UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE COMPUTAÇÃO
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

JULIA DE MIRANDA BANDEIRA

AVALIAÇÃO DA APLICAÇÃO DA NORMA NBR ISO/IEC 27002:2013 E A CONFORMIDADE COM ITIL NO PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Niterói
2017

JULIA DE MIRANDA BANDEIRA

AVALIAÇÃO DA APLICAÇÃO DA NORMA NBR ISO/IEC 27002:2013 E A CONFORMIDADE COM ITIL NO PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação, como requisito parcial para conclusão do curso e obtenção do Título de Bacharel em Sistemas de Informação.

Orientadora:
Prof.ª Dr.ª Luciana Cardoso de Castro Salgado

Niterói
2017

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

B214 Bandeira, Julia de Miranda
Avaliação da aplicação da norma NBR ISO/IEC 27002:2013 e a conformidade com ITIL no processo de gestão de segurança da informação / Julia de Miranda Bandeira. – Niterói, RJ : [s.n.], 2017.
59 f.

Projeto Final (Bacharelado em Sistemas de Informação) – Universidade Federal Fluminense, 2017.
Orientador: Luciana Cardoso de Castro Salgado.

1. Segurança da informação. 2. Tecnologia da informação. 3. Gestão da informação. 4. ISSO IEC 27002. I. Título.

CDD 005.8

JULIA DE MIRANDA BANDEIRA

AVALIAÇÃO DA APLICAÇÃO DA NORMA NBR ISO/IEC 27002:2013 E A CONFORMIDADE COM ITIL NO PROCESSO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Trabalho de conclusão de curso apresentado ao curso de Bacharelado em Sistemas de Informação, como requisito parcial para conclusão do curso e obtenção do Título de Bacharel em Sistemas de Informação.

Aprovada em 13 de Julho de 2017.

BANCA EXAMINADORA

_____

Prof.ª Dr.ª Luciana Cardoso de Castro Salgado

_____

Prof. Dr. Leonardo Cruz da Costa

_____

Prof. Dr. Marcos Kalinowski

Niterói
2017

AGRADECIMENTOS

Aos meus pais, por terem me guiado e me fornecerem o suporte necessário por toda a minha graduação.

À minha orientadora Luciana Salgado, pelo estímulo e por me conduzir até a conclusão desta atividade com dicas que elevaram o nível do meu trabalho.

Aos meus professores da Universidade Federal Fluminense por todos os ensinamentos durante o curso.

“A persistência é o caminho do êxito”

Charles Chaplin

RESUMO

O presente trabalho visa avaliar o atual nível de maturidade no processo de Gerenciamento de Segurança da Informação das empresas estudadas, com base no conceito de melhores práticas de TI divulgadas na ITIL. O método consiste em avaliar as cinco dimensões do PMF (Visão e Orientação, Processos, Pessoas, Ferramentas e Cultura) por meio de uma série de questionamentos, resultando na qualificação da maturidade do processo ITIL em cinco níveis: Nível 1 – Inicial, Nível 2 – Repetitivo, Nível 3 – Definido, Nível 4 – Gerenciado e Nível 5 - Otimizado. A metodologia foi aplicada em duas empresas com público-alvo de 2 colaboradores responsáveis pelas áreas de segurança da informação e infraestrutura, das respectivas empresas. O trabalho apresenta a fundamentação teórica e os resultados observados em prática, no que diz respeito a mensuração da qualidade de execução do processo de gerenciamento de segurança da informação ITIL, gerando oportunidades de melhorias na forma de atuação das equipes de técnicas e possibilidades de geração de valor nos processos de gerenciamento de segurança da informação.

Palavras-chave: ITIL. PMF. Maturidade de Processos. Gerenciamento de Segurança da Informação.

ABSTRACT

The present work aims to evaluate the current maturity level in the Information Security Management process of the studied companies, based on the concept of IT best practices disclosed in ITIL. The method consists of evaluating the five dimensions of the PMF (Vision and Guidance, Processes, People, Tools and Culture) through a series of questions, resulting in the qualification of ITIL process maturity in five levels: Level 1 - Initial, Level 2 - Repetitive, Level 3 - Defined, Level 4 - Managed and Level 5 - Optimized. The methodology was applied in two companies with a target audience of two employees responsible for information security and infrastructure from the respective companies. The paper presents the theoretical basis and presentation of the results observed in practice, regarding the measurement of the execution quality for ITIL information security management process, generating opportunities for improvements in the way the technical teams act and consequently adding value in the information security management processes.

Keywords: ITIL. PMF. Process Maturity. Information Security Management.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BYOD	*Bring Your Own Device*
CCTA	*Central Computer and Telecommunications Agency*
CMMI	*Capability Maturity Model Integration*
CTO	*Chief Technology Officer*
GSI	Gerenciamento de Segurança da Informação
IEC	*International Electrotechnical Commission*
ISSO	*International Standards Organization*
ITIL	*Information Technology Infrastructure Library*
OGC	*Office of Governant Commerce*
PEMM	*Process and Enterprise Maturity Model*
PMF	*Process Maturity Framework*
PSI	Política de Segurança da Informação
SEI	*Software Engineering Institute*
SI	Segurança da Informação
TI	Tecnologia da Informação
ISO/IEC 27002	*Code of Practice for Information Security Management*

SUMÁRIO

1 INTRODUÇÃO

A área de Tecnologia da Informação (TI) tem se tornado, nas últimas décadas, estratégica para empresas públicas e privadas. Como consequência, está havendo uma transformação nos ambientes empresariais no que se trata de Segurança da Informação. Esse conceito tem necessitado de atenção diferenciada em diversas instituições, com a intenção de resguardar informações e atividades internas.

> No fim do segundo milênio da Era Cristã, vários acontecimentos de importância histórica transformaram o cenário social da vida humana. Uma revolução tecnológica concentrada nas tecnologias da informação começou a remodelar a base material da sociedade em ritmo acelerado. (Castells, 2007, p. 39).

A rapidez e a abrangência das informações trazem aos responsáveis pelo negócio preocupações, uma vez que mal utilizadas e desprotegidas podem prejudicar o patrimônio organizacional. Em um ambiente de empresas interligadas e competitivas, a informação torna-se um fator de risco e/ou sucesso para o negócio. Assim, uma má gestão ou inexistência das normas e políticas de Segurança da Informação resulta em vulnerabilidades para um ambiente corporativo.

Nesse contexto, temos a Segurança da Informação como um dos principais desafios para o alinhamento estratégico. Para Laureano (2005), “determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente”. Além disso, para o alcance das metas e redução de riscos, é necessária uma atuação eficiente e grau de maturidade elevado da TI interna.

> Diferentes organizações possuem distintos níveis de maturidade para a gestão de sua tecnologia. Departamentos de TI com níveis iniciais em maturidade costumam conduzir suas atividades de gestão da tecnologia com fins em si mesmos, e não como um meio para um atingir objetivos maiores. (Palmas, 2013).

Para Palmas (2013) a definição dos níveis de maturidade está relacionada à organização do departamento de TI, com formalização de documentos e procedimentos, além de integração com as tecnologias adotadas e alinhamento da TI com o negócio.

1.1 **Motivação**

A motivação para a realização desse trabalho se deu pela resistência ainda existente em algumas organizações de reconhecer a necessidade de uma gestão mais detalhada de Segurança da Informação (SI) e entender o valor estratégico desse tópico.

> Geralmente uma área de segurança da informação (SI) começa dentro da hierarquia de Tecnologia da informação, isso acontece porque os gestores relacionam SI com servidores e senhas, ou seja, controle de acesso em geral. Mas o grande desafio de um gestor de segurança é mostrar que essa não é a única tarefa e que existem situações onde controle de acesso não resolve o problema. (Albuquerque, 2009).

A partir desse cenário, houve o interesse em investigar os benefícios do enquadramento das empresas estudadas com normas e frameworks relacionados à SI. Foi utilizado como perspectiva para esse estudo de casos o framework *Information Technology Infrastructure Library* (ITIL), que consiste em um modelo de boas práticas para o gerenciamento dos serviços de TI adequando-se a qualquer cenário de TI, independente de tecnologias (Amaral, 2009), e a Norma ABNT NBR ISO/IEC 27002:2013, que auxilia na segurança da informação de acordo com requisitos de negócio, leis e regulamentações relevantes (Fontes, 2008).

1.2 **Objetivos**

O objetivo principal do estudo é a realização de uma investigação em empresas de pequeno e grande porte de diferentes setores, a fim de avaliar a maturidade dos processos de gestão de segurança da informação e os impactos causados às empresas pelo grau de maturidade apontados, levando em consideração o alinhamento estratégico com o negócio.

1.2.1 Objetivos específicos

Os objetivos específicos do trabalho são:

a) Desenvolver um critério de avaliação de maturidade ITIL, com base no *Process Maturity Framework* (PMF);

b) Desenvolver um questionário de avaliação de maturidade ITIL, usando o PMF como referência;
c) Mensurar o grau de atendimento aos princípios que determinam um bom gerenciamento de segurança da informação (GSI);
d) Apresentar os pontos de atenção, a partir dos resultados práticos das avaliações de maturidade do processo de GSI.

1.3 **Metodologia**

O trabalho utilizou como metodologia uma abordagem qualitativa e bibliográfica, segundo Marconi e Lakatos (1996), e possui caracterização exploratória quanto aos objetivos, com a realização de investigação mais profunda através de entrevistas.

São apresentados os conceitos de Governança em TI, Segurança da Informação: Princípios, Ameaça, Vulnerabilidade e Risco, Normas, Políticas de Segurança da Informação e os benefícios do ITIL associados à Segurança da Informação.

Foi adotado um estudo que busca analisar o cenário mais especificamente. O estudo foi realizado nas áreas de Infraestrutura e de Segurança da Informação de duas empresas, sendo uma de grande porte no setor de Petróleo e Gás e outra de pequeno porte no setor de Tecnologia da Informação (Rede Social). A coleta de dados foi realizada através de entrevistas com roteiros estruturados, aplicados aos gerentes da área de Infraestrutura/Segurança da Informação.

A pesquisa consiste em uma análise documental e revisão bibliográfica da Norma NBR ISO/IEC 27002:2013, do framework ITIL de boas práticas, e literatura relacionada, para a fundamentação do trabalho e apoio na realização do estudo de caso. Foram realizadas pesquisas na internet, leitura de livros, artigos, trabalhos e monografias com conteúdos relacionados às Normas de SI, Governança de TI e ITIL. Ademais, foram consultados especialistas em ITIL para a formatação do questionário aplicado às empresas e entendimento do modelo de avaliação de maturidade utilizado.

1.4 **Organização do Texto**

O trabalho está dividido em cinco capítulos. O primeiro capítulo trata da introdução ao tema, motivação para o estudo, objetivo da pesquisa e metodologia adotada.

O segundo capítulo evidencia o referencial teórico, salientando os principais conceitos de apoio à realização da pesquisa e explicação de normas relacionadas e processos de gestão utilizados, são vistos também os trabalhos relacionados à gestão de SI e maturidade de processos, formando uma base de informações úteis na construção do trabalho.

O terceiro capítulo descreve a estratégia de avaliação de maturidade definido, a composição do questionário, a atribuição das notas e seus critérios.

No quarto capítulo são apresentados os resultados do estudo de caso, onde é analisada a maturidade dos processos de gestão de SI para cada uma das empresas estudadas, seguindo o modelo determinado previamente, com base na aplicação da Norma NBR ISO/IEC 27002:2013 e do ITIL na organização.

Por fim, no quinto capítulo são apresentadas as considerações finais sobre o estudo, as limitações e os trabalhos futuros.

2 **REFERENCIAL TEÓRICO**

O capítulo 2 neste trabalho abrange a fundamentação teórica acerca dos conceitos de Segurança da Informação, dando ênfase para a área de Gestão de SI. O estudo adotado baseou-se na Norma ABNT NBR ISO/IEC 27002:2013(ABNT, 2013), ITIL(Colin; Vernon, 2010), Modelos de Política de Segurança da Informação e Maturidade de Processos.

2.1 **Princípios básicos da Segurança da Informação**

A segurança da informação consiste na garantia de que as informações, sejam elas em qualquer formato, estejam protegidas contra acesso de pessoas não autorizadas, a fim de preservar seu valor para a organização ou indivíduo. Seus principais pilares são: confidencialidade, disponibilidade e integridade, de acordo com o TCU (2007).

As informações recebem uma classificação de acordo com sua importância. Nem todas as informações são tidas como essenciais para uma organização, não sendo necessariamente consideradas formas de preservá-las (Laureano, 2005). Contudo, existem informações vitais para o sucesso de um negócio. Esses pontos serão revisados e explicados de forma detalhada nos tópicos subsequentes.

2.1.1 Informação e Segurança: conceitos gerais

A informação é um componente crucial para a comunicação, existem diversas definições, e as disponíveis nos dicionários conseguem descrever o que é informação de fato. Michaelis, conhecido dicionário da língua portuguesa, descreve informação como “ato ou efeito de informar -se; conjunto de conhecimentos acumulados sobre certo tema por meio de pesquisa ou instrução; explicação ou esclarecimento de um conhecimento, produto ou juízo; comunicação”.

Existe ainda certa dificuldade para a diferenciação entre os conceitos de “dado”, “informação” e “conhecimento”. Esses conceitos são essenciais para o desenvolvimento do trabalho, portanto, serão expostas visões de diferentes autores.

Para Davenport (1998), a informação é uma junção entre os dados e conhecimento, é essencial para ele que haja uma boa definição, por parte das organizações, acerca dos termos de

dado, informação e conhecimento, entendendo que o fracasso ou sucesso organizacional dependem da aplicação correta dos conceitos na solução de problemas. Já Shedroff (1999, p.272) elabora os termos informáticos a fim de garantir que o termo “entendimento” seja compreendido como um resultado do processamento da informação. Para ele, dado é “material bruto [...] para construir nossas comunicações”, nesse caso deve existir um processamento desse dado, a fim de que seja construído um significado. A sequência da estrutura apresentada por Shedroff (1999) está ilustrada na figura 1.

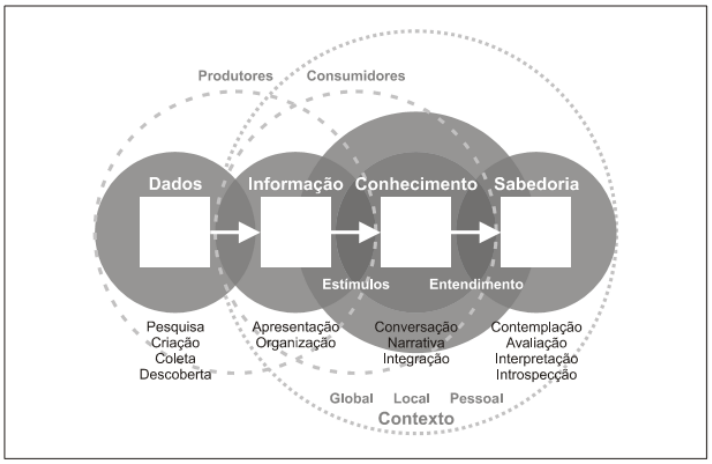

Figura 1– O Contínuo do Entendimento. Extraído de: Shedroff (1999, p.271).

Porém, a consideração que mais se aplica ao contexto não é exatamente a definição dos dicionários ou autores anteriormente citados, e sim a definição de acordo com a ABNT NBR ISO/IEC 27002:2013, que descreve a informação como um ativo valorizado.

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especificamente importante no ambiente dos negócios, cada vez mais interconectado. Como resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (ABNT, 2013, p. ix)

A definição do Dicionário Michaelis para segurança é descrita como “ato ou efeito de segurar; aquilo que protege de agentes exteriores; condição ou estado do que está livre de danos ou riscos”. Desta forma, entendemos que a Segurança da Informação – empresarial - nada mais é do que a proteção dos ativos informacionais de uma organização, em relação às perdas, exposição indevida ou dano (Williams, 2001).

2.1.2 Classificação das Informações

Para a gestão da segurança da informação, a classificação das informações é um dos pontos cruciais para um processo bem definido. É importante entender que, nesse aspecto, não existe uma determinação, por parte da ISO 27000, para a definição de cada um dos níveis, esse trabalho deve ser desenvolvido pela própria organização com fim de determinar a confidencialidade das informações.

É indispensável que haja participação de um Gestor do Negócio na classificação das informações, visto que somente ele consegue mensurar a importância de uma informação para a estratégia do negócio (Feliciano Neto; Furlan; Higo, 1988).

> Independentemente da relevância ou tipo da informação, a gestão dos dados organizacionais é estratégica, pois possibilita o apoio para a tomada de decisões em qualquer âmbito institucional. Algumas informações são centrais para organização e a divulgação parcial ou total destas pode alavancar um número de repercussões cuja complexidade pode ser pouco ou nada administrável pela organização com conseqüências possivelmente nefastas. (Laureano, 2005, p.8)

Não são todos os tipos de informação que precisam de atenção diferenciada. Wadlow (2000), expõe que existem níveis de prioridade para a classificação das informações, isso vai de acordo com a necessidade de cada organização, tal como a importância das definições para as atividades da empresa. Conforme o quadro 1, as classes definidas habitualmente são:

TIPO DA INFORMAÇÃO	**DEFINIÇÃO**
Pública	Todos podem ter acesso a informação, sua divulgação não prejudica o funcionamento da empresa.
Interna	Baixo nível de confidencialidade, não é vital para o negócio, porém deve ser evitado o acesso de público externo.
Restrita	Médio nível de confidencialidade, é restrita para alguns grupos da empresa, podendo levar a perdas expressivas se divulgada.
Confidencial	Mais alto nível de confidencialidade, é crítica e vital para a atividade da empresa, aqui é comum que haja a restrição da visualização aos executivos da empresa.

Quadro 1 - Classificação da Informação

2.1.3 Pilares da Segurança da Informação

Os pilares da SI são os conceitos que guiam as ações realizadas dentro dessa área de atuação. Há a descrição por parte de diversos autores sobre os tópicos que garantem a segurança dessas informações, dentre eles, Sêmola (2003), que define o objetivo da SI como sendo preservação da confidencialidade, integridade e disponibilidade. Esses descritos no quadro 2:

PILAR	OBJETIVO
Confidencialidade	Garantir a prevenção da revelação não autorizada das informações, ou seja, apenas pessoas autorizadas terão acesso às informações. É necessário assegurar que apenas pessoas com permissão tenham acesso à informação
Integridade	Garantir que a informação permanecerá sem alteração indevida. É necessário assegurar que a informação esteja correta e sem modificações por pessoas sem autorização prévia
Disponibilidade	Garantir que as pessoas autorizadas tenham acesso à informação sempre que solicitada. É necessário assegurar a prestação contínua do serviço, sem interrupções no fornecimento de informações para as pessoas autorizadas.

Quadro 2 - Pilares da Segurança da Informação

É importante notar na Figura 2 que, além dos pilares anteriormente citados, temos envolvidos na Segurança da Informação outros aspectos, são eles:

- Pessoas: é importante que as organizações tenham investimentos para a capacitação, conscientização e aculturamento de seus funcionários.
- Processos: criação de mecanismos de controle e regras claras para a utilização das tecnologias presentes na empresa.
- Tecnologia: é usada para garantir o controle dos processos já definidos, assegurando a conformidade com regras e impactando diretamente no negócio.

Figura 2 - 3 Pilares da Segurança da Informação. Traduzido de: Curvello (2016)

Diversas vezes temos acesso a exemplos de fraudes de grandes empresas causadas por falhas humanas, essas podendo ou não ser intencionais. DeMarco e Lister (1990), discorreram sobre a natureza dos principais problemas de uma empresa, que para eles são sociológicas, e não tecnológicas. A partir daí, é possível afirmar que no processo de segurança empresarial, a maior parte das falhas é humana, pois o homem é o ator mais sujeito à erros.

2.1.4 Ameaças, Vulnerabilidades e Riscos

Como dito anteriormente, a informação é o bem mais valioso de uma organização, sendo utilizada em diversos processos de negócio e está sujeita a ameaças.

> A ameaça pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e consequentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem. (Laureano, 2005)

As ameaças utilizam das falhas de segurança para provocar danos e prejuízos aos negócios de uma empresa. De acordo com Sêmola (2003), as ameaças se dividem em 3 grupos:

- Naturais: resultante de fenômenos naturais, tais como incêndios, terremotos, que podem causar danos aos ativos.
- Involuntárias: erros ou falta de conhecimento no uso do ativo, tratando-se de erros inconscientes dos usuários, possivelmente sem capacitação, como infecções por vírus e acessos indevidos.

- Voluntárias: provocadas por fraudes, invasões e roubos de informações.

Wadlow (2000, p. 12) mostrou que vulnerabilidades se tratam de pontos de fragilidade nos ativos, que se explorados por uma ameaça, afetam os pilares de segurança da informação (disponibilidade, integridade e confiabilidade). Para assegurar a melhoria na segurança da informação empresarial, é necessário identificar e eliminar os possíveis pontos fracos do ambiente.

De acordo com Gallagher (2012), temos os conceitos de risco, vulnerabilidade e ameaça, descritas no quadro 3:

CONCEITO	EXPLICAÇÃO
Risco	Probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização
Vulnerabilidade	Falha ou fraqueza de procedimento, *design*, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança
Ameaça	Possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade específica

Quadro 3 - Conceitos de Risco, Vulnerabilidade e Ameaça

Para a avaliação dos riscos devem ser delimitados os ativos considerados, com objetivo de minimizar a ocorrência ameaças que podem interferir no negócio. Quando se identifica um risco, é possível agir com intuito de combatê-lo ou adaptar-se a ele, fazendo com que exista então uma forma de geri-lo.

2.2 **ITIL: Visão geral**

ITIL (*Information Technology Infrastructure Library*) é um framework de boas práticas, que permite uma gerência eficiente dos serviços de TI, visando atender empresas de qualquer porte. Foi desenvolvido no final da década de 80 pela CCTA (*Central Computer and Telecommunications Agency*), hoje OGC (*Office for Government Commerce*) da Inglaterra e está atualmente na terceira versão.

O framework consiste em práticas para identificar processos na área de TI e alinhá-los às necessidades da organização, utilizando uma abordagem qualitativa para o uso eficiente da

infraestrutura de TI. Seu objetivo é gerar melhorias na organização, levando em consideração a redução de custos, com o aumento de eficiência dos serviços.

As empresas passaram a se preocupar com o gerenciamento de serviços de TI e, com o intuito de melhorar os processos existentes e reduzir custos, mais de 10.000 empresas, públicas e privadas, no mundo já adotaram as melhores práticas da ITIL, comprovando assim sua aceitação no mercado, segundo Amaral (2009).

Na figura 3, temos o Ciclo de Vida do Serviço e seus principais elementos contidos nos livros.

Figura 3 - Ciclo de Vida do Serviço. Extraído de: Ramos (2015)

A ITIL traduz-se num conjunto de livros, cada um deles representando uma área específica de manutenção e operação da infraestrutura de TI. Sendo os principais:

- Estratégia do Serviço: é o estágio onde se alinha a estratégia da TI com as necessidades do negócio. Essa etapa do ciclo de vida reflete em desdobramentos nos demais processos (Silva, 2012). São abordados os seguintes processos:
    a. Gerenciamento estratégico para serviços de TI
    b. Gerenciamento de portfólio de serviços
    c. Gerenciamento financeiro
    d. Gerenciamento de demanda
    e. Gerenciamento de relacionamento de negócio

- Desenho do Serviço: essa etapa auxilia no desenvolvimento dos serviços. São feitos detalhes de implementações e definições de escopos, começa-se a pensar em acordo de nível de serviço com o cliente e na capacidade da infraestrutura de suportar o serviço (Colin; Vernon, 2010). São abordados os seguintes processos:
    a. Coordenação do desenho
    b. Gerenciamento do catálogo de serviços
    c. Gerenciamento de nível do serviço
    d. Gerenciamento de disponibilidade
    e. Gerenciamento de capacidade
    f. Gerenciamento de continuidade do serviço
    g. Gerenciamento de segurança da informação
    h. Gerenciamento de fornecedor
- Transição do Serviço: aqui é feita a migração do serviço. Os detalhes para que os serviços definidos nas etapas anteriores entrem em produção são definidos nessa etapa, de forma a mitigar possíveis falhas (Silva, 2012). São abordados os seguintes processos:
    a. Planejamento e suporte a transição
    b. Gerenciamento de mudanças
    c. Gerenciamento de configuração e de ativo de serviço
    d. Gerenciamento de liberação e implantação
    e. Validação e teste de serviço
    f. Avaliação de mudança
    g. Gerenciamento de conhecimento
- Operação do Serviço: neste estágio é garantido o suporte dos serviços em produção. O foco é a correção de falhas e atendimento de requisições de serviços (Silva, 2012). São abordados os processos abaixo:
    a. Gerenciamento de evento
    b. Gerenciamento de incidentes
    c. Gerenciamento de requisições de serviço

d. Gerenciamento de problema
e. Gerenciamento de acesso

- Melhoria Contínua do Serviço: é feita uma avaliação de todos os processos e serviços, com foco em melhorias e analisando o atendimento desse serviço à demanda existente. Nessa etapa controla-se a qualidade na execução dos processos. É abordado o seguinte processo:
    a. Melhoria de sete passos

Com a aplicação de todos os estágios do ciclo de vida, existe menos retrabalho e os processos e serviços terão um alinhamento com as necessidades do negócio, segundo a ITIL.

2.2.1 ITIL e o Gerenciamento de Segurança da Informação

O ideal de ITIL para a segurança da informação é certificar que ela esteja implantada nos níveis estratégico, operacional e tático. Para ITIL, a segurança da informação é dividida em:

- Políticas: objetivos a serem atingidos
- Processos: o que deve ser feito para atingir
- Procedimentos: papéis e deadlines para atingir
- Instruções de trabalho: como executar as ações

O processo de Gerenciamento da Segurança da ITIL descreve a integração de TI na organização. Esse processo é baseado na norma ABNT NBR ISO/IEC 27002 e se relaciona com todos os outros processos de ITIL, mas principalmente com Gerenciamento do Nível do Serviço, Gerenciamento de Incidentes e Gerenciamento de Mudanças. Segundo Weil (2010), a SI é definida em ITIL como processo cíclico e com revisão contínua e melhorias incrementais, como mostrado na figura 4:

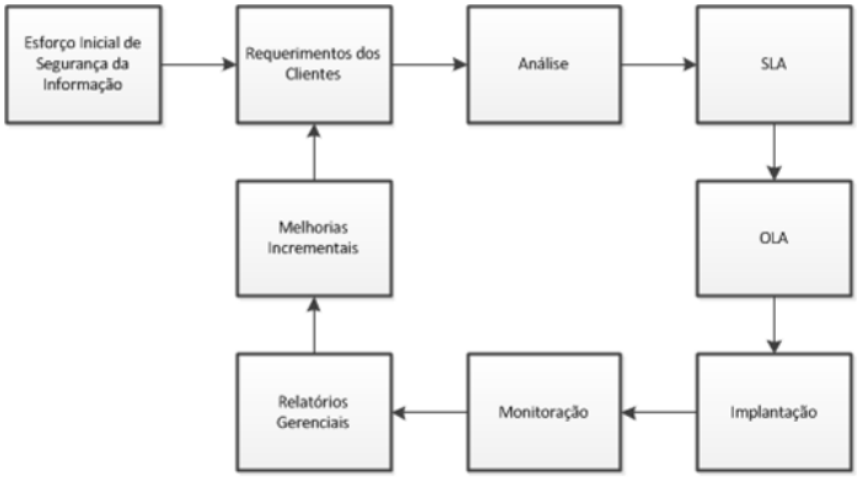

Figura 4 - Processo de Segurança da Informação. Extraído de: Smith (2010)

A partir desse processo, é possível dizer que ITIL reflete melhorias para as organizações. Manter um processo padronizado e baseado nas melhores práticas o torna menos custoso, eficiente e seguro.

2.3 **Norma ABNT NBR ISO/IEC 27002:2013**

A norma ABNT NBR ISO/IEC 27002:2013 consiste em um código de boas práticas para a segurança da informação. Nela é abordado que é necessário proteger a informação de ameaças para minimizar o risco, maximizar retornos dos investimentos e tornar possível a continuidade do negócio. É necessária a aplicação dos controles adequados, esses sendo processos, procedimentos, políticas, a fim de garantir a segurança da informação.

Os controles e mecanismos a serem implementados são listados como forma de auxiliar no atendimento aos requisitos após uma análise dos riscos, além de servir como um guia prático para a implementação de padrões de segurança da informação em empresas.

Sua base foi um documento publicado pelo governo do Reino Unido, que se tornou um padrão em 1995, chamado BS7799. A norma foi publicada como um novo nome para o padrão ISO 17799 em 2000, e se tratava também de um código de prática para SI, até que em 2005 foi publicada uma nova versão, da família de normas internacionais 27000, onde foram lançados alguns documentos acerca do tema, para serem usados em conjunto.

Em sua versão atual, publicada em 2013, a ISO 27002 consta com 114 controles, diferindo da versão de 2005 que possuía 133 controles documentados. E suas seções, para uma melhor definição, foram divididas em 14, em vez das 11 seções da versão anterior.

De acordo com a ISO, a norma foi desenhada para ser usada por organizações que pretendem selecionar os controles dentro do processo de implementação de Sistemas de Gerenciamento de Segurança da Informação baseados na norma ISO/IEC 27001, implementar controles comumente aceitos de segurança da informação, desenvolver as regras internas de GSI.

2.3.1 Áreas de Controle e Objetivos

A norma tem em sua estrutura os controles necessários para o GSI. As seções da norma são divididas entre os objetivos de controle, que são importantes para o processo de SI. Os controles são estruturados através de: nome do controle, diretrizes para a implementação e informações adicionais.

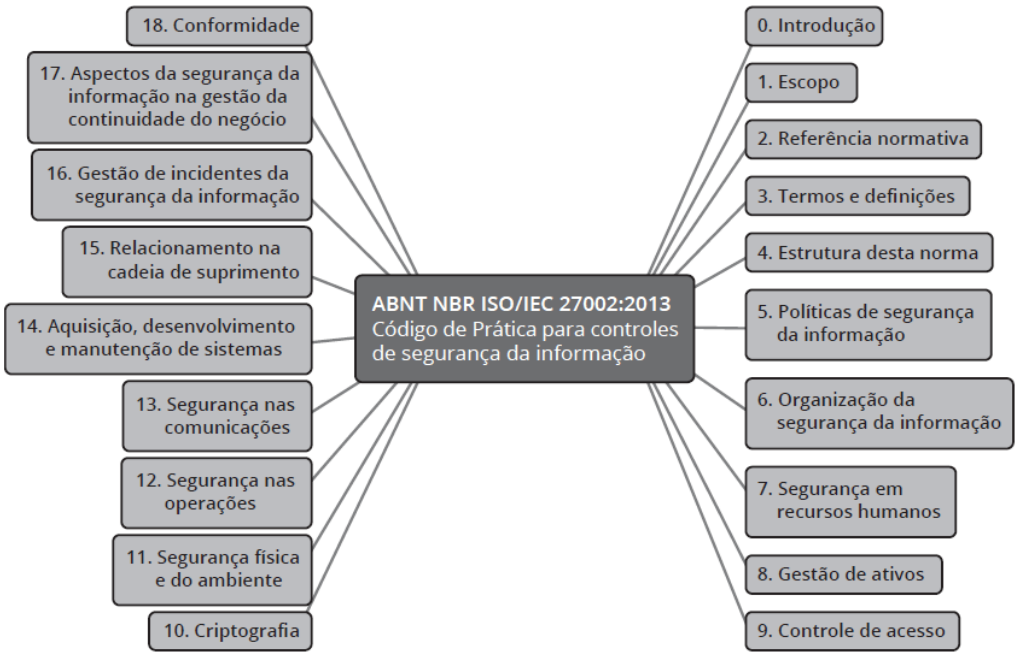

Figura 5 - Estrutura da norma ABNT NBR ISO/IEC 27002:2013. Extraído de: Coelho, Araújo e Bezerra (2014).

Na figura 5 temos a divisão dos capítulos, sendo os capítulos 0 até 4 temas de introdução e a partir do capítulo 5 eles passam a ser chamados de seção, apresentando os códigos de práticas de gerenciamento de segurança.

O quadro 4 foi montado de acordo com os objetivos presentes na norma NBR ISO/IEC 27002:2013, para cada uma das seções.

SEÇÃO	OBJETIVOS
5. Políticas de segurança da informação	Fornecer orientação de gestão e suporte para a segurança da informação de acordo com os requisitos de negócio e as leis e regulamentos relevantes.
6. Organização da segurança da informação	Estabelecer um quadro de gestão para iniciar e controlar a implementação e funcionamento da segurança da informação dentro da organização.
7. Segurança em recursos humanos	Antes do contrato: garantir que os funcionários e contratados compreendam suas responsabilidades e são adequados para as funções para as quais são considerados. Durante o contrato: garantir que os funcionários e partes externas estejam conscientes e cumpram as suas responsabilidades de segurança da informação. Encerramento do contrato: proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.
8. Gestão de ativos	Identificar ativos organizacionais e definir responsabilidades de proteção apropriadas, além de assegurar que as informações recebam um nível adequado de proteção de acordo com a sua importância para a organização, e prevenir a divulgação não autorizada, modificação, remoção ou destruição da informação armazenada nas mídias.
9. Controle de acesso	Limitar o acesso a informações e instalações de processamento de informações, garantir o acesso de usuários autorizados e impedir o acesso não autorizado a sistemas e serviços, tornar os usuários responsáveis pela proteção de suas informações de autenticação, impedir o acesso não autorizado a sistemas e aplicações.
10. Criptografia	Garantir a utilização adequada e eficaz da criptografia para proteger a confidencialidade, autenticidade e / ou integridade da informação.
11. Segurança física e do ambiente	Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização.

Quadro 4 - Seções e objetivos da NBR ISO/IEC 27002:2013 *(continua).* (ABNT, 2013)

SEÇÃO	OBJETIVOS
12. Segurança nas operações	Garantir a operação segura e correta dos recursos de processamento da informação, assegurar que as informações e os recursos de processamento da informação estão protegidos contra *malware*, proteger contra a perda de dados e gravar eventos e gerar evidências.
13. Segurança nas comunicações	Assegurar a proteção das informações em redes e da infraestrutura de suporte.
14. Aquisição, desenvolvimento e manutenção de sistemas	Assegurar e desenvolver a segurança da informação nas aplicações da organização
15. Relacionamento na cadeia de suprimento	Assegurar a proteção dos ativos da organização que podem ser acessados pelos fornecedores.
16. Gestão de incidentes da segurança da informação	Garantir uma boa gestão de incidentes de segurança da informação, incluindo a comunicação sobre eventos e deficiências de segurança.
17. Aspectos da segurança da informação na gestão de continuidade do negócio	Incorporar a continuidade da segurança da informação nos sistemas de gerenciamento de continuidade de negócios da organização.
18. Conformidade	Evitar violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança.

Quadro 5 - Seções e objetivos da NBR ISO/IEC 27002:2013 *(conclusão).* (ABNT, 2013)

2.3.1.1 A política de segurança da informação para a norma ISO/IEC 27002:2013

A ideia da seção de política de segurança da informação é que o documento contenha conceitos sobre a segurança da informação e o comprometimento da direção da organização com o documento.

Além disso, é determinada uma estrutura onde estejam estabelecidos os objetivos de controle e os próprios controles, a estrutura de análise e o gerenciamento de riscos, assim como

as regras, políticas e requisitos de conformidade de segurança da informação específicos para essa organização.

Como explicado na norma, é importante que a política seja comunicada a todos da organização, tal como devem ser realizadas as devidas análises e revisões críticas, a partir da direção da organização, em intervalos regulares, ou mesmo quando necessárias mudanças.

2.4 **Avaliação de Maturidade de Processos**

Um modelo de maturidade consiste em um sistema de medidas, possibilitando uma categorização por níveis, esses pré-definidos, existindo estágios evolutivos entre os níveis. É possível identificar atividades que não são realizadas e afetam diretamente a evolução do nível de maturidade durante o processo de avaliação, o que mostra oportunidades de melhorias.

O principal objetivo de um modelo de maturidade é contribuir para a melhoria contínua, utilizando um processo controlado e mensurado, o qual exige práticas específicas de gestão, de acordo com o *Software Engineering Institute* (SEI, 2006) da Carnegie Mellon University.

O ITIL possui um modelo de maturidade bem definido, chamado *Process Maturity Framework* – PMF. Em Pereira e Silva (2010) é descrito que apenas o PMF é notadamente desenhado para o ITIL, apesar de existirem diversos modelos de maturidade.

No modelo abordado, PMF, existem cinco níveis de maturidade entendidos por: Inicial, Repetitivo, Definido, Gerenciado e Otimizado, o que é de utilidade para a avaliação da melhoria contínua dos serviços e processos (Colin; Vernon, 2010).

2.4.1 Níveis e Dimensões de Maturidade do PMF

De acordo com Colin e Vernon (2010), o PMF utiliza cinco níveis de maturidade para avaliar o estado dos processos, sendo esses:

- Nível 1: conhecido por nível inicial, ‘ad hoc’ ou caótico. Nele existe o reconhecimento do processo, porém há poucas atividades que estejam dentro do seu escopo. Não é amparado financeiramente (sem orçamento determinado) ou mesmo existem recursos para realizarem o escopo.

- Nível 2: conhecido por nível repetitivo, existe reconhecimento do processo, mas não é de interesse para a organização e, por isso, não recebe os recursos adequados. As atividades são executadas sem uma administração correta, normalmente de forma irregular e têm pouca efetividade para a organização.
- Nível 3: conhecido por nível definido, o processo é reconhecido e documentado, porém não existe formalização ou mesmo aceitação de sua função na organização. Contudo, são definidos responsáveis, objetivos e metas, e, diferente dos níveis anteriores, possui recursos e foco numa maior efetividade. São feitos relatórios sobre o que foi executado, com o objetivo de serem usados como referências.
- Nível 4: conhecido por nível gerenciado, existe uma aceitação e reconhecimento do processo por toda a área de TI. Seu foco é na prestação de serviços e seus objetivos e metas têm como base os objetivos e metas do negócio. Processo mapeado e gerenciado de forma proativa, existindo interfaces estabelecidas e documentadas, inclusive em relação aos outros processos de TI.
- Nível 5: conhecido por nível otimizado, o processo, além de ter um reconhecimento pleno, tem objetivos e metas estratégicas alinhadas com os objetivos e metas estratégicas da TI e do negócio. Encontra-se institucionalizado, como parte das atividades cotidianas e existem atividades de melhoria contínua, estabelecidas como parte do próprio processo.

Para o PMF há a qualificação dos processos a partir de um modelo que engloba diversos aspectos ou dimensões, sendo essas: Visão e Orientação, Processos, Pessoas, Tecnologia e Cultura (Colin; Vernon, 2010). Conforme quadro 5:

DIMENSÃO	DESCRIÇÃO
Visão e Orientação	Estão relacionadas com os objetivos que a organização pretende alcançar e que estão diretamente vinculados ao orçamento disponível e ao estabelecimento de metas a serem atingidas.

Quadro 6 - Dimensões PMF (continua). Adaptado de: Colin; Vernon (2010).

DIMENSÃO	DESCRIÇÃO
Processos	Refere–se à forma como a organização se estrutura para atingir seus objetivos, se existe predominância de áreas isoladas, determinadas pela função, ou se atua numa abordagem voltada para processos.
Pessoas	Refere-se à forma como os profissionais interagem na organização, se predomina o isolamento ou a integração, o que é determinante para o estabelecimento de níveis de colaboração e compartilhamento de informações.
Tecnologia	Trata da existência de uma arquitetura global de TI, que tenha integração com pessoas e processos.
Cultura	Refere-se ao conjunto de ideias, valores, crenças, práticas e expectativas, compartilhadas entre as pessoas dentro da organização.

Quadro 7 - Dimensões PMF (conclusão). Adaptado de: Colin; Vernon (2010).

A determinação do nível de maturidade dos processos é ligada diretamente à maturidade nas dimensões citadas. Além disso, essa visão dividida por dimensões permite aos gestores que ajam pontualmente nestas dimensões, de acordo com a prioridade por eles estabelecida e torna mais fácil a estratégia de elevação da maturidade.

2.5 **Trabalhos Relacionados**

Hoje existem alguns modelos de melhores práticas e normas acerca do assunto de SI, e tratando-se do assunto de gestão, é dado destaque para a norma ISO/IEC 27002 que aborda o código de prática para o GSI.

Muitos trabalhos mostram propostas para a aplicação das normas no ambiente corporativo. Quase todos os trabalhos sobre GSI têm como base a norma ISO/IEC 27002. Souto, Silva e Lima (2006) propõem a aplicação da norma para ambientes corporativos, porém o trabalho tem um direcionamento muito técnico. Para Rosa (2011), o envolvimento da direção e alta gerência na formulação de política de segurança da informação (PSI) garante que o documento esteja alinhado com os requisitos do negócio e com requisitos legais. Almeida (2014), examina a maturidade dos processos de segurança da informação aplicando um

questionário, baseado na norma ISO/IEC 27001:2013, para os responsáveis pela gestão na instituição estudada.

Existem, no Brasil e no exterior, órgãos que publicam recomendações para gestão de SI. O NIST, órgão de tecnologia dos EUA, disponibiliza um apanhado de informações relacionadas à segurança e auditoria. No Brasil é possível encontrar órgãos públicos, como o TCU (2007), disponibilizando um manual de boas práticas em segurança da informação, que contempla decisões do órgão sobre segurança em TI.

Além disso, há outras normas e guias que recomendam ações para melhores práticas de TI de forma ampla, que mesmo não abordando especificamente o tema de SI, instruem de fato a manter sistemas, organizações e informações protegidos, encaixando-se dessa forma o framework ITIL.

2.5.1 Proposta e Aplicação de um Modelo de Maturidade da Gestão por Processos

As organizações têm se interessado pela adoção de modelos de gestão orientados para processos de negócio, como meio para o aumento da agilidade, integração e flexibilidade. O gerenciamento da TI não é mais assunto apenas de grandes corporações, mas uma necessidade de qualquer organização que busca melhorar o desenvolvimento das atividades realizadas. O propósito desse trabalho correlato, Felippio e Moreno (2010), foi avaliar a utilidade e aplicabilidade de questionários para analisar o estágio da implantação da Gestão por Processos em uma grande empresa brasileira do setor de energia.

Para chegar ao resultado, o estudo de Felippio e Moreno (2010) criou um novo instrumento de avaliação do nível de maturidade em Gestão de Processos, consolidando os modelos do *Capability Maturity Model Integration* (CMMI) e *Process and Enterprise Maturity Model* (PEMM) que classificaram os níveis de maturidade dos processos de TI. Com a o desenvolvimento do novo método, a partir dos já estudados, foi possível avaliar o nível de maturidade da Gestão de Processos da organização por meio de questionários direcionados.

Em Felippio e Moreno (2010), foi feito um estudo de caso exploratório numa grande empresa multinacional com o objetivo de identificar o nível de maturidade da mesma, houve uma apresentação de um questionário para diferentes colaboradores por meio de um modelo de

gestão em TI com base nas boas práticas do Cobit® para a otimização do gerenciamento da tecnologia em uma pequena organização, bem como o reconhecimento do nível de maturidade atual dos processos desenvolvidos na instituição.

O que difere o trabalho correlato do estudo que está sendo realizado é o foco do questionário, por ser generalista em relação a processos e não voltado a uma área específica, o que torna o público-alvo do trabalho que está sendo realizado de mais fácil definição. O padrão de boas práticas estudado pelo autor é o Cobit® e não o ITIL. Outra importante diferença é que foi elaborado um novo instrumento de diagnóstico de nível de maturidade, enquanto nesta pesquisa é apresentado um modelo já utilizado e mostra a importância da aplicação de padrões e boas práticas para a avaliação de maturidade da organização, com base nos levantamentos adquiridos.

2.5.2 Análise do Processo de Change Management Utilizando as Boas Práticas do ITIL

A pesquisa de Santos (2013) tem como objetivo apresentar uma visão crítica sobre o gerenciamento de serviços de TI, identificando as práticas que devem ser utilizadas para a melhoria e a maturidade dos serviços em uma organização carente de gerenciamento, sua finalidade é mostrar os benefícios de um efetivo gerenciamento de serviços.

Ao decorrer do trabalho, foram apresentadas técnicas e boas práticas que auxiliam no desenvolvimento e maturidade de processos de TI da organização estudada, assim como padrões e mecanismos tratados como referências no mercado.

O trabalho teve como base o modelo PMF para chegar ao resultado. O uso de questionário direcionado para a área de Gerenciamento de Mudanças tornou possível a avaliação do nível de maturidade do processo citado, visto que foi aplicado para um público de seis colaboradores que tinham algum tipo de interação com o processo.

A investigação foi realizada em uma empresa multinacional alemã do segmento de Telecomunicações. No estudo é explicitada a necessidade, por meios contratuais, da conformidade da empresa com o modelo ITIL, mas são vistas diversas dificuldades, visto que a área de gestão de serviços da empresa é relativamente nova.

Foram divididos, na avaliação de maturidade do processo, tópicos de causas apontadas de problemas para cada uma das dimensões PMF, pontos positivos do processo e sugestões de melhoria para a empresa. Após concluir a análise da maturidade, foi observado pelo autor que a avaliação dos processos utilizando o modelo PMF tornou fácil a identificação das falhas e possibilitou também a avaliação da evolução da qualidade dos serviços prestados pela área de TI da organização. A partir dela, foi viabilizada uma reorganização nas equipes técnicas.

O autor monta para o usuário todo um plano de ação voltado para as falhas existentes nos processos estudados, o que é um ponto de diferença entre ele e o objeto de estudo atual. É possível notar que ambos têm foco em um processo específico do ITIL, mostrando a eficácia do modelo PMF para a avaliação pontual de processos.

2.5.3 Gerenciamento de Serviços de TI: O Uso das Boas Práticas de Gerenciamento de Serviços de TI com Base na Biblioteca ITIL v3

No estudo “Gerenciamento de Serviços de TI: O Uso das Boas Práticas de Gerenciamento de Serviços de TI com Base na Biblioteca ITIL v3”, Santana (2015) discute sobre a utilização das melhores práticas de TI no Gerenciamento de Serviços, realizando análises sobre o cenário da organização. Para isso discorre sobre o ciclo de vida dos serviços visto na ITIL e seu modelo de avaliação de maturidade de processos, o PMF.

A pesquisa nos mostra as principais falhas nos processos da organização estudada, do segmento de construção. Para isso é feita uma análise com base nos conceitos vistos na ITIL e é utilizada a estrutura do PMF para realizar os estudos sobre as dimensões. Além da exposição das falhas, é realizada uma proposta de melhoria, com plano de ação definido.

De acordo com o Santana (2015), o gestor de TI é fundamental para o sucesso do estudo, pois é a partir dele que se certifica que a TI está alinhada com a área de negócios, identificando necessidades dos demais gestores e buscando alinhar a operação de TI com o negócio.

Os resultados da pesquisa possibilitaram identificar os problemas e falhas vistos durante a análise dos dados, bem como apresentar um plano de ações criado para o benefício da operação de TI. Ademais, a organização ficou com uma ferramenta consistente de avaliação dos processos,

o que permite a utilização para a continuidade da evolução da maturidade dos processos e consequentemente a melhoria na entrega dos serviços.

O trabalho citado possui como semelhança ao estudo realizado o uso do PMF, o que mostra uma efetividade do modelo. As diferenças entre os trabalhos se apresentam no foco da pesquisa, sendo a citada voltada para os processos de gerenciamento de serviços como um todo e neste estudo o foco é no processo de gestão de segurança da informação.

3 ESTRATÉGIA PARA AVALIAÇÃO DA MATURIDADE

No desenvolvimento do modelo foi determinado como primeiro passo a elaboração de um questionário, levando em consideração o processo ITIL Gerenciamento de Segurança da Informação e a norma NBR ISO/IEC 27002:2013 e contendo perguntas específicas sobre cada uma das dimensões apontadas, para com isso conseguir as informações necessárias sobre o processo. A elaboração das perguntas observou as exigências de cada um dos níveis de maturidade de acordo com Colin e Vernon (2010), sendo eles:

1- Inicial
2- Repetitivo
3- Definido
4- Gerenciado
5- Otimizado

O quadro 6 apresenta as descrições das dimensões de acordo com cada nível citado, pelo modelo PMF, que formaram a base para a criação do questionário do processo de Gerenciamento de Segurança da Informação ITIL:

Dimensões da Maturidade dos Processos	**Nível**	**Descrição das Dimensões**
Visão e Orientação	1	Fundos e recursos orçamentários mínimos, com pouca ou nenhuma atividade. Resultados temporários e não registrados. Relatos e opiniões esporádicas.
	2	Sem objetivos claros ou metas formais. Fundos e recursos orçamentários disponíveis. Atividades irregulares e não planejadas.
	3	Documentação e objetivos acordados, com metas formais. Planos publicados formalmente, monitorados e revisados. Fundos disponíveis, com recursos apropriados. Relatórios regulares, com revisões periódicas.

Quadro 8 - Indicadores das Dimensões (continua). Adaptado de: Silva (2012)

Dimensões da Maturidade dos Processos	Nível	Descrição das Dimensões
Visão e Orientação	4	Direção clara dos objetivos de negócios e metas estabelecidas e mensuradas. Relatórios de gestão usados para tomada de decisão. Processos de negócios alinhados aos planos de TI. Melhorias regulares, planejadas e revisadas.
	5	Plano estratégico integrado aos planos de negócios, com metas e objetivos controlados. Monitoramento contínuo, medição, elaboração de relatórios de alerta e relatórios sobre o processo contínuo de melhoria. Revisões periódicas e / ou auditorias com eficácia, eficiência e observância das normas.
Processos	1	Processos e procedimentos vagamente definido, executado de forma reativa quando ocorrem problemas. Processos totalmente reativos. Atividades irregulares e não planejadas.
	2	Processos e procedimentos definidos. Processo em grande parte reativo. Atividades irregulares e não planejadas.
	3	Processos e procedimentos claramente definidos e bem divulgados. Atividades planejadas regularmente. Existência de documentação do processo. Ocasionalmente processo proativo.
	4	Processos, procedimentos e padrões bem definidos, incluído todas as descrições de trabalho da equipe de TI. Interfaces e dependências do processo claramente definidas. Processos proativo. Gerenciamento de serviços integrados e processos de desenvolvimento de sistemas
	5	Processos e procedimentos bem definidos, fazendo parte da cultura corporativa. Processo proativo e preventivo.

Quadro 9 - Indicadores das Dimensões (continuação). Adaptado de: Silva (2012)

Dimensões da Maturidade dos Processos	Nível	Descrição das Dimensões
Pessoas	1	Papéis e responsabilidades vagamente definidos.
	2	Papéis e responsabilidades descritos, contudo sem formalidade.
	3	Papéis e responsabilidades claramente definidos e acordados. Objetivos e metas formais. Processos formalizados com planos de treinamentos.
	4	Equipe de trabalho multidisciplinar com foco em processos. Responsabilidades claramente definidas para todas as atividades de trabalho da TI.
	5	Objetivos de negócio alinhados com a TI, com metas formais ativamente monitorados, como parte da atividade diária. Papéis e responsabilidades faz parte de uma cultura corporativa geral.
Tecnologia	1	Processos manuais, sem ferramentas de automatização.
	2	Possui ferramentas padrão, contudo falta controle e os dados são armazenados em locais separados.
	3	Coleta de dados contínua com alarmes e limiar monitoração dos serviços. Dados consolidados acumulados e usados para o planejamento formal, previsão e análise de tendências.
	4	Monitoração contínua, com indicação de alarmes e um conjunto de ferramentas e bancos de dados integrados.
	5	Documentação da arquitetura geral com ferramentas integradas em todas as áreas de pessoas, processos e tecnologia.
Cultura	1	Ferramentas tecnológicas utilizadas nas atividades com foco nos processos de TI.
	2	Produtos e serviços controlados.
	3	Serviços orientados ao cliente com uma abordagem formalizada – Acordo de Nível de Serviço.
	4	Foco no negócio com uma compreensão ampla das estratégias corporativas.
	5	Uma atitude de melhoria contínua, juntamente com uma estratégica focada no negócio. Uma compreensão do valor da TI para o negócio e seu papel dentro da cadeia de valor do negócio.

Quadro 10 - Indicadores das Dimensões (conclusão). Adaptado de: Silva (2012)

Foi analisado o modelo proposto pelo PMF e feitas adaptações para a elaboração do questionário relativo ao processo de Gerenciamento de Segurança da Informação. O questionário, apresentado no quadro 7, foi aplicado a um público alvo de dois profissionais, sendo um Gerente da área de Segurança da Informação de uma empresa do segmento de Petróleo e Gás e o segundo *Chief Technology Officer* (CTO) de uma empresa do segmento de Tecnologia da Informação (Rede social). De acordo com a quantificação das respostas, foram determinados os respectivos níveis de maturidade.

Questionário Gerenciamento de Segurança da Informação	
Dimensão	**Pergunta**
Visão e Orientação	A importância da segurança da informação é assimilada pela alta gestão? Como o assunto é tratado na organização?
	A organização tem uma estratégia de segurança? Se sim, é alinhada com a estratégia de negócios?
	O conselho é informado sobre as questões de segurança da informação? São passadas instruções sobre riscos e melhoria no estado de segurança? Como isto acontece?
	Se houver um incidente grave de segurança, seu custo para a organização é determinado? Como é determinado?
Processos	Existe uma política / estrutura de segurança de informações e conteúdo?
	Você tem políticas e procedimentos para a segurança de conteúdo e proteção de ativos?
	Você tem políticas e procedimentos de controle de alterações? Como é feito o controle?
	Você tem políticas de mídia social ou diretrizes que abordam o seguinte: como os colaboradores são autorizados a associar-se com a instalação; Proibir o compartilhamento de informações ou conteúdos sensíveis com a comunidade externa; E padrões de comportamento?
Pessoas	Existem cargos de segurança de informação com responsabilidades bem definidas? Como são comunicadas?
	Os colaboradores são capacitados para reconhecer e relatar possíveis incidentes e violações de segurança? Como é feita a capacitação?
	A interação entre os colaboradores na execução do processo é satisfatória?

Quadro 11 - Questionário de Gerenciamento de Segurança da Informação (continua)

Questionário Gerenciamento de Segurança da Informação	
Dimensão	**Pergunta**
Pessoas	Existe uma matriz de comunicação com a indicação dos responsáveis?
Tecnologia	Como você garante que seus processos de *disaster recovery* atendam aos requisitos de continuidade de negócios da organização?
	Existe um plano de resposta a incidentes que estabelece uma equipe de resposta a incidentes, procedimentos de relatórios, processos de resposta e notificações de violação de segurança?
	A organização implementa controles de segurança física e lógica? Que medidas você toma para garantir que suas políticas e configurações de segurança sejam aplicadas de forma consistente em toda a organização?
	Como você garante que seus processos de backup e restauração atendam aos requisitos de continuidade de negócios da organização?
	Como você governa o uso de identidades de serviço e credenciais administrativas?
	Como a organização implementa requisitos de segurança no gerenciamento de operações e comunicações tais como gestão de mudanças, segregação de funções, segregação de ambientes de produção/ homologação/ desenvolvimento? Implementa ainda recursos de proteção de infraestrutura para dispositivos portáteis, computadores e equipamentos de redes e teleprocessamento?
Cultura	Que tipos de verificações de antecedentes (emprego, histórico criminal, crédito, rastreamento de drogas, etc.) você conduz para pessoas (novos colaboradores, contratados, estagiários, terceiros, etc.) que trabalham em suas instalações?
	São feitos programas de conscientização para garantir que os colaboradores estejam cientes das suas responsabilidades de segurança e das expectativas da gestão? Como você capacita seus colaboradores?
	Existe, de forma satisfatória, o compartilhamento das informações sobre os processos de TI? Como é feito o compartilhamento?
	Existe um canal para que os colaboradores possam sugerir melhorias ao processo?

Quadro 12 - Questionário de Gerenciamento de Segurança da Informação (conclusão)

Para o preenchimento do questionário foi necessária a realização das entrevistas e foram atribuídas notas de acordo com os níveis de maturidade (1, 2, 3, 4 ou 5) para cada uma das perguntas formuladas nas dimensões PMF.

Após a análise dos dados das entrevistas, foi feita a média aritmética das dimensões abordadas a partir das notas atribuídas a cada pergunta, calculando assim o nível de maturidade da respectiva dimensão.

Na análise final da maturidade dos processos foram consideradas ponderações nas dimensões definidas, dando maior foco nas ações consideradas mais essenciais ao GSI, assim conseguindo estabelecer prioridades na execução de ações de melhoria. Para isso, os pesos definidos indicam o grau de importância de cada dimensão, mostrado no quadro 8:

Dimensão	**Peso**	**Justificativa**
Processos	3	Foi atribuído o peso (3) para a dimensão Processos em razão de sua grande relevância no GSI. Quanto maior o nível de maturidade desta dimensão, significa que a organização está voltada para processos.
Visão e Orientação	2	Foi atribuído o peso (2) para a dimensão Visão e Orientação tendo em vista sua importância no estabelecimento de metas e alinhamento com o negócio.
Pessoas	2	Foi atribuído o peso (2) para a dimensão Pessoas em razão da sua importância ao se tratar de Recursos Humanos.
Tecnologia	2	Foi atribuído o peso (2) para a dimensão Tecnologia em razão da sua importância ao se tratar de ferramentas para operacionalização do processo.
Cultura	1	Foi atribuído o peso (1) para a dimensão Cultura tendo em vista sua importância ao se tratar dos comportamentos necessários para o GSI.

Quadro 13 - Dimensões Ponderadas

Enquanto o cálculo da maturidade por dimensão utiliza a média aritmética com as notas atribuídas às perguntas, o cálculo de maturidade do processo faz uso da média ponderada com as notas atribuídas para cada dimensão.

É importante ressaltar que todas as dimensões são essenciais e que esta organização baseada em ponderações objetiva o estabelecimento de prioridades nos pontos necessários para a elevação de maturidade dos processos ITIL.

4 ANÁLISE DE RESULTADOS

A avaliação da maturidade ITIL foi executada para 1 (um) processo ITIL, o processo de Gerenciamento de Segurança da Informação, do estágio de Desenho do Serviço. Para determinar o nível de maturidade de Gerenciamento de Segurança da Informação em que se encontram as organizações pesquisadas foi formatado um conjunto de perguntas a serem respondidas pelos colaboradores. O questionário fornece um roteiro que objetiva a obtenção de respostas sobre as dimensões anteriormente citadas, dando oportunidade de avaliar separadamente cada uma delas.

4.1 **Empresa A**

A empresa A é uma sociedade anônima de capital aberto, do segmento de Petróleo e Gás, classificada como empresa de grande porte.

4.1.1 Visão e Orientação

Após a análise dos dados da entrevista realizada na empresa A, é verificada uma participação contínua da alta gestão nos assuntos estratégicos de segurança da informação, fato examinado em acordo com as respostas do Gerente de Segurança da Informação. Existem membros de diversas áreas de negócio no comitê de segurança da informação, com isso é mais fácil haver desdobramentos sobre o assunto por toda a companhia, pois o comitê valida as necessidades das áreas envolvidas por meio de análises de risco e posteriormente aprova ou recusa as necessidades provindas das áreas.

O panorama reativo não possui uma orientação clara, visto que ao sofrer algum incidente grave de segurança, o mesmo não tem seu custo determinado para a organização, o que pode se tornar um empecilho na construção de um *business case* para a solicitação de investimentos na área de segurança.

A média de maturidade da dimensão foi determinada de acordo com a tabela 1:

Empresa	Dimensão	Média de Maturidade da Dimensão
A	Visão e Orientação	4

Tabela 1 - Maturidade da Dimensão Visão e Orientação (Empresa A)

4.1.2 Processos

A visão de processos da empresa é muito bem definida, existindo uma política de segurança da informação em mais alto nível, que se integra com diretrizes sobre diferentes conteúdos de segurança da informação. Entende-se que os processos foram criados para serem utilizados de forma proativa, com planejamento de atividades e frequência definida para a execução de procedimentos. Todos os processos possuem um gestor e uma equipe formal e previamente definidos para executá-los.

A média de maturidade da dimensão foi determinada de acordo com a tabela 2:

Empresa	Dimensão	Média de Maturidade da Dimensão
A	Processos	5

Tabela 2 - Maturidade da Dimensão Processos (Empresa A)

4.1.3 Pessoas

Existe no organograma da empresa uma estrutura de SI bem definida, com analistas, gerentes, etc. No comitê de segurança da informação existe a participação das mais diversas áreas de negócio da empresa, os membros desse comitê são indicados pelos gestores formalmente.

A organização patrocina a capacitação dos funcionários para segurança da informação, de capacitações gerais a capacitações técnicas dos colaboradores da área de SI. Anualmente são reforçados os conceitos de SI como uso e descarte de informações, classificação das informações, entre outros. No final dos treinamentos anuais é feito um questionário para verificar a absorção do conteúdo.

Além disso, os colaboradores interagem continuamente através das ferramentas da organização para relatar possíveis incidentes de segurança da informação.

A média de maturidade da dimensão foi determinada de acordo com a tabela 3:

Empresa	Dimensão	Média de Maturidade da Dimensão
A	Pessoas	5

Tabela 3 - Maturidade da Dimensão Pessoas (Empresa A)

4.1.4 Tecnologia

As ferramentas da empresa são integradas de forma a facilitar a automatização do processo. Existem equipes de testes e de tratamento de incidentes. O ferramental de monitoração dos ambientes provê a geração de relatórios automatizados, menos passíveis de erro.

No ponto sobre segurança física e lógica, existe todo um ambiente com ferramentas e monitoração preparado para uma possível auditoria. Cada um desses pontos possui um padrão de comportamento para ser analisado e isso é exposto nas políticas e diretrizes de segurança da organização.

Como ponto de atenção vemos não são implementados recursos de proteção de infraestrutura para dispositivos portáteis, o que torna inviável a aplicação de *bring your own device* (BYOD) na organização. Além disso a segregação de função só é aplicada para ambientes críticos, o que prejudica a efetividade dos controles sobre as aplicações.

A média de maturidade da dimensão foi determinada de acordo com a tabela 4:

Empresa	**Dimensão**	**Média de Maturidade da Dimensão**
A	Tecnologia	4,16

Tabela 4 - Maturidade da Dimensão Tecnologia (Empresa A)

4.1.5 Cultura

Na dimensão de cultura vemos que a organização realiza diversos programas de conscientização e que os mesmos são feitos por todos os colaboradores, além disso existem canais de comunicação para a sugestão de melhorias no processo conhecidos amplamente na organização.

Como ponto de atenção não vemos verificação de antecedentes dos novos colaboradores e não há a intenção de implantar esse tipo de processo na organização. Além disso, a base de conhecimento, onde são compartilhados os processos e informações de segurança, não é amplamente divulgada na organização, o compartilhamento ocorre principalmente a nível de analistas.

A média de maturidade da dimensão foi determinada de acordo com a tabela 5:

Empresa	Dimensão	Média de Maturidade da Dimensão
A	Cultura	3,5

Tabela 5 - Maturidade da Dimensão Cultura (Empresa A)

4.1.6 Análise e conclusões

Conclui-se na análise da empresa A que praticamente a maioria dos domínios resultados do Gerenciamento de Segurança da Informação eficaz encontra-se em níveis de maturidade otimizados, com algumas dimensões em níveis mais baixos.

É visto um modelo concebido originalmente voltado para a SI em vista do conteúdo respondido pelo entrevistado.

Por todos os domínios levantados no questionário respondido pela empresa A, é possível verificar que a mesma se enquadra no nível gerenciado de maturidade, porém em transição para o nível otimizado de maturidade em GSI.

Empresa	Maturidade do Processo	Nível
A	4,48	Nível Gerenciado: existe uma aceitação e reconhecimento do processo por toda a área de TI. Seu foco é na prestação de serviços e seus objetivos e metas têm como base os objetivos e metas do negócio. Processo mapeado e gerenciado de forma proativa, existindo interfaces estabelecidas e documentadas, inclusive em relação aos outros processos de TI.

Tabela 6 - Maturidade do Processo (Empresa A)

Como pontos de atenção relativos ao nível de maturidade da empresa temos:

- Não existe orientação sobre o custo do panorama reativo;
- Segregação de funções é feita apenas para ambientes críticos;
- Falta de recursos de proteção para dispositivos portáteis;
- Falta de divulgação da base de conhecimento para os colaboradores da empresa.

4.2 **Empresa B**

A empresa B é uma associação privada, de capital fechado, no segmento de Tecnologia da Informação, entregando uma rede social de relacionamentos, classificada como empresa de pequeno porte.

4.2.1 Visão e Orientação

A empresa enxerga a SI como um fator preocupante e está investindo em sistemas e políticas, além de estar aumentando a área de segurança da informação.

Não existe uma orientação provinda das lideranças sobre a execução do gerenciamento de segurança da informação. Existem problemas para definir as instruções sobre riscos e melhoria no estado de segurança da empresa e não são feitas priorizações.

Incidentes de segurança têm custo estimado com base no histórico de venda e acessos à rede social, porém não estimam com precisão os vazamentos de dados.

A média de maturidade da dimensão foi determinada de acordo com a tabela 7:

Empresa	**Dimensão**	**Média de Maturidade da Dimensão**
B	Visão e Orientação	1,75

Tabela 7 - Maturidade da Dimensão Visão e Orientação (Empresa B)

4.2.2 Processos

Se tratando de uma rede social, a maior preocupação está no desenvolvimento da plataforma. A organização realiza um controle de alterações seguindo boas práticas e revisão de alterações por outros membros da equipe.

Em contrapartida, não existem políticas de segurança da informação definidas e nem diretrizes abordando outros tópicos relacionados à segurança da informação como um todo. Ademais, não existe uma definição formalizada para a restrição de acessos às informações ou sobre categorização das informações. A média de maturidade da dimensão foi determinada de acordo com a tabela 8:

Empresa	Dimensão	Média de Maturidade da Dimensão
B	Processos	1,5

Tabela 8 - Maturidade da Dimensão Processos (Empresa B)

4.2.3 Pessoas

A capacitação dos colaboradores é realizada apenas para os especializados, o que torna a identificação de possíveis incidentes mais difícil. Existe um colaborador na equipe especializado em segurança, porém suas responsabilidades não são bem definidas. Não há uma matriz de comunicação definida e os colaboradores não sabem distinguir as responsabilidades.

A média de maturidade da dimensão foi determinada de acordo com a tabela 9:

Empresa	Dimensão	Média de Maturidade da Dimensão
B	Pessoas	1,25

Tabela 9 - Maturidade da Dimensão Pessoas (Empresa B)

4.2.4 Tecnologia

Os recursos tecnológicos utilizados pela organização são voltados principalmente para a área de desenvolvimento do site, tendo uma boa gestão dos ambientes, com segregação de ambientes de homologação, produção e desenvolvimento. Além disso existe uma facilidade na elasticidade do ambiente, por ser um ambiente de nuvem.

Os procedimentos de *backup* e *restore* são feitos por uma equipe terceirizada, que domina o processo e o implementa. A gestão de identidades existe de maneira bem definida, com ferramentas próprias e monitoração do comportamento.

Em contrapartida, não são feitos controles físicos de segurança, tornando o ambiente vulnerável. Além disto, não existe um plano de resposta a incidentes e os colaboradores são responsáveis por detectar possíveis incidentes e corrigi-los. A média de maturidade da dimensão foi determinada de acordo com a tabela 10:

Empresa	Dimensão	Média de Maturidade da Dimensão
B	Tecnologia	2,66

Tabela 10 - Maturidade da Dimensão Tecnologia (Empresa B)

4.2.5 Cultura

Não são realizadas verificações de antecedentes para novos colaboradores e não existe a intenção de fazê-las. Além disso, a empresa não conta com investimentos em programas de conscientização dos funcionários. Além disso, não há um canal de sugestões de melhoria de processos pelos funcionários.

O compartilhamento das informações não é feito, pois não há processos documentados. Porém os funcionários são treinados para acompanharem os processos da empresa. A média de maturidade da dimensão foi determinada de acordo com a tabela 11:

Empresa	Dimensão	Média de Maturidade da Dimensão
B	Cultura	1,25

Tabela 11 - Maturidade da Dimensão Cultura (Empresa B)

4.2.6 Análise e conclusões

Conclui-se na análise da empresa B que a maioria dos domínios se encontra em nível de maturidade inicial, mostrando um gerenciamento de segurança da informação ineficaz. Não há a aderência aos modelos práticos de segurança da informação para guiar as iniciativas relativas.

Diante desse contexto, a empresa B deve priorizar uma estratégia que envolva a segurança da informação e adotar práticas relacionadas para colaborar positivamente para a governança de TI, para o gerenciamento de segurança da informação e alinhar a estratégia da TI com o negócio. Sem esse alinhamento, a empresa fica vulnerável aos riscos apresentados.

Empresa	Maturidade do Processo	Nível
B	1,70	Nível inicial: ‘ad hoc’ ou caótico. Nele existe o reconhecimento do processo, porém há poucas atividades que estejam dentro do seu escopo. Não é amparado financeiramente (sem orçamento determinado) ou mesmo existem recursos para realizarem o escopo.

Tabela 12 - Maturidade do Processo (Empresa B)

Como pontos de atenção acerca do nível de maturidade da empresa temos:

- Não existe orientação das lideranças sobre a execução do GSI;
- Não existem políticas de segurança, nem diretrizes, voltados para o processo de GSI;
- Não há formalização sobre restrição de acessos;
- Sem distinção de responsabilidades para os colaboradores da empresa;
- A capacitação só é realizada em nível de especialização, outros colaboradores não têm acesso aos materiais de capacitação sobre SI;
- Não são feitos controles físicos de acesso;
- Não existe um plano de resposta a incidentes.

5 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

A análise do processo de Gerenciamento de Segurança da Informação utilizando como base as boas práticas do ITIL e a norma NBR ISO/IEC 27002:2013 teve por finalidade avaliar o atual nível de maturidade no processo de Gerenciamento de Segurança da Informação das duas empresas, apresentando assim os estágios da qualidade, no que diz respeito à execução deste processo. Com esta abordagem foi possível identificar lacunas que prejudicam a execução do processo de Gerenciamento de Segurança da Informação nestas empresas e consequentemente, enxergar oportunidades de melhorias.

Avaliar o processo de Gerenciamento de Segurança da Informação, utilizando a metodologia ITIL e normas referentes ao tópico, traz efeitos positivos para governança de TI, sendo uma ferramenta mais eficaz de gestão para avaliar a evolução da qualidade dos serviços prestados pela área de TI.

Assim, a utilização do modelo de maturidade PMF propiciou uma visão sistêmica do processo de Gerenciamento de Segurança da Informação, conseguindo extrair através de suas dimensões as melhorias necessárias para elevar a maturidade do processo ITIL.

É visto que, com a avaliação do nível de maturidade do processo de Gerenciamento de Segurança da Informação do ITIL, é possível organizar e priorizar os trabalhos das equipes técnicas.

Entende-se que os objetivos deste trabalho foram atendidos, foram apresentados os processos ITIL e sua implantação para a segurança da informação, bem como foi possível, a partir do modelo estudado, avaliar e identificar as falhas do processo no cenário atual das duas empresas.

Para esse trabalho, o universo de colaboradores contribuindo na resposta ao questionário foi considerado uma limitação, o motivo desse problema foi a indisponibilidade de outros colaboradores.

Além disso, na prática, as ponderações determinadas para cada dimensão deveriam ter considerado as prioridades dos próprios responsáveis pela área de SI de cada uma das empresas. Para uma maior efetividade, as perguntas incluídas no questionário deveriam ter sido ponderadas

com a consulta à especialistas da área de SI. Contudo, foi possível aprofundar o estudo, que teve como principais figuras gestores de TI das organizações estudadas.

Como trabalhos futuros o intuito é continuar mapeando os procedimentos e investir na ampliação das boas práticas para outros processos ITIL. É importante manter a realização das análises com uma certa frequência, para a evolução do gerenciamento de serviços e o cumprimento de melhorias nos processos citados neste trabalho.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro. 2013.

ALBUQUERQUE, F. Estruturando a Segurança da Informação. Profissionais de TI. 2009.

ALMEIDA, F. H. S. Avaliação da Maturidade dos Processos de Segurança da Informação em uma Instituição de Ensino Superior Pública Federal. Lavras. 2014.

AMARAL, L. S. A implantação dos processos de Governança da TI segundo o framework do COBIT. 2009.

CASTELLS, M. 2007. A sociedade em rede. 11ª ed., São Paulo, Paz e Terra, 698 p.

COELHO, F. E. S. ; ARAÚJO, L. G. S. ; BEZERRA, E. K. Gestão da Segurança da Informação: NBR 27001 e NBR 27002. RNP. Rio de Janeiro. 2014.

COLIN, R.; VERNON, L. Service Design ITIL Version 3. Editora The Stationery Office. 2010.

CURVELLO, A. M. de L. Segurança em Foco no IoT – Protegendo as Informações das Coisas. 2016. Disponível em: http://www.slideshare.net/andrecurvello/segurana-em-foco-no-iot-protegendo-as-informaes-das-coisas

DAVENPORT, T. Ecologia da Informação. Futura. São Paulo. 2002.

DeMARCO, T. ; LISTER, T. Peopleware – Como Gerenciar Equipes e Projetos Tornados-os mais Produtivos. Editora McGraw-Hill. São Paulo, 1990.

FELICIANO NETO, A. ; FURLAN, J. D. ; HIGO, W. Engenharia da Informação – Metodologia, Técnicas e Ferramentas. Editora McGrawHill. São Paulo. 1988.

FELIPPIO, C. K.; MORENO, V. de A. Proposta de Aplicação de um Modelo de Maturidade de Gestão por Processos. Rio de Janeiro. 2013.

FONTES, E. Praticando a Segurança da Informação - Orientações práticas alinhadas com Norma NBR ISO/IEC 27002, Norma ISO/IEC 27001, Norma NBR 15999-1, COBIT, ITIL. Editora Brasport. 2008

GALLAGHER, Patrick D. NIST SP 800-30 – Guide for Conducting Risk Assessments. Computer Security Division Information Technology Laboratory. 2012.

ITIL. Disponível em: http://www.itil-officialsite.com/

LAUREANO, M. A. P. Gestão de Segurança da Informação. 2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf

PALMA, F. Níveis de Maturidade na Gestão de TI. Portal GSTI. 2013. Disponível em: https://www.portalgsti.com.br/2013/07/niveis-de-maturidade-na-gestao-de-ti.html. Acesso em: julho, 2017.

PEREIRA, R. F. de S.; SILVA, M.M. da. ITIL Maturity Model. 2010.

RAMOS, L. ITIL – Como Ferramenta no Desenvolvimento Estratégico de sua Empresa. Acelerato. 2015. Disponível em: http://blog.acelerato.com/agile/itil-como-ferramenta-no-desenvolvimento-estrategico-de-sua-empresa/. Acesso em: julho, 2017.

SANTANA, D. Gerenciamento de Serviços de TI: O Uso das Boas Práticas de Gerenciamento de Serviços de TI com Base na Biblioteca ITIL v3. Universidade do Vale do Rio dos Sinos. Porto Alegre, 2015.

SANTOS, A. L. A. M. Análise do Processo de Change Management Utilizando as Boas Práticas do ITIL. Universidade Tecnológica Federal do Paraná. Curitiba. 2013.

SÊMOLA, M. Gestão da Segurança da Informação – Uma visão Executiva. Editora Campus. Rio de Janeiro. 2003.

SHEDROFF, N. Information interaction design: a unified field theory of design. Information Design. London: MIT Press, 1999.

SILVA, L. C. Avaliação da maturidade ITIL: uma abordagem prática. 2012. 97 f. Monografia (Especialização em Governança de Tecnologia da Informação) – Serviço Nacional de Aprendizagem Comercial. Brasília, 2012. Disponível em: http://www.edilms.eti.br/uploads/file/orientacoes/GTIDF03%20-%20Lucinaldo%20Cirino.pdf. Acesso em: junho, 2017.

SIMIÃO, R. S. Segurança da Informação e Comunicações: conceito aplicável em organizações governamentais. Brasília. 2009. Disponível em: http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/reinaldo_silva.pdf

SMITH Jr, R. ITIL – Benefícios Associados à Segurança da Informação. Microsoft Technet. 2010. Disponível em: https://blogs.technet.microsoft.com/ronaldosjr/2010/01/05/itil-benefcios-associados-segurana-da-informao/

SOFTWARE ENGINEERING INSTITUTE (SEI). CMMI para Desenvolvimento. Versão 1.2. 2006.

SOUTO, C. C.; SILVA, M. A.; LIMA, W. D. Estudo e Aplicação da Norma NBR ISO/IEC 17799:2005 em Segurança da Informação. Dissertação (Trabalho Final de Curso) — UNIEURO Centro Universitário. Brasília. 2006.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Boas práticas em segurança da informação. 2. ed. Brasília. 2007.

WADLOW, T. Segurança de Redes. Editora Campus. Rio de Janeiro, 2000.

WEIL, S. How ITIL Can Improve Information Security. 2010. Disponível em: https://www.symantec.com/connect/articles/how-itil-can-improve-information-security

Apêndice A

O apêndice A apresenta as notas atribuídas a cada uma das perguntas definidas no questionário, para ambas as empresas estudadas.

1. Empresa A

Processo de Gerenciamento de Segurança da Informação		
Dimensão	**Pergunta**	**Nota**
Visão e Orientação	A importância da segurança da informação é assimilada pela alta gestão? Como o assunto é tratado na organização?	**5**
	A organização tem uma estratégia de segurança? Se sim, é alinhada com a estratégia de negócios?	**5**
	O conselho é informado sobre as questões de segurança da informação? São passadas instruções sobre riscos e melhoria no estado de segurança? Como isto acontece?	**5**
	Se houver um incidente grave de segurança, seu custo para a organização é determinado? Como é determinado?	**1**
Processos	Existe uma política / estrutura de segurança de informações e conteúdo?	**5**
	Você tem políticas e procedimentos para a segurança de conteúdo e proteção de ativos?	**5**
	Você tem políticas e procedimentos de controle de alterações? Como é feito o controle?	**5**
	Você tem políticas de mídia social ou diretrizes que abordam o seguinte: como os colaboradores são autorizados a associar-se com a instalação; Proibir o compartilhamento de informações ou conteúdos sensíveis com a comunidade externa; E padrões de comportamento?	**5**
Pessoas	Existem cargos de segurança de informação com responsabilidades bem definidas? Como são comunicadas?	**5**
	Os colaboradores são capacitados para reconhecer e relatar possíveis incidentes e violações de segurança? Como é feita a capacitação?	**5**
	A interação entre os colaboradores na execução do processo é satisfatória?	**5**
	Existe uma matriz de comunicação com a indicação dos responsáveis?	**5**
Tecnologia	Como você garante que seus processos de *disaster recovery* atendam aos requisitos de continuidade de negócios da organização?	**4**
	Existe um plano de resposta a incidentes que estabelece uma equipe de resposta a incidentes, procedimentos de relatórios, processos de resposta e notificações de violação de segurança?	**4**
	A organização implementa controles de segurança física e lógica? Que medidas você toma para garantir que suas políticas e configurações de segurança sejam aplicadas de forma consistente em toda a organização?	**5**
	Como você garante que seus processos de backup e restauração atendam aos requisitos de continuidade de negócios da organização?	**5**
	Como você governa o uso de identidades de serviço e credenciais administrativas?	**5**
	Como a organização implementa requisitos de segurança no gerenciamento de operações e comunicações tais como gestão de mudanças, segregação de funções, segregação de ambientes de produção/ homologação/ desenvolvimento? Implementa ainda recursos de proteção de infraestrutura para dispositivos portáteis, computadores e equipamentos de redes e teleprocessamento?	**2**
Cultura	Que tipos de verificações de antecedentes (emprego, histórico criminal, crédito, rastreamento de drogas, etc.) você conduz para pessoas (novos colaboradores, contratados, estagiários, terceiros, etc.) que trabalham em suas instalações?	**1**
	São feitos programas de conscientização para garantir que os colaboradores estejam cientes das suas responsabilidades de segurança e das expectativas da gestão? Como você capacita seus colaboradores?	**5**
	Existe, de forma satisfatória, o compartilhamento das informações sobre os processos de TI? Como é feito o compartilhamento?	**3**
	Existe um canal para que os colaboradores possam sugerir melhorias ao processo?	**5**

2. Empresa B

Processo de Gerenciamento de Segurança da Informação		
Dimensão	**Pergunta**	**Nota**
Visão e Orientação	A importância da segurança da informação é assimilada pela alta gestão? Como o assunto é tratado na organização?	**2**
	A organização tem uma estratégia de segurança? Se sim, é alinhada com a estratégia de negócios?	**2**
	O conselho é informado sobre as questões de segurança da informação? São passadas instruções sobre riscos e melhoria no estado de segurança? Como isto acontece?	**1**
	Se houver um incidente grave de segurança, seu custo para a organização é determinado? Como é determinado?	**2**
Processos	Existe uma política / estrutura de segurança de informações e conteúdo?	**1**
	Você tem políticas e procedimentos para a segurança de conteúdo e proteção de ativos?	**1**
	Você tem políticas e procedimentos de controle de alterações? Como é feito o controle?	**3**
	Você tem políticas de mídia social ou diretrizes que abordam o seguinte: como os colaboradores são autorizados a associar-se com a instalação; Proibir o compartilhamento de informações ou conteúdos sensíveis com a comunidade externa; E padrões de comportamento?	**1**
Pessoas	Existem cargos de segurança de informação com responsabilidades bem definidas? Como são comunicadas?	**1**
	Os colaboradores são capacitados para reconhecer e relatar possíveis incidentes e violações de segurança? Como é feita a capacitação?	**1**
	A interação entre os colaboradores na execução do processo é satisfatória?	**2**
	Existe uma matriz de comunicação com a indicação dos responsáveis?	**1**
Tecnologia	Como você garante que seus processos de *disaster recovery* atendam aos requisitos de continuidade de negócios da organização?	**2**
	Existe um plano de resposta a incidentes que estabelece uma equipe de resposta a incidentes, procedimentos de relatórios, processos de resposta e notificações de violação de segurança?	**1**
	A organização implementa controles de segurança física e lógica? Que medidas você toma para garantir que suas políticas e configurações de segurança sejam aplicadas de forma consistente em toda a organização?	**1**
	Como você garante que seus processos de backup e restauração atendam aos requisitos de continuidade de negócios da organização?	**4**
	Como você governa o uso de identidades de serviço e credenciais administrativas?	**4**
	Como a organização implementa requisitos de segurança no gerenciamento de operações e comunicações tais como gestão de mudanças, segregação de funções, segregação de ambientes de produção/ homologação/ desenvolvimento? Implementa ainda recursos de proteção de infraestrutura para dispositivos portáteis, computadores e equipamentos de redes e teleprocessamento?	**4**
Cultura	Que tipos de verificações de antecedentes (emprego, histórico criminal, crédito, rastreamento de drogas, etc.) você conduz para pessoas (novos colaboradores, contratados, estagiários, terceiros, etc.) que trabalham em suas instalações?	**1**
	São feitos programas de conscientização para garantir que os colaboradores estejam cientes das suas responsabilidades de segurança e das expectativas da gestão? Como você capacita seus colaboradores?	**1**
	Existe, de forma satisfatória, o compartilhamento das informações sobre os processos de TI? Como é feito o compartilhamento?	**2**
	Existe um canal para que os colaboradores possam sugerir melhorias ao processo?	**1**