa: Controles ISO/IEC 27001 e 27002

O questionário é o mesmo utilizado e avaliado por Alencar (2019).

Formulário de Pesquisa: Controles ISO/IEC 27001 e 27002
O preenchimento do formulário tem como fins a pesquisa acadêmica. Desse modo, os dados aqui obtidos serão tratados de forma estatística e não será, em nenhum momento, mencionado o nome da empresa ou indícios que a caracterize diretamente.

CONTROLES ISO/IEC 27001 E 27002 UTILIZADOS NA ESTRATÉGIA PRIMASIA

No que tange os controles da ISO/IEC 27001 e 27002, exposto abaixo, marque, de 1 a 5, o quão importante ele é para o ambiente de sua empresa:

Onde: 1significa nenhuma importância, 3 como neutro e 5 para muito importante.
Obs.: As informações contidas entre parênteses e em itálico no final de alguns controles, por exemplo, no número 4, são apenas exemplos inserido pelo autor para um melhor entendimento do controle, não fazendo parte, originalmente, do mesmo.

1.(5.1.1) Convém que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

2.(5.1.2) Convém que as políticas para a segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

3. (6.1.1) Convém que todas as responsabilidades pela segurança da informação sejam definidas e atribuídas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

4.(6.1.2) Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.
(o solicitante e o aprovador são pessoas distintas)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

5.(6.1.3) Convém que contatos apropriados com autoridades relevantes sejam mantidos.
(fiscais, polícia, bombeiros...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

6.(6.1.4) Convém que contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em segurança da informação sejam mantidos.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

7.(6.1.5) Convém que a segurança da informação seja considerada no gerenciamento de projetos, independentemente do tipo do projeto.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

8.(6.2.1) Convém que uma política e medidas que apoiam a segurança da informação seja adotada para gerenciar os riscos decorrentes do uso de dispositivos móveis.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

9.(6.2.2) Convém que uma política e medidas que apoiam a segurança da informação sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

10.(7.1.1) Convém que verificações do histórico sejam realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e seja proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

11.(7.1.2) Convém que as obrigações contratuais com funcionários e partes externas, declarem as suas responsabilidades e a da organização para a segurança da informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

12.(7.2.1) Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

13.(7.2.2) Convém que todos os funcionários da organização e, onde pertinente, partes externas devem recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

14.(7.2.3) Convém que exista um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

15.(7.3.1) Convém que as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação, sejam definidas, comunicadas aos funcionários ou partes externas e sejam cumpridas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

16.(8.1.1) Convém que os ativos associados com informação e com os recursos de processamento da informação sejam identificados e um inventário destes ativos seja estruturado e mantido.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

17.(8.1.2) Convém que os ativos mantidos no inventário tenham um proprietário.
(Notebooks, PC's, Roteadores...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

18.(8.1.3) Convém que regras para o uso aceitável das informações, dos ativos associados com a informação e dos recursos de processamento da informação, sejam identificadas, documentadas e implementadas. (Notebooks, PC's, Roteadores...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

19.(8.1.4) Convém que todos os funcionários e partes externas devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo.
(Notebooks, PC's, Roteadores...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

20.(8.2.1) Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada.
(Notebooks, PC's, Roteadores...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

21.(8.2.2) Convém que um conjunto apropriado de procedimentos para rotular e tratar a informação seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado pela organização.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

22.(8.2.3) Convém que procedimentos para o tratamento dos ativos sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotada pela organização.
(informação confidencial, restrita ou pública...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

23.(8.3.1) Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis, de acordo com o esquema de classificação adotado pela organização.
(Modens, Roteadores, Switchs...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

24.(8.3.2) Convém que as mídias sejam descartadas de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

25.(8.3.3) Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou corrupção, durante o transporte.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

26.(9.1.1) Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

27.(9.1.2) Convém que os usuários somente recebam acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

28.(9.2.1) Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição de direitos de acesso.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

29.(9.2.2) Convém que um processo formal de provisionamento de acesso do usuário seja implementado para conceder ou revogar os direitos de acesso do usuário para todos os tipos de usuários em todos os tipos de sistemas e serviços.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

30.(9.2.3) Convém que a concessão e uso de direitos de acesso privilegiado sejam restritos e controlados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

31.(9.2.4) Convém que a concessão de informação de autenticação secreta seja controlada por meio de um processo de gerenciamento formal.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

32.(9.2.5) Convém que os proprietários de ativos analisem criticamente os direitos de acesso dos usuários, a intervalos regulares.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

33.(9.2.6) Convém que os direitos de acesso de todos os funcionários e partes externas às informações e aos recursos de processamento da informação sejam retirados logo após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

34.(9.3.1) Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

35.(9.4.1) Convém que o acesso à informação e às funções dos sistemas de aplicações seja restrito, de acordo com a política de controle de acesso.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

36.(9.4.2) Convém que, onde aplicável pela política de controle de acesso, o acesso aos sistemas e aplicações sejam controlados por um procedimento seguro de entrada no sistema (log-on).
(incluindo autoridades e lideranças...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

37.(9.4.3) Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

38.(9.4.4) Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações sejam restrito e estritamente controlado.
APÊNDICE C. Formulário de Pesquisa: Controles ISO/IEC 27001 e 27002 215
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

39.(9.4.5) Convém que o acesso ao código-fonte de programa seja restrito.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

40.(10.1.1) Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

41.(10.1.2) Convém que uma política sobre o uso, proteção e ciclo de vida das chaves criptográficas, seja desenvolvida e implementada ao longo de todo o seu ciclo de vida.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

42.(11.1.1) Convém que perímetros de segurança sejam definidos e usados para proteger tanto as áreas que contenham as instalações de processamento da informação como as informações críticas ou sensíveis.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

43.(11.1.2) Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

44.(11.1.3) Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

45.(11.1.4) Convém que sejam projetadas e aplicadas proteção física contra desastres naturais, ataques maliciosos ou acidentes.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

46.(11.1.5) Convém que seja projetado e aplicado procedimentos para o trabalho em áreas seguras.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

47.(11.1.6) Convém que pontos de acesso, tais como áreas de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controlados e, se possível, isolados das instalações de processamento da informação, para evitar o acesso não autorizado.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

48.(11.2.1) Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio-ambiente, bem como as oportunidades de acesso não autorizado.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

49.(11.2.2) Convém que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

50.(11.2.3) Convém que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos.
(ambientes protegidos de raios, inundações...)
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

51.(11.2.4) Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

52.(11.2.5) Convém que equipamentos, informações ou software não sejam retirados do local sem autorização prévia.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

53.(11.2.6) Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

54.(11.2.7) Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança, antes do descarte ou do seu uso.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

55.(11.2.8) Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

56.(11.2.9) Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

57.(12.1.1) Convém que os procedimentos de operação sejam documentados e disponibilizados a todos os usuários que necessitem deles.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

58.(12.1.2) Convém que mudanças na organização, nos processos do negócio, nos recursos de processamento da informação e nos sistemas que afetam a segurança da informação, sejam controladas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

59.(12.1.3) Convém que a utilização dos recursos seja monitorada e ajustada e as projeções sejam feitas para necessidades de capacidade futura para garantir o desempenho requerido do sistema.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

60.(12.1.4) Convém que ambientes de desenvolvimento, teste e produção sejam separados para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

61.(12.2.1) Convém que sejam implementados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, combinado com um adequado programa de conscientização do usuário.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

62.(12.3.1) Convém que cópias de segurança das informações, softwares e das imagens do sistema, sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

63.(12.4.1) Convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

64.(12.4.2) Convém que as informações dos registros de eventos (log) e seus recursos sejam protegidas contra acesso não autorizado e adulteração.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

65.(12.4.3) Convém que as atividades dos administradores e operadores do sistema sejam registradas e os registros (logs) protegidos e analisados criticamente, a intervalos regulares.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

66.(12.4.4) Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma única fonte de tempo precisa.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

67.(12.5.1) Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

68.(12.6.1) Convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso, sejam obtidas em tempo hábil, com a exposição da organização a estas vulnerabilidades avaliadas e tomadas as medidas apropriadas para lidar com os riscos associados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

69.(12.6.2) Convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

70.(12.7.1) Convém que os requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar interrupção dos processos do negócio.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

71.(13.1.1) Convém que as redes sejam gerenciadas e controladas para proteger as informações nos sistemas e aplicações.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

72.(13.1.2) Convém que mecanismos de segurança, níveis de serviço e requisitos de gerenciamento de todos os serviços de rede, sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente como para terceirizados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

73.(13.1.3) Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

74.(13.2.1) Convém que políticas, procedimentos e controles de transferências formais, sejam estabelecidos para proteger a transferência de informações, por meio do uso de todos os tipos de recursos de comunicação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

75.(13.2.2) Convém que sejam estabelecidos acordos para transferência segura de informações do negócio entre a organização e partes externas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

76.(13.2.3) Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

77.(13.2.4) Convém que os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados, analisados criticamente e documentados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

78.(14.1.1) Convém que os requisitos relacionados com segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

79.(14.1.2) Convém que as informações envolvidas nos serviços de aplicação que transitam sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

80.(14.1.3) Convém que informações envolvidas em transações nos aplicativos de serviços sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação da mensagem não autorizada.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

81.(14.2.1) Convém que regras para o desenvolvimento de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

82.(14.2.2) Convém que as mudanças em sistemas no ciclo de vida de desenvolvimento sejam controladas utilizando procedimentos formais de controle de mudanças.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

83.(14.2.3) Quando plataformas operacionais forem modificadas, convém que as aplicações críticas de negócio sejam analisadas criticamente e testadas para assegurar que não ocorreu nenhum impacto adverso nas operações da organização ou na segurança.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

84.(14.2.4) Convém que modificações em pacotes de software sejam desencorajadas e estejam limitadas às mudanças necessárias, e todas as mudanças sejam estritamente controladas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

85.(14.2.5) Convém que princípios para projetar sistemas seguros sejam estabelecidos, documentados, mantidos e aplicados para qualquer implementação de sistemas de informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

86.(14.2.6) Convém que as organizações estabeleçam e protejam adequadamente ambientes de desenvolvimento seguros para os esforços de desenvolvimento e integração de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistema.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

87.(14.2.7) Convém que a organização supervisione e monitore as atividades de desenvolvimento de sistemas terceirizado.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

88.(14.2.8) Convém que os testes de funcionalidades de segurança sejam realizados durante o desenvolvimento de sistemas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

89.(14.2.9) Convém que programas de testes de aceitação e critérios relacionados sejam estabelecidos para novos sistemas de informação, atualizações e novas versões.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

90.(14.3.1) Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

91.(15.1.1) Convém que os requisitos de segurança da informação para mitigar os riscos associados com o acesso dos fornecedores aos ativos da organização sejam acordados com o fornecedor e documentados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

92.(15.1.2) Convém que todos os requisitos de segurança da informação relevantes sejam estabelecidos e acordados com cada fornecedor que possa acessar, processar, armazenar, comunicar, ou prover componentes de infraestrutura de TI para as informações da organização.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

93.(15.1.3) Convém que acordos com fornecedores incluam requisitos para contemplar os riscos de segurança da informação associados com a cadeia de suprimento de produtos e serviços de tecnologia das comunicações e informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

94.(15.2.1) Convém que a organização monitore, analise criticamente e audite a intervalos regulares, a entrega dos serviços executados pelos fornecedores.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

95.(15.2.2) Convém que mudanças no provisionamento dos serviços pelos fornecedores, incluindo manutenção e melhoria das políticas de segurança da informação, dos procedimentos e controles existentes, sejam gerenciadas, levando-se em conta a criticidade das informações do negócio, dos sistemas e processos envolvidos, e a reavaliação de riscos.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

96.(16.1.1) Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

97.(16.1.2) Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

98.(16.1.3) Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização, sejam instruídos a registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou observada, nos sistemas ou serviços.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

99.(16.1.4) Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

100.(16.1.5) Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

101.(16.1.6) Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

102.(16.1.7) Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, as quais podem servir como evidências.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

103.(17.1.1) Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

104.(17.1.2) Convém que a organização estabeleça, documente, implemente e mantenha processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

105.(17.1.3) Convém que a organização verifique os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

106.(17.2.1) Convém que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

107.(18.1.1) Convém que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente identificados, documentados e mantidos atualizados para cada sistema de informação da organização.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

108.(18.1.2) Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de software proprietários.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

109.(18.1.3) Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

110.(18.1.4) Convém que a privacidade e proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação e regulamentação pertinente, quando aplicável.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

111.(18.1.5) Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

112.(18.2.1) Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivo dos controles, políticas, processos e procedimentos para a segurança da informação) seja analisado criticamente, de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

113.(18.2.2) Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade dos procedimentos e do processamento da informação, dentro das suas áreas de responsabilidade, com as normas e políticas de segurança e quaisquer outros requisitos de segurança da informação.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]

114.(18.2.3) Convém que os sistemas de informação sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.
1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 [ ]