UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS ARARANGUÁ

Anne Caroline Dias Bezerra

UMA MODELAGEM DE SEGURANÇA DA INFORMAÇÃO BASEADA NA ISO/IEC 27001 E GESTÃO ITIL APLICADA ÀS MICROS E PEQUENAS EMPRESAS

Araranguá,10 de julho de 2015.

Anne Caroline Dias Bezerra

UMA MODELAGEM DE SEGURANÇA DA INFORMAÇÃO BASEADA NA ISO/IEC 27001 E GESTÃO ITIL APLICADA ÀS MICROS E PEQUENAS EMPRESAS

Trabalho de Curso submetido à Universidade Federal de Santa Catarina, como parte dos requisitos necessários para a obtenção do Grau de Bacharel em Tecnologias da Informação e Comunicação.
Orientadora: Profª. Drª. Analúcia Schiaffino Morales

Araranguá, 15 de julho de 2015.

Anne Caroline Dias Bezerra

UMA MODELAGEM DE SEGURANÇA DA INFORMAÇÃO BASEADA NA ISO/IEC 27001 E GESTÃO ITIL APLICADA ÀS MICROS E PEQUENAS EMPRESAS

Este Trabalho de Conclusão de Curso foi julgado aprovado para a obtenção do Título de Bacharel em Tecnologias da Informação e Comunicação, e aprovado em sua forma final pelo Curso de Graduação em Tecnologias da Informação e Comunicação.

Araranguá, 15 de julho de 2015

Prof.ª Dr.ª Patrícia Fiuza,
Coordenadora do Curso

Banca Examinadora:

Prof.ª Dr.ª Analúcia Schiaffino Morales
Orientadora

Prof. Dr. Paulo César Leite Esteves

Prof. Dr. Márcio Roberto Machado da Silva

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Bezerra, Anne Caroline Dias
UMA MODELAGEM DE SEGURANÇA DA INFORMAÇÃO BASEADA NA ISO/IEC 27001 E INFRAESTRUTURA ITIL APLICADA ÁS MICROS E PEQUENAS EMPRESAS / Anne Caroline Dias Bezerra ; orientadora, Analúcia Schiaffino Morales - Araranguá, SC, 2015.
100 p.

Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Santa Catarina, Campus Araranguá. Graduação em Tecnologias da Informação e Comunicação.

Inclui referências

1. Tecnologias da Informação e Comunicação. 2. Segurança da informação. 3. ISO/IEC 27001 . 4. ITIL. 5. Micros e pequenas empresas. I. Morales, Analúcia Schiaffino. II. Universidade Federal de Santa Catarina. Graduação em Tecnologias da Informação e Comunicação. III. Título.

Este trabalho é dedicado à deus, minha família, meus amigos e namorado.

AGRADECIMENTOS

Agradeço primeiramente a deus por me acompanhar nesta jornada. A minha família que mesmo longe me incentivou desde o inicio dessa caminhada e me proporcionou apoio nos momentos de tristeza e desafios, e principalmente meu pai e minha mãe. Aos meus amigos que sempre estiveram ao meu lado, fazendo com que esta caminhada se tornasse mais leve, ao meu namorado Valter Savi que sempre me apoiou e me motivou. E finalmente, agradeço ao professor Ricardo Moraes que me ajudou no inicio desse caminho e a minha orientadora Analúcia Schiaffino Morales que me orientou de maneira que a pudesse concretizar esse trabalho.

“A insanidade é continuar fazendo sempre a mesma coisa e esperar por resultados diferentes”

(Albert Einstein)

RESUMO

A segurança da informação é um assunto que vem crescendo e tomando um âmbito de pesquisa muito amplo, a Internet e a domesticação dos ativos tecnológicos tornou-se parte essencial do cotidiano da sociedade. Devido a isso, as micros e pequenas empresas tem sofrido um atraso de estruturação no contexto de segurança de seus ativos, pois as normas internacionais não são direcionadas para este porte de organização. O presente trabalho, através da análise das normas de segurança e de infraestrutura internacional, propõe uma modelagem para empregar diretivas de segurança em empresas menores. Foram analisadas as diretivas de segurança da ISO/IEC 27001 e de infraestrutura do ITIL (*Information Technology Infrastructure Library*), que são referência nestas áreas. Avaliando os principais fatores que estão associados a este cenário, e através da realização de um levantamento de empresas de tecnologia do Vale do Araranguá, foi então proposta uma modelagem de forma a agregar segurança da informação e de infraestrutura a estes estabelecimentos.

Palavras-chave: Segurança da informação, Governança em TI, ITIL, ISO 27001, ISMS, Micro e pequenas empresas.

ABSTRACT

Information security is a subject that has been growing and taking a broad scope within research, as the Internet and domestication of technological assets has become an essential part of the day-to-day of society. Due to this, micro-enterprise and small companies have suffered a delay in structuring within the context of security of its assets, as the international standards are not directed to this size of organization. The present work, through analysis of the standards of security and of international infrastructure, proposes a modeling to employ directives of security within small companies. The directives of security of ISO/IEC 27001 and of the infrastructure of ITIL (*Information Technology Infrastructure Library*), which are references in this area, were analyzed. By evaluating the principal factors that are associated with such scenario, and through the realization of raising technological businesses of the Araranguá Valley, a model to increase security of information and infrastructure of such establishments was proposed.

Key-words: Information security, Governance in IT, ITIL, ISO 27001, ISMS, micro-enterprise and small businesses.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

TIC – Tecnologia da Informação e Comunicação

MPE – Micro Pequena Empresa

TI - Tecnologias da informação

ITIL – *Information Technology Infrastructure Library*

VPN – *Virtual Private Network*

PK*I* – *Public Infrastructure Key*

ISMS – Information Security Management System

PDCA – *Plan Do Check Act*

ITSM –*Information Technology Service Management*

CEO – Chief Executive Office

SUMÁRIO

1 INTRODUÇÃO

Quando o assunto é segurança da informação nos atuais parâmetros da sociedade é impossível não associar as diversas notícias hoje vinculadas sobre vírus e ataques cibernéticos contra indivíduos ou organizações corporativas. Hoje com a expansão da Internet, das tecnologias, e do valor das informações que trafegam em dispositivos portáteis como celulares, *tablets* e computadores, torna-se inviável não possuir um método efetivo que proporcione a segurança a estes ativos.

A tecnologia e as redes de computadores deixaram de ser vistas como acessórios e entraram na categoria de necessidade, principalmente dentro do contexto organizacional.

Em uma pesquisa realizada pela revista Exame (2014) é demonstrado que o setor de micro e pequenas empresas (MPEs) é representado por aproximadamente 9 milhões de empresas que compõe cerca de 27% do PIB brasileiro.

Através desses dados se pode observar a importância e o crescimento deste setor para a economia brasileira.

Outra pesquisa realizada pelo IBGE em 2010 demonstra que o uso das TIC's dentre as empresas pesquisadas, ou seja 2,2 milhões cerca de 80,8% delas utilizam computadores, e 2,1 milhões totalizando 76,9% delas fazem uso da Internet e por fim cerca de 2,3 milhões, aproximadamente 83,3% utilizam o telefone celular como ferramenta de trabalho.

Esses dados apontam a abrangência das TIC's dentro desse ambiente empresarial brasileiro, mas que, no entanto esses dados possuem uma curva de declínio quando é separado e tratado a proporção das empresas analisadas. Assim sendo, observa-se que entre micro empresa esse percentual de uso de computadores cai para 78% enquanto pequenas empresas, e a taxa de uso das TIC's foi de 94,1% e a mesma proporção se manteve em relação ao uso de Internet e telefones móveis, que são respectivamente 73,7% e 94,1%.

Faixas de pessoal ocupado	Proporção de empresas que utilizaram (%)									
	Computador					Internet				
	Total	Atividades incluídas no âmbito da pesquisa				Total	Atividades incluídas no âmbito da pesquisa			
		Indústrias	Comércio	Informação e Comunicação	Outros serviços		Indústrias	Comércio	Informação e Comunicação	Outros serviços
Total	**80,8**	**82,1**	**78,9**	**87,0**	**83,2**	**76,9**	**80,1**	**74,2**	**86,4**	**79,5**
01 a 09	78,0	73,4	76,6	85,4	81,5	73,7	71,1	71,5	84,8	77,6
10 a 19	94,1	93,3	96,0	98,9	91,0	91,5	91,1	94,0	98,5	86,8
20 a 49	97,0	97,2	98,2	99,5	95,0	95,7	96,2	97,0	99,5	93,0
50 a 499	99,2	98,7	100,0	100,0	99,3	98,7	98,1	99,6	100,0	98,7
500 ou mais	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0	100,0

Tabela 1. Proporção de empresas que utilizaram computador e Internet
Fonte: IBGE, 2010.

Esse comportamento é destacado pelo (IBGE, 2010) como o potencial de crescimento que seguirá nos próximos anos em relação à utilização desses ativos em empresas de pequeno-médio porte.

A partir desses dados que apontam para uma clara curva de potencial de crescimento dentro do contexto de MPEs é possível expor a importância que a segurança pode adquirir conforme aconteça essa curva de crescimento do uso de tecnologias no setor MPEs, somado ao crescimento de sua representação no PIB na economia brasileira. Resultantes que se somadas provocam uma margem crescente da necessidade e importância que o setor segurança assume conforme o continuo crescimento dessas variáveis no setor.

Em sequência, pode-se argumentar que a partir desse crescente uso de ferramentas tecnológicas, é importante que seja definido políticas e boas práticas que assegurem a segurança dos dados e informações que trafegam na rede e nos dispositivos. Dentro desta questão, existe a problemática de que muitas MPEs se enxergam livres de quaisquer riscos e perigos existentes na rede.

Porém um recente relatório revelado pela Symantec (2013) nos conduz a uma realidade diferente, no qual é descrito no relatório de ameaças à segurança na Internet e constatado um crescimento no roubo de informações valiosas e confidenciais no setor de manufatura e, principalmente nas pequenas empresas nas quais, foram alvos de 31% dos ataques em 2012.

A pesquisa Symantec ainda acrescenta que as MPEs são alvos atraentes, por não darem a devida importância às ferramentas ou políticas que as protejam dessas ameaças.

Essa problemática é confirmada através dos dados adquiridos pela pesquisa realizada pelo IBGE que demonstra o percentual de MPEs que possuíam uma política de segurança definida, o qual é demonstrado na figura 1 e tabela 2 a seguir.

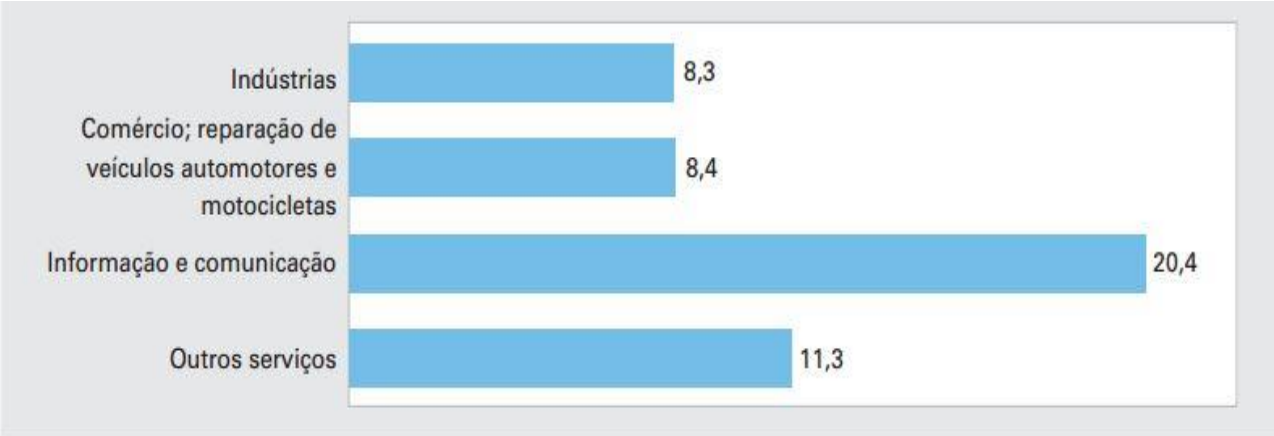

Figura 1. Percentual de microempresas que tinham uma politica de segurança em TI/TIC formalmente definida.

Fonte: IBGE, 2010.

Atividades incluídas no âmbito da pesquisa	Proporção de empresas com 1 ou mais pessoas ocupadas que tinham política de segurança em TI/TIC formalmente definida (%)					
	Total	Faixas de pessoal ocupado				
		01 a 09	10 a 19	20 a 49	50 a 499	500 ou mais
Total	**11,9**	**9,7**	**17,1**	**19,9**	**36,5**	**66,6**
Indústrias	12,9	8,3	11,1	15,8	34,3	71,4
Comércio; reparação de veículos automotores e motocicletas	10,4	8,4	20,3	21,9	38,8	70,1
Informação e comunicação	23,2	20,4	31,6	44,9	66,4	86,7
Outros serviços	12,9	11,3	16,1	21,2	36,0	57,0

Tabela 2. Proporção de empresas que possuem politicas de segurança definidas.

Fonte: IBGE, 2010.

Como é observado, de acordo com o IBGE (2010) é evidente a falta de estrutura de segurança da informação no setor MPEs com relação a estrutura e a uma política de segurança da informação. Percebe-se essa deficiência, pois apesar das MPEs serem o segmento com maior número de empresas do país, elas ainda possuem o que Castro (2014) explicita como um problema que está relacionado em como a estrutura da TI é tratada neste setor. Ela é vista

como um ponto de suporte para os processos dentro da organização, enquanto deveria ser abordada como uma vantagem estratégica com toda uma estrutura de suporte.

A perspectiva que a governança em TI incorporada ao negócio está tomando em importantes ferramentas de gestão e boas práticas internacionais, nas quais são atreladas pode ser constatada quando respeitáveis nomes como ITIL, ISO 27001 tratam deste assunto de estrutura e gestão estratégica de modo que podem transformar o olhar dos gestores quanto a importância dessas práticas na organização, embora seja argumentado por gestores de MPE que os motivos nos quais Não há uma estrutura adequada para comportar e gerenciar os ativos de TIC na organização são os custos elevados que tais processos possuem. Apesar disto, existe uma contra argumentação que enquanto os gestores falam sobre custos desses processos os mesmos devem enxergar os valores e benefícios que a implementação dessas práticas causam na governança da TI da organização.

Partindo desse cenário, neste presente trabalho foi realizada uma pesquisa e avaliação da gestão ITIL e norma ISO/IEC 27001 e suas práticas com intuito de explorar suas principais características no contexto de segurança da informação e seus parâmetros, com um olhar aplicado à micro e pequena empresa.

1.1 Justificativa e motivação

A segurança da informação é um tema que tem adquirido bastante foco e importância na atualidade. A pesquisa aplicada pela escola de administração de São Paulo da Fundação Getúlio Vargas (FGV 2010), afirma que no Brasil o número de computadores por habitante chega a ser de três computadores a cada cinco habitantes, foram analisados também detalhes sobre o uso das tecnologias da informação em médias e grandes empresas.

Diante destes números é claramente percebido que as TIC’s estão ocupando um espaço de grande importância nesse cenário. Partindo dessa premissa, tem-se verificado a necessidade de uma efetiva estrutura de controle e segurança dessas informações que trafegam todos os dias no contexto das pequenas organizações.

O que se percebe é que nem todos que fazem o uso dessa tecnologia estão devidamente capacitados no ponto de vista de segurança, em contrapartida à quantidade crescente de situações de violação a informações pessoais ou de órgãos e empresas.

A partir disto, este trabalho teve como justificativa e motivação a realização de um levantamento que ajudasse a entender as necessidades que este setor possui e através de uma pesquisa bibliográfica dos modelos ITIL e ISO/IEC 27001 modelar uma estrutura adaptada para essas micros e pequenas e empresas.

1.2 Objetivos gerais e específicos

O objetivo principal do presente trabalho é avaliar a modelagem de estruturas internacionais de segurança da informação ISO 27001 e o gerenciamento de infraestrutura do ITIL considerando os aspectos que são aplicáveis para empresas de pequeno-médio porte, ou seja micros e pequenas empresas.

Entre os objetivos específicos, destacam-se:

1. Apresentar uma revisão bibliográfica sobre normas internacionais de segurança da informação e seus modelos e técnicas;
2. Identificar características dos padrões ISO/IEC 27001 e ITIL que são mais relevantes e se encaixam no cenário de micros e pequenas empresas;
3. Especificar um modelo de gestão da estrutura da segurança da informação com enfoque em micros e pequenas empresas.

1.3 Metodologia

Inicialmente realizou-se uma pesquisa bibliográfica para o desenvolvimento de uma fundamentação teórica sólida sobre o tema.

Em seguida realizou-se um modelo de pesquisa diagnóstica qualitativa para captar dados do conhecimento e utilização de técnicas de segurança e da utilização de normas e padronizações da área, e quais as dificuldades, expectativas e investimentos na área.

O diagnóstico foi desenvolvido por meio de uma pesquisa com sete empresas de desenvolvimento de ramo de tecnologia do Vale do Araranguá . Sendo que somente cinco delas autorizaram o uso da coleta de dados serem representados neste trabalho.

As empresas entrevistadas são caracterizadas como micros e pequenas empresas, no qual a empresa definida como micro empresa foi a empresa de número um que possuía uma média de ocupação de sete colaboradores e fazia parte do setor econômico de desenvolvimento de sites e artes digitais.

As empresas caracterizadas por pequenas empresas foram as empresa de número dois com a ocupação de 33 colaboradores que faz parte do setor de provedor de serviços de internet, a empresa representada pelo número 3 com ocupação de 12 colaboradores do setor de desenvolvimento de software, a empresa de número quatro com uma média de 50 colaboradores com atuação no setor de desenvolvimento de sistemas governamentais, e por fim a empresa 5 com ocupação equivalente a 15 colaboradores com atuação em desenvolvimentos de aplicativos e sistemas comerciais.

Antes da visita foi pré-elaborada as questões que seriam abordadas em todas as empresas, e que foi respondida por todos os envolvidos, subsequente às perguntas foi feito um bate-papo aberto para melhor caracterizar as necessidades e desafios de cada empresa individualmente e detectar quais as características, desafios e necessidades em comuns entre elas com intuito de fazer uma observação sobre os problemas que são enfrentados neste segmento.

Subsequente ao diagnóstico realizou-se uma modelagem estruturada a partir das necessidades e dificuldades encontradas dentro do ambiente das micros e pequenas empresas na etapa de levantamento.

1.4 Organização do trabalho

Este trabalho, além desta introdução, está dividido em cinco capítulos e um anexo.

- O capítulo 2 apresenta definições sobre a segurança da informação e seus componentes, pilares, técnicas, ferramentas e as diretivas mais importantes presentes na norma ISO/IEC 27001;
- O capítulo 3 trata da gestão da infraestrutura, e portanto os aspectos relevantes de presentes no ITIL, bem como as questões de segurança direcionadas à infraestrutura, tais como, tipos de vulnerabilidades quesão apresentadas neste capítulo;
- O capítulo 4 apresenta a problemática da segurança da informação em MPEs, apresentando o levantamento realizado nas MPEs de tecnologia no Vale do Araranguá. Neste capítulo são analisados os dados obtidos;
- Conclusão do trabalho realizado através da investigação teórica das normas internacionais e pela pesquisa realizada com as MPEs; e indicados trabalhos futuros que podem ser desenvolvidos e,
- Referências bibliográficas e os anexos.

.

2 SEGURANÇA DA INFORMAÇÃO

Segundo o dicionário Michaelis o termo segurança significa: “Um conjunto de ações e recursos que são utilizados para proteger algo ou alguém, é algo que serve para diminuir os riscos e os perigos”. Ou seja, segurança é ter a certeza de algo estável.

Em redes de computadores o termo segurança refere-se à proteção contra acessos indevidos de usuários não habilitados a um sistema, programa ou rede de computadores

(TANENBAUM, 2011). Assim sendo, faz referência à implementação de métodos, de políticas de prevenção, do monitoramento do acesso, do uso incorreto ou modificação não autorizada dos recursos que compõe esse sistema.

Os sistemas computacionais, atualmente, possuem uma interligação através de uma infraestrutura de redes, onde também se atribuem os métodos de controle de dados, autorização de acesso, e autenticação de usuários.

Segundo (TANENBAUM, 2011), uma rede de computadores é definida como:

> "um conjunto de módulos processadores capazes de trocar informações e partilhar recursos, interligados por um subsistema de comunicação, ou seja, é quando há pelo menos dois ou mais computadores e outros dispositivos interligados entre si de modo a poderem compartilhar recursos físicos e lógicos."

No cenário computacional o conceito de segurança está atrelado ao termo rede de informações, por isso é importante que sejam levantados alguns questionamentos que ajudam na fundamentação sobre a segurança computacional, são eles: "O que você está tentando proteger? Por que você está tentando proteger? Como você vai protegê-lo?" (RHODES-OUSLEY, 2013). Após a exposição destes questionamentos é importante conhecer e entender o valor agregado à informação. Segundo ABNT (2005), "A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios." A mesma ainda expõe que a segurança da informação pode "Ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado".

Visto isso fica claro que a segurança de âmbito computacional para as organizações não se encaixa apenas como uma necessidade, mas sim como uma vantagem competitiva.

2.1 Pilares e Princípios da segurança da informação

De acordo com Rhodes-ousley (2013) "A segurança da informação tem como preocupação a proteção da informação em todas as suas formas seja escrita, falada, eletrônica, gráfica, ou usando outros métodos de comunicação. Já a segurança da rede está preocupada com a proteção de dados, hardware e software em uma rede de computadores".

Até agora foi tratado a segurança em rede de computadores como um conjunto de métodos, procedimentos e políticas que protegem uma rede computacional que possui dados. Estes dado nada mais são que um amontoado de bits organizados, que formam a informação que é o resultado da organização destes dados.

Em redes de computadores, pacotes ou datagramas são caracterizados como uma estrutura de transmissão desses dados que são enviados através de um sistema de comunicação chamada de redes de Internet que é onde a informação normalmente é quebrada em inúmeros pacotes e então transmitida.

Em meio a este processo entre remetente e destinatário esses pacotes repletos de informação podem ser copiados, adulterados, perdidos ou roubados. E para prover segurança em redes de computadores dessas informações desde sua transmissão até a chegada ao destinatário há a necessidade de garantir algumas propriedades. (KUROSE, 2010) define quatro propriedades estreitamente interligadas:

- **Confidencialidade**, que tem como objetivo garantir que o conteúdo da mensagem seja entendido somente pelo remetente e destinatário, além de assegurar que em caso de interceptação da mensagem terceiros não sejam capazes de entender o conteúdo dela.
- **Autenticação**, o conceito da propriedade de autenticação engloba a ação de confirmação de identidade do usuário com o intuito de provar sua identidade, garantindo que o usuário é quem ele alega ser para assim confiar a mensagem a ele. Deste modo as mensagens são entregues somente aos usuários autorizados.
- **Integridade da mensagem**, garante a integridade da mensagem se encaixa na necessidade de assegurar-se de que o conteúdo da mensagem não seja violado durante seu trajeto de transmissão.
- **Disponibilidade**, garante que a informação esteja sempre disponível de forma segura para a utilização dos usuários autorizados.

Outro autor como Tanebaum (2011) inclui mais uma propriedade que se deve também garantir, o **não repúdio** que é definido por Bar (2003) como sendo "suficiente evidência para persuadir a autoridade legal à respeito de sua origem, submissão, entrega e integridade, apesar da tentativa de negação do suposto responsável pelo envio". Ou seja o **não repúdio** é o ato de impedir que o usuário negue a execução ou alteração de alguma ação ou dado.

Até então se sabe que a informação é o resultado da organização de dados, e se tornou um importante elemento que deve ser protegido. De acordo com (RHODES-OUSLEY, 2013) "A informação é um ativo importante. Quanto mais informações você tem em seu comando melhor você consegue se adaptar ao mundo ao seu redor. No mundo dos negócios, a informação é muitas vezes um dos bens mais importantes que uma empresa possui". Visto

isso, compreende-se a existência de mais um fator para a necessidade da segurança computacional.

Em uma visão global conforme Peltier (2013) é citado que a informação faz parte dos "Recursos valiosos de uma organização, tais como informações, hardware e software". E o mesmo acrescenta que "Segurança ajuda a organização a alcançar seus objetivos de negócio ou missão por proteger seus recursos físicos e financeiros, reputação, posição legal, funcionários e outros ativos tangíveis e intangíveis".

Sendo assim percebe-se que com o passar dos anos a informação tornou-se um ativo importante, um bem de valor não palpável, porém de extrema importância para as organizações. Com o aumento significativo do seu valor a informação está cada vez mais exposta a uma série de ameaças e vulnerabilidades que devem ser tratadas com resguardo.

A informação suportou diversos tipos de representação, ao longo dos anos. Com a explosão do uso e da difusão das tecnologias é inevitável pensar no que diz respeito à infraestrutura dessas tecnologias quando se trata do tráfego desses dados nos serviços disponíveis.

No aspecto de segurança desses serviços a linha de pesquisa voltada a informação tem que ser relacionada à proteção dos dados na rede, e na investigação e a aplicação de serviços de proteção das informações. Algumas dessas propriedades já foram acima mencionadas são elas: confidencialidade, autenticação, integridade da mensagem e segurança operacional além de outras que foram consideradas por outros autores como muito importantes, sendo elas o sigilo, e o não repudio.

2.2 Técnicas da segurança da informação

A segurança da rede começa no mais básico nível de segurança até ao mais complexo., Esse é um passo importante para garantir a não violação da rede. Segundo o Whashington Journal (2014), a segurança de rede envolve diversas áreas :

- Criptografia de chaves públicas;
- Vulnerabilidade em máquinas de sistemas distribuídos;
- Vulnerabilidade em rede local de grande escala;
- *Firewalls*
- Sistemas de detecção de intrusão;
- Redes privadas virtuais VPN's;

- Controle de roteamento;
- Assinatura digital;
- Autenticação;
- Controle de acesso;

Existem algumas políticas que podem ser feitas para garantir o acesso seguro de serviços e informações.

Segundo Quintao (2005) os conceitos de segurança devem seguir padrões que resolvam e preveem problemas, vendo isto, o mercado passou a agrupar os principais mecanismos de segurança utilizados são eles (YOURDON E., 2002):

1) Identificação do usuário e autorização de controle de acesso

É um mecanismo que parece ser ingênuo e às vezes até inofensivo mas é um passo extremamente importante para garantir a segurança e a confiabilidade da rede, este mecanismo garante que somente tenha acesso à rede de usuários cadastrados.

Esse mecanismo determina uma teia de acesso para cada nível de usuário, ou seja, nele é determinado quais conteúdos e serviços determinados usuários possuem permissão de acesso.

Atualmente para o controle de acesso a combinação *login* e senha já não é o suficiente para fazer a garantia da rede, são utilizados certificados digitais, biometria e outros tipos de mecanismos.

2) Proteção de dados armazenados

Este mecanismo diz respeito ao conceito de integridade da informação e a integridade da mensagem, no qual englobam questões de como a informação é armazenada seja física ou logicamente (*hardware*, nuvem, banco de dados).

Para que isso seja feito de maneira que não aconteça a quebra do conteúdo da mensagem. Por isso é preciso adotar alguns sistemas como o antivírus, e ou sistemas que fazem a autenticação e autenticidade da mensagem.

3) Proteção de dados em trânsito

Quando dados estão trafegando na rede eles correm riscos de serem perdidos, alterados, ou interceptados para que isso não aconteça existem alguns métodos que são empregados (YOURDON, 2002): Criptografia é a codificação da mensagem de forma que seja ininteligível para qualquer pessoa, a não ser para as que possuam a chave requerida para decodificar a mensagem em seu formato original.

Outro método de segurança é usado pra quando a informação é interceptada. È preciso, que haja a autenticação do usuário para que a mensagem só seja aberta caso haja a confirmação de que aquele usuário tenha permissão de acesso à informação.

4) Auditoria de acesso as informações

Auditoria é uma prática comum em empresas, onde um sistema mantem registros das atividades e transações realizadas pelos usuários do sistema. Através desse mecanismo o administrador pode ter um controle de dados e acesso, consegue perceber se existe algum usuário malicioso tentando acessar dados fora da sua teia de acesso. Tudo isso através da prática de manter registro e análise desses registros. (YOURDON, 2002)

5) Monitoramento de intrusos

Uma prática que envolve sistemas específicos, sistemas que fazem monitoramento de ataques. Esses sistemas fazem também analise e diagnóstico de vulnerabilidades já explicitadas anteriormente. Eles são responsáveis por avisar o administrador da rede se o sistema está sofrendo algum ataque, ou até mesmo fazer uma varredura nas portas para identificar anomalias, um comportamento inesperado ou alguma possível falha que possa levar a uma intrusão. (YOURDON, 2002)

2.3 Ferramentas para a prevenção de ataques

Existe uma série de ferramentas de prevenção de ataques, desde as mais básicas às mais complexas, dentre as quais estão: o *Firewall*, Criptografia, PKI *(Public Key Infrastructe)*, VPNs (*Virtual Private Networks*), Antivírus, e as menos usuais como scanner de vulnerabilidades, *packet sniffers*, assinaturas virtuais, certificados digitais, *scanner* de portas,

ferramenta de operação e detecção de sistema, e ferramentas de segurança em *wireless*, dentre essas, adiante será discorrido uma breve explicação das mais usuais (MICHAEL E. WHITMAN, 2011).

1) Firewall

De acordo com tradução livre da palavra, entende-se por *firewall* como sendo uma parede de incêndio. É, uma variação de parede que protege ou impede que um incêndio se alastre para outro lugar, a partir disto é possível entender o conceito básico de funcionamento do *firewall*, que é basicamente bloquear, isolar algo,de um sistema ligado a uma rede de computadores.

De acordo com Michael E. Whitman (2011) "Um *Firewall* em um programa de segurança da informação é similar a uma parede de incêndio de um edifício, no qual evita que tipos específicos de informações se movam para redes não confiáveis". Em suma o *Firewall* é uma entidade que protege a rede interna, de agentes externos. Como explicitado na figura 2.

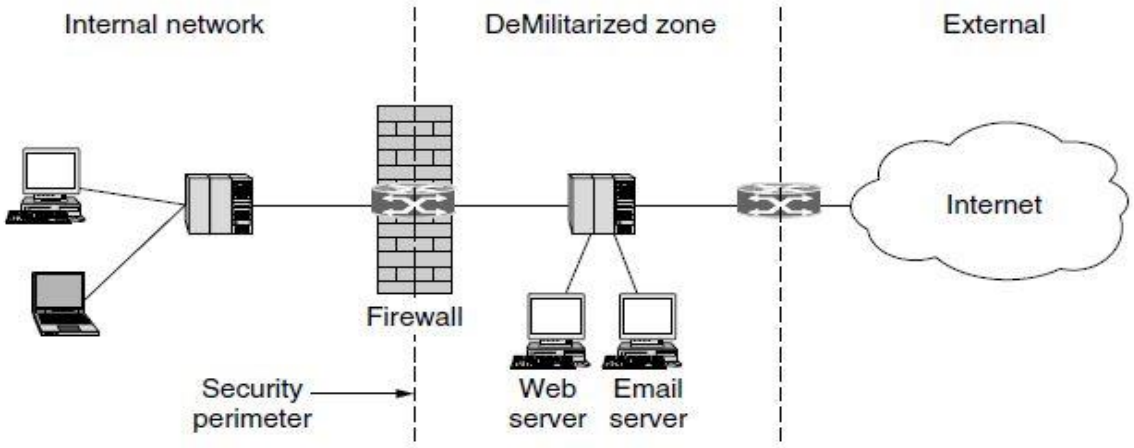

Figura 2 Demonstração da funcionalidade de um *Firewall*
Fonte: Tanenbaum 2011

2) Criptografia e infraestrutura de chaves públicas- PKI

Dentro do tráfego de uma rede, garantir que sua mensagem não seja interceptada é extremamente custoso e inviável.

Para que uma informação interceptada não se torne um problema, ou viole as propriedades básicas da segurança, utiliza-se a infraestrutura de chaves públicas que é um método de criptografia e protocolos que transformam a mensagem em cifras que sem a chave correta para decifrá-las não é possível lê-la ou entendê-la.

O método PKI é composto por chaves e certificados digitais “Infraestrutura de chave pública é um sistema integrado de software, metodologias, criptografia, protocolos, acordos legais, e serviços de terceiros que permitem que os usuários se comuniquem de forma segura.” Desta forma, garante a segurança da informação já que o usuário final somente conseguirá acessar a mensagem se possuir a chave de acesso (MICHAEL E. WHITMAN, 2011).

3) Redes privadas virtuais - VPN

A Rede privada é uma infraestrutura capaz de utilizar uma rede privada utilizando o tráfego e comunicação de dados de uma rede pública, por ser uma tecnologia que une redes privadas, criptografia e conexões ponto a ponto, que atrelados formam a VPN, ela garante uma combinação de acesso seguro ponto a ponto com uma rede de internet pública.

Uma das vantagens da VPN é conectar todos os pares com firewalls e túneis utilizando a Internet. Como demonstrado na figura a seguir (TANENBAUM, 2011)

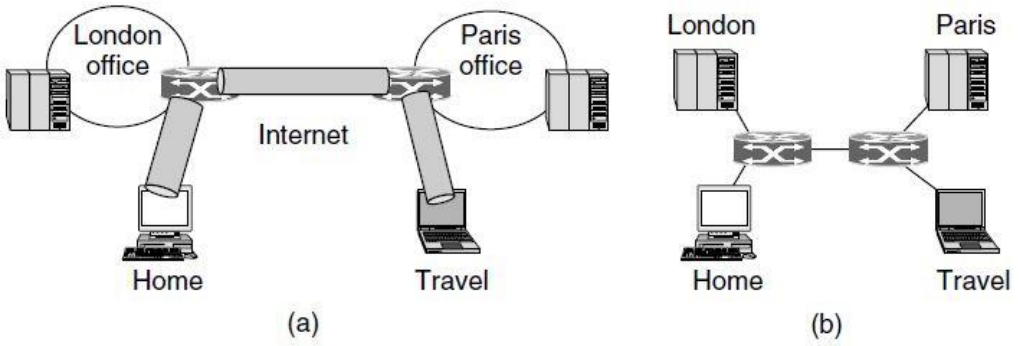

Figura 3. Demonstração de uma VPN.
Fonte: Tanenbaum 2011

2.4. Normas do sistema de gestão de segurança da informação ISO/IEC 27001

De valor inegável uma norma de certificação acrescenta no domínio de gestão de empresas, novas certificações que vêm surgindo e se tornando práticas obrigatórias nesse mercado competitivo.

É possível destacar diversas características e singularidades que a implementação de uma norma de certificação pode trazer para uma organização, algum dos benefícios segundo (TSO, I., 2012) desse processo é definido como “Uma grande oportunidade para impulsionar a imagem da organização; aumento da satisfação dos clientes; mudança de foco da correção

para a prevenção; mobilização em torno de um objetivo comum; redução de desperdícios e custos". O mesmo também acrescenta:

> A certificação configura uma forma de organização empresarial – de se colocar as coisas nos seus devidos lugares de maneira sistêmica; ajuda as companhias a entender o que se passa internamente e, de certa forma, orienta no tratamento dos processos e ações que devem ser executados para que não conformidades não ocorram novamente." (TSO, I., 2012)

Baseando-se nessa avaliação fica claro que as normas e certificações são práticas de competitividade no panorama atual das organizações, segundo a própria (VERHEIJEN, 2008) "O sistema de gestão de segurança da informação é uma decisão estratégica para uma organização", a mesma também afirma que essa norma "Foi preparada para estabelecer e implementar requisitos que mantenham e melhore continuamente o sistema de segurança da informação".

Surgindo em 1989 nos primórdios do comércio e indústria do Reino Unido, através das necessidades de um código de boas práticas do departamento de comércio britânico (MOURA, 2007); e a partir dai se transformou na família *ISMS (Information Security Management System)* que consiste nas seguintes normas internacionais:

> ISO/IEC 27000, Information security management systems — Overview and vocabulary
> ISO/IEC 27001, Information security management systems — Requirements
> ISO/IEC 27002, Code of practice for information security controls
> ISO/IEC 27003, Information security management system implementation guidance
> ISO/IEC 27004, Information security management — Measurement
> ISO/IEC 27005, Information security risk management
> ISO/IEC 27006, Requirements for bodies providing audit and certification of information security
> management systems
> ISO/IEC 27007, Guidelines for information security management systems auditing
> ISO/IEC TR 27008, Guidelines for auditors on information security controls
> ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
> ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
> ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000‑1
> ISO/IEC 27014, Governance of information security
> ISO/IEC TR 27015, Information security management guidelines for financial services
> ISO/IEC TR 27016, Information security management Organizational economics (OGC, 2014)

2.4.1 ISO/IEC 27001

Segundo Moura (2007) a modelagem de especificações inclui requisitos de controle de segurança personalizado para que seja adaptável para as características e exigências de cada organização e suas partes competentes.

Busca trazer como parâmetros de resposta métodos que implementam, operam, monitoram, revisam, mantem e melhoram o sistema de gestão documental da segurança da informação (ISMS ou SGSI).

Dentro da organização é uma característica bem específica de acordo com Moura (2007): "O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionais que protegem os ativos de informação e dá confiança às partes interessadas". Além desta norma ter como base a política organizacional a implementação da segurança, também foi projetada para ser flexível e como resultado introduziu o modelo cíclico "*PLAN-DO-CHECK-ACT*" (PDCA), nos quais a etapa de planejamento define políticas, processos, objetivos, metas e procedimentos considerados importantes para a gestão de risco e desenvolve os processos de segurança da informação para assim atrair resultados consistentes com os objetivos organizacionais.

Subsequente ao planejamento (*Plan*) é a etapa de fazer (*Do*), que possui como objetivo a implementação dos processos, procedimentos e políticas definidos na etapa de planejamento, para assim na etapa de checagem (*Check*) no qual é feito um balanço de ações corretivas para que por fim na etapa de agir (*Act*) seja garantido que existam ações preventivas e de melhoria baseados nas implicações resultantes do processo de auditoria interna para que assim haja contínua melhoria do processo de gestão da ISMS (CAMPONAR, 2004).

As variáveis das práticas organizacionais serão apresentadas nas seções posteriores, elas se referem às operações que devem ser adotadas e que implicam em uma estrutura que facilitam o planejamento, interação, detecção de problemas e uma gestão funcional e responsável dentre outros inúmeros benefícios que essas boas práticas podem agregar a uma organização. Para o melhor entendimento deste ciclo segue a figura 4 que ilustra os processos envolvidos dessas práticas agrupadas pelo padrão PDCA.

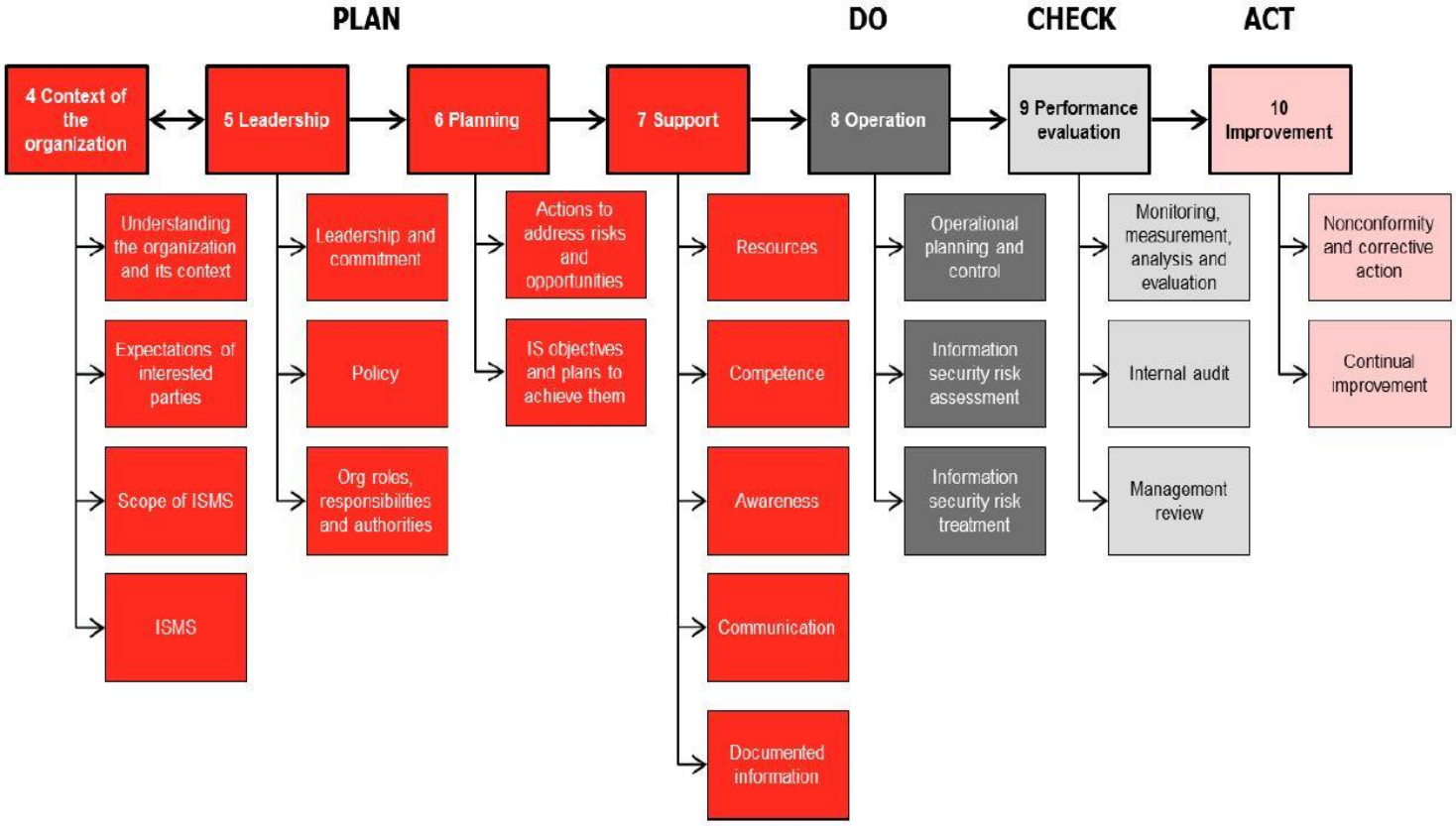

Figura 4. Estrutura dos processos agrupados pelo padrão PDCA.

Fonte: Bsi 2013

2.4.1.1 Requisitos de contexto organizacional

A ISO pode ser aplicada em qualquer ambiente organizacional, contando que esse contexto seja devidamente respeitado.

Para que a norma seja implementada de maneira correta, é necessário estabelecer níveis de entendimento sobre a organização e seu sobre contexto na qual a mesma será inserida. Devem estar claros quais os objetivos, metas e a natureza da organização e seu papel dentro de sua conjuntura como organização.

Logo nos primeiros tópicos da regulamentação é documentado que se deve entender e determinar sobre as questões internas e externas que são importantes como propósito da organização e que ao mesmo tempo podem impactar na capacidade funcional de atingir o êxito no sistema de gestão da segurança da informação (ISO/IEC, 2013). É proposto em sequência que após compreender o propósito da organização é importante alinhá-los aos procedimentos estabelecidos pela norma de modo que os padrões e processos do sistema estejam sincronizados em prol da organização.

O próximo item mencionado dentro desse contexto seria a necessidade de compreender as expectativas das partes interessadas. É importante determinar quais são as partes interessadas que são relevantes e quais os requisitos legais e/ou regulamentares das mesmas. E então, após a determinação de todas essas questões, é preciso, determinar os limites e aplicabilidade do sistema de gestão da segurança da informação e para determiná-lo será preciso dois elementos citados anteriormente, como as questões externas e internas e os requisitos.

Ao determinar esse escopo, a organização também deve considerar a determinação de interfaces e vínculos de seus métodos e atividades com outras organizações, deve ser feito uma documentação sobre as informações do escopo que precisam incluir quais as atividades são realizadas pela organização e quais são realizadas por outras organizações, além de também incluir dados sobre as determinações feitas no discorrer deste tópico, e por fim a organização precisa estabelecer, implementar, manter e melhorar continuamente o sistema de gestão da segurança da informação (ISO/IEC, 2013).

A ISO 27001 separa seus processos de boas práticas através de contextos, que serão abordados um por um na próxima seção.

2.4.1.2 Contexto de liderança

1) Liderança e compromisso

Dentro deste contexto a norma expõe que a liderança e a alta administração devem demonstrar seu compromisso com a o sistema de gestão de segurança através dos seguintes argumentos:

> - Garantindo que os objetivos da política de segurança da informação estejam estabelecidos;
> - Assegurando a integração dos requisitos do sistema de gestão de segurança da informação nos processos da organização;
> - Assegurando que o recursos necessários para o sistema de gestão de segurança da informação estejam disponíveis;
> - Comunicando sobre a importância de uma gestão eficaz de segurança e de conformidade com os requisitos do sistema de gestão de segurança da informação;
> - Garantindo que o sistema de gestão de segurança da informação atinja seu(s) resultado(s) pretendido(s);
> - Dirigindo e apoiando as pessoas a contribuir para a eficácia do sistema de gestão da segurança da informação;
> - Promovendo a melhoria continua;
> - Apoiando outros aspectos relevantes;
> (ISO/IEC, 2013).

2) Políticas

Neste tópico observa-se na norma que é explicitado a necessidade de que a alta administração estabeleça as políticas de segurança que devem seguir algumas condições,

> "Devem ser apropriadas junto ao propósito da organização; devem incluir os objetivos da segurança da informação além de fornecer as definições dos objetivos; inclui também um compromisso para satisfazer as exigências aplicáveis" além dessas condições as políticas de segurança devem satisfazer essas qualidades, e estar disponíveis e documentada; além de estar disponível para as partes interessadas e ser aberta dentro da organização (ISO/IEC, 2013).

3) Papéis organizacionais, responsabilidades e autoridades.

Neste tópico é tratada a importância da alta gestão garantir que sejam atribuídas autoridades e responsabilidades aos papéis e funções importantes da gestão da informação.

Dentro deste tópico a norma expõe que é importante delegar responsabilidades de autoridade para "Assegurar que o sistema de gestão de segurança da informação está em conformidade com os requisitos da presente regulamentação; elaboração de relatórios sobre o desempenho do sistema de gestão de segurança da informação para a alta administração"(ISO/IEC, 2013)

Visto isso, é importante que fique claro o papel de cada um na gestão da segurança da informação.

2.4.1.3 Contexto de Planejamento

1) Ações para enfrentar os riscos e oportunidades

Este contexto trata de estabelecer objetivos de segurança da informação orientadas para a *ISMS (Information Structure Management System)* é um parâmetro importante quando se trata das habilidades que a organização precisa considerar.

O planejamento é imprescindível e nele devem ser considerados os requisitos determinados no contexto organizacional, que devem ser coerentes em sua totalidade e competências.

Esses parâmetros devem estar alinhados a um ponto em que aconteça uma linha de coerência que leve em consideração ambos os lados, dos riscos e oportunidades e o contexto organizacional.

A norma neste contexto relaciona as seguintes práticas "Garantir que o sistema de gestão de segurança da informação possa atingir o seu resultado pretendido; prevenir, ou reduzir, efeitos indesejados; alcançar a melhoria continua". E ainda ressalta que a organização deve realizar um planejamento de como lidar com riscos e oportunidades e assegurar a integração da implementação de ações na *ISMS* além de avaliar a eficácia dessas ações (ISO/IEC, 2013).

2) Avaliação de riscos de segurança da informação

A avaliação de riscos de segurança da informação é uma forma de tratar esse risco, O departamento de segurança e Comunicações (2013) afirma que a gestão desses processos é um "Conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação".

A partir disso fica evidente que a avaliação de um panorama dessas competências de avaliação também é um dos processos tratados na norma, nela é descrito que a organização deve definir e aplicar um processo de risco de segurança a informação e que é necessário estabelecer critérios de risco e segurança.

Dentro destes critérios estão incluídos os seguintes componentes (ISO/IEC 27001, 2013): Aceitação de risco; realização de avaliações de risco; garantir que avaliações de riscos repetidas sejam feitas para uma verificação consistente em uma comparação de resultados, assim como identificar os riscos de segurança da informação e avaliar os processos, e identificar a perda da confiabilidade, integridade e disponibilidade no âmbito SGSI; avaliar as potenciais consequências que resultariam se os riscos que forem identificados incidirem, avaliar a probabilidade da ocorrência desses riscos, determinar e identificar o nível desses riscos, comparar os resultados em analise de risco e fazer uma analise de critério e prioridade.

Cada um desses processos são importantes e devem ser documentados em cada passo de avaliação dos riscos conforme é explicitado pela norma.

3) Tratamento de riscos de segurança da informação

Segundo a norma ISO/IEC 27001 (2013) deve-se direcionar a organização na definição e aplicação do processo de tratamento de riscos de segurança da informação. Do mesmo modo como a avaliação dos riscos é um tópico importante do processo, a mesma seria de completa inutilidade sem o tratamento de tal. Os requisitos para o tratamento que são abordados são amplos e bem definidos. A seguir são mencionados os tópicos citados pela norma que são julgados importantes:

> A) Selecionar opções de tratamento de riscos adequadas, tendo em conta o risco e os resultados da avaliação;
> B) Determinar todos os controles que são necessários para implementar o tratamento de riscos de segurança da informação.
> C) Comparar os controles determinados nos tópicos acima.
> D) Produzir uma declaração de aplicabilidade que contém os controles necessários, e justificativa para implementações ou exclusões.
> E) Formular um plano de tratamento de riscos de segurança de informação.
> Obter aprovação do plano de tratamento de riscos de segurança da informação e aceitação da informação residual dos riscos de segurança, bem como manter toda essas informações documentadas e armazenadas (ISO/IEC, 2013).

4) Objetivos de segurança da informação e planejamento para alcançá-los.

Já foi mencionado que é preciso analisar o contexto em que a organização se encontra e suas competências para que as boas práticas de *ISMS* estejam alinhadas com o contexto organizacional, pois isso traz mais coerência e conformidade ao *ISMS*.

Neste tópico a ABNT NBR ISO/IEC 27001 (2013) expõe que os objetivos de segurança da informação devem ser consistentes com a política de segurança, bem como suas etapas para alcança-los, desta forma os requisitos de aplicações de segurança da informação, e os resultados da avaliação servirão de pontos de avaliação do processo.

Outro ponto muito importante é a comunicação, que é utilizada para que esses requisitos e objetivos devam ser passados adiante, e que devem estar em constante atualização, mantendo estas práticas sempre documentadas, para assim então após o estabelecimento dos objetivos planejar como alcançar esses objetivos e determinar passos bem definidos, para servir como exemplo, de como será feito, quais recursos serão necessários, quem será o responsável, o tempo de conclusão, como será avaliada no término, se os objetivos foram alcançados em sua totalidade e se houve atrasos. Esses são os

tratamentos de uma fase de consolidação das práticas do processo que deve estar estruturada e adequada ao padrão internacional.

2.4.1.4 Contexto de suporte

1) Recursos

Neste tópico é importante uma rede que disponibilize instâncias, componentes e recursos que satisfaçam às necessidades dos processos *ISMS*.

A descoberta ou disponibilização de recursos devem ser projetados para considerar um domínio de aplicação específico e deve ser sensível às melhorias contínuas, e de acordo com seu objetivo em seu contexto, a norma afirma como sendo importante "Determinar e prover recursos necessários para a criação, implementação, manutenção e melhoria contínua do sistema de gestão de segurança da informação". (ISO/IEC, 2013)

2) Competências

Neste requisito é proposto uma relação entre as competências dos recursos humanos disponíveis. Portanto é preciso se certificar que os colaboradores estão de acordo e que possuem competências necessárias para a realização de seu papel para que não afete o desempenho organizacional e da segurança da informação. Além de garantir que esses colaboradores estão sendo treinados, e entendendo os princípios e "o por que" dos padrões, se eles estão sendo educados para entender as questões das boas práticas. Outro princípio importante é a documentação como prova de competência e como ação aplicável de transferência de competências.

Este tópico tem ênfase no conteúdo, a norma nos direciona para que haja estímulos de comunicação entre as partes envolvidas, para que os requisitos de gestão de documentos sejam atendidos o que exige que a informação tenha que ser documentada. (ISO/IEC 27001, 2013).

3) Consciência

A consciência dos colaboradores da organização é o assunto tratado e com suma importância neste tópico, controlar esses ativos é garantir que padrões, normas e políticas estão sendo cumpridos.

Nele é assegurado que cada um está cumprindo seu papel conscientemente e contribuindo para a eficácia do *ISMS* e entendo quais as implicações e inconformidades são resultantes no *ISMS* caso esses requisitos não sejam atendidos. (ISO/IEC 27001, 2013).

4) Comunicação

Neste requisito é tratado sobre como é determinado a organização da necessidade de comunicação interna e externa relevantes para o *ISMS*.

De acordo com a (ISO/IEC 27001, 2013) devem ser incluídos os seguintes objetos na determinação da comunicação: "No que se comunicar; quando se comunicar; com quem se comunicar; em quais processos pelos quais a comunicação deverá ser efetuada". Para que se garanta um bom ciclo de comunicação entre as partes interessadas.

5) Documentação da informação

Manter uma documentação concisa que está em alinhamento com normas e com as informações necessárias da organização para que garanta sua eficácia é um fator importante que traz impactos no *ISMS* de uma organização. Uma boa documentação elimina brechas de má interpretação ou dúvidas, e aumenta o grau de entendimento sobre o assunto documentado.

Ao discorrer os tópicos anteriores relacionados nota-se que a norma exige em grande parte dos processos de boas práticas que se mantenha uma documentação. A partir disso é possível enxergar a importância que a documentação carrega quando o assunto é boas práticas no contexto *ISMS*. A norma (ISO/IEC 27001, 2013) é clara e sucinta sobre este assunto, ela solicita que a documentação seja criada e que esteja sempre atualizada, e também que a organização deve se assegurar de que haja uma descrição detalhada de identificação (título, data, autor, número de referência) e se mantenha um formato padrão de documentação e que passe sempre por uma análise e aprovação antes de sua publicação.

Existe um tópico que fala sobre o controle dessas informações documentadas onde é exigido que a documentação esteja propriamente disponível porém adequadamente protegida,

também é ressaltado os seguintes parâmetros: deve-se assegurar o controle de informações documentadas através das atividades seguintes: “distribuição, acesso, recuperação e uso; armazenamento e conservação, incluindo a preservação da legibilidade; controle de alterações; retenção e descarte” (ISO/IEC 27001 2013).

2.4.1.5 Contexto de Operação

Uma operação é obra de um agente ou de um poder que realiza a execução metódica, de forma sistemática em um objeto ou processo. A ISO/IEC 27001 (2013) aponta o controle deste processo de operações como uma diretriz importante no manual de boas práticas. Esse controle pode ser enxergado como uma fase desse processo no qual a organização deve planejar, implementar e controlar tudo que engloba e impacta de alguma forma a segurança da informação.

Neste tópico a regulamentação trata a implementação como um plano para alcançar objetivos citados nos tópicos de ações para enfrentar riscos e oportunidades e nos objetivos e planos para alcançá-los. Dentro deste plano operacional e de controle são exigidos ações que confirmem que os processos foram realizados de forma consistente de acordo com o que foi planejado, além de manter as informações documentadas para assegurar-se de tal. Outra medida de controle que é citado é sobre o controle de processos terceirizados que devem ser devidamente controlados. Ainda dentro deste foco de controle, é exigida então a contenção de mudanças planejadas e que se avalie tanto as consequências involuntárias quanto seus efeitos adversos e por fim que se tome medidas para minimizar esses efeitos quando necessário. (ISO/IEC 27001, 2013).

Também é descrito o resgate do levantamento dos objetivos e dos planos para alcançá-los. Partindo do tópico anterior que discorre sobre os riscos, é necessário que a partir deles, a organização considere a realização de avaliações desses riscos em intervalos de tempos pré-determinados ou quando mudanças significativas incidirem e sempre manter todas as informações resultantes deste processo documentada.

E por fim manter um plano de tratamento desses riscos e reter informações dos resultados da segurança destes tratamentos. Em resumo devem ser planejadas e, controladas e avaliadas as operações necessárias para atender aos requisitos do *ISMS*. As operações expostas pela norma foram (ISO/IEC 27001, 2013):

- Manter documentos de manutenção;
- Realizar a gestão de mudanças;

- Responder a eventos adversos;
- Fazer o controle de todos os processos terceirizados;
- Planejar o controle de operações;
- Realizar a avaliação de riscos e intervalos pré-determinados;
- Implementar um plano de tratamento de riscos de segurança.

Essas são as ações que são consideradas variantes de boas práticas no requisito de operações tratadas com grande importância no processo de controle dos requisitos de operações que é exposto pela regulamentação. Deste modo é importante salientar que é um contexto que avalia todos os efeitos e consequências, com intuito de entendê-las e minimizar tais consequências quando necessários.

2.4.1.6 Contexto de avaliação de desempenho

1) Monitoramento, medição, análise e avaliação

Segundo a norma, a avaliação de desempenho e sua eficácia no sistema SGSI, alguns tópicos são determinados para que a organização os preencha, consistem eles em: o monitoramento de métodos e medição de processos e controles e segurança, quando o monitoramento e medições devem ser efetuados, o que deve ser medido e quando os resultados devem ser analisados e avaliados, e o que deve ser avaliado, além de que deve ser garantido que através destas medições os resultados sejam comparáveis, válidos e reproduzíveis, e que a diagnóstico dos resultados e medições seja provada na documentação (ISO/IEC 27001, 2013).

2) Auditoria interna

O processo de auditoria interna é um método chave para avaliar e acompanhar o desempenho do *ISMS*.

Através dela é possível verificar desempenho de processos e ferramentas para auxiliar em sua melhoria contínua. É documentado pela norma com as seguintes determinantes:

> "Estar de acordo com as necessidades da organização para seu sistema de gestão de segurança da informação; seja efetivamente implementado e mantido; planejar, criar, aplicar e manter um programa de auditoria,

> incluindo a frequência, métodos, responsabilidade, necessidades de planejamento e relatórios, levar em consideração a importância dos processos em causa e os resultados anteriores; definir os critérios de auditoria e possibilidades de cada auditoria; selecionar auditores e assegurar sua imparcialidade e objetividade; garantir que os resultados sejam notificados aos órgãos pertinentes; reter informações documentadas como prova dos resultados do programa de auditoria". (ISO/IEC 27001, 2013)

Esses são os princípios determinantes esclarecidos, além disso, é explicitado de maneira clara e objetiva que é uma prática importante que traz respostas e resultados de avaliação que se feitas de maneira adequada conduzem a grandes resultados e impactam na qualidade da *ISMS*.

3) Gestão de avaliação

Neste tópico cabe a alta a administração garantir a contínua pertinência, adequação e eficácia dos tópicos anteriores e de qualquer alteração nas questões externas e internas.

Os tópicos abordados que garantem esses parâmetros foram os seguintes: "A avaliação de gestão deve incluir e considerar (ISO/IEC 27001, 2013): o estado das ações das análises críticas anteriores; mudanças nas questões externas e internas que são relevantes para a gestão da segurança da informação; *feedback* sobre o desempenho de segurança da informação".

Além disso, devem ser incluídos e realizados *feedback* sobre o desempenho do resultado de processos dos tópicos anteriores, como os de "não conformidade e ações corretivas; auditoria; monitoramento e medição; cumprimento dos objetivos de segurança da informação; o feedback das partes interessadas; os resultados dos riscos; do status do plano de tratamento de riscos e as oportunidades de melhoria continua".

Esses são requisitos que são abordados neste tópico que garantem a pertinência, e eficácia das operações e da gestão de *ISMS*.

2.4.1.7 Melhorias

O tópico final trabalha requisitos que abordam a não conformidade e medidas corretivas.

Ele discorre sobre como a organização deve reagir a qualquer não conformidade identificada e tomar medidas corretivas e de controle, lidar com as consequências, avaliar a necessidade de medidas para eliminar essas ocorrências.

Outro processo mencionado é o de fazer um estudo que determine essas causas e se existem similaridades em outros processos, implementar alterações e ações corretivas quando

necessário, avaliar sua eficácia e documentar o caráter dessa inconformidade, bem como, as causas, consequências e ações tomadas subsequentemente, assim sendo, a organização deve buscar através dessas boas práticas buscar a melhoria contínua, reagindo sempre a inconformidades, as corrigindo e adequando para que torne o *ISMS* mais eficaz (ISO/IEC 27001, 2013).

3 A INFRAESTRUTURA DA TECNOLOGIA DA INFORMAÇÃO

O termo infraestrutura conforme (G. C. BOWKER 2010): "Evoca vastos conjuntos de equipamentos coletivos necessários para as atividades humanas, tais como edifícios, estradas, pontes, trilhos, canais, portos e rede de comunicações". O autor também acrescenta que "Além de tijolos, argamassa, tubos ou cabos, infraestrutura abrange também as entidades mais abstratas como os protocolos (humanos e computacionais), normas e memória". Como foi definido acima pode-se concluir que a infraestrutura de suporte a informação envolve recursos diversos.

No âmbito computacional a infraestrutura da informação é definida pela NFS (2006) como sendo uma "*Cybe*r infraestrutura que integra hardware de computação, redes de dados, sensores digitalmente habilitados, observatórios de instalações experimentais, um switch Inter operável de software e serviços de middleware e ferramentas". Com isso fica evidente que uma estrutura segura em uma organização não envolve somente um único componente, mas sim um conjunto de elementos.

Em uma organização existem diversos fatores que contribuem para uma boa infraestrutura e política de segurança.

Atualmente os computadores, celulares e as pessoas são responsáveis pelo processamento da maioria das informações operacionais de uma organização, por isso a proteção dos dados circulados nesses dispositivos e a conscientização dos deveres e responsabilidades dos colaboradores possui um papel fundamental na proteção dos dados de uma organização. Sendo assim a estrutura principal da segurança computacional segundo (E. H. DINIZ, 2010) É definida em camadas: a camada física, camada lógica e camada humana que atendem às demais características:

A camada física é composta pelo ambiente em que os equipamentos e periféricos estão fisicamente, residência ou escritório do usuário, ou ainda no espaço público de um cybercafé, escola, biblioteca. É o local onde está instalado o hardware – computadores,

servidores, o meio de telecomunicação utilizado – linha de conexão e de transmissão. (HARRIS, 2002)

A camada lógica, segundo E. H. DINIZ (2010), que apresentou sua ideia de segurança da informação voltada a aplicativos de Internet Banking: "A camada lógica é composta por programas e aplicativos que podemos denominar softwares. Esta camada é o "cérebro" do Internet Banking, na qual estão as regras, normas, protocolos de comunicação e onde, efetivamente, ocorrem as transações e consultas". Como explicado na citação podemos estender a ideia não somente para o contexto do Internet Banking, quando assumido que qualquer organização pode implementar o contexto de infraestrutura de camadas física, lógica e humana na segurança da informação.

A camada humana que foi definida de acordo com E. H. DINIZ (2010) como sendo "Composta pelo recurso humano, envolvido no processo, desde o analista responsável pela programação técnica; o operacional, que cuida da infraestrutura; a gerência e diretoria que administram o canal; até o cliente, seu usuário final".

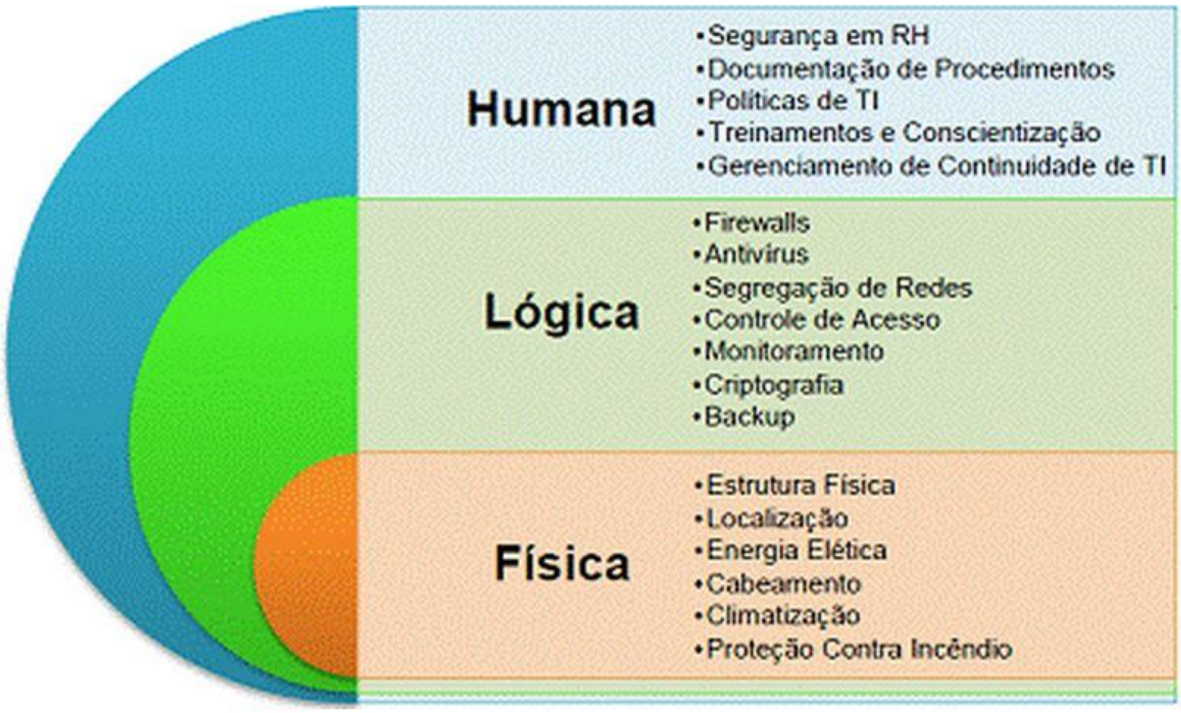

Figura 5. Esquema de camadas da estrutura da segurança da informação.
Fonte: Teleco 2012

Quando o assunto é a infraestrutura desses meios computacionais foi visto anteriormente que a segurança de dados em rede deve ser feita a partir do meio lógico, através de aplicações de segurança, e seguir para o âmbito físico e humano.

Quando se cria uma estrutura da segurança de dados somente no meio lógico implica-se em uma segurança básica com aplicações médias e com alto risco de incidentes de

segurança. Para se possuir uma estrutura completa foi exposto que deve se aderir aos aspectos: físicos, que podem envolver desde acesso limitado em salas, escritórios, arquivos e datacenter, acesso controlado, câmeras de monitoramento e policiamento ao aspecto humano.

O maior problema atualmente quando se trata de segurança, que de acordo com SCHNEIER; VIEIRA (2001, apud DINIZ 2010) são os recursos humanos. "É o elo mais fraco na corrente da segurança, sendo, cronicamente, responsável pela falha dos sistemas de segurança". O autor também adiciona que "os aspectos importantes desta camada são a percepção do risco pelas pessoas: como elas lidam com os sinistros que ocorrem raramente; se são usuários confiantes ou ignorantes no uso do computador; o perigo dos intrusos maliciosos ou ingênuos".

Sabendo disso e entendendo os riscos como eles são, a infraestrutura da segurança deve envolver todos os aspectos vulneráveis abordados, com a finalidade de prover uma composição de agentes que tornam a estrutura mais segura para a informação.

3.1 ITIL

A biblioteca de infraestrutura da tecnologia da informação mais conhecida como ITIL é um conjunto de práticas que foi desenvolvida na Inglaterra pela OGC (*Office Government of Commerce*) na década 1980, seu principal conceito é descrever as melhores práticas quando se trata do processo de gestão de tecnologias da informação.

"Boas práticas podem ser um sólido apoio para as organizações que querem melhorar seus serviços de TI." (VERHEIJEN, 2008) E como explicitado a ITIL (*Information Technology infrastructure Library*) é considerada como um conjunto de boas práticas.

É um padrão reconhecido mundialmente como uma fonte confiável das melhores práticas de *ITSM (Information Technology Service Management)*, é descrita por Tso (2012) como sendo uma importante estrutura que possui técnicas de gerenciamento de serviços e controles de gestão.

O autor ainda acrescenta que a ITIL "Centra-se na medição contínua e melhora da qualidade do serviço de TI prestado, tanto na perspectiva de negócio quanto na do cliente". Dentro desta perspectiva a ITIL destaca que é importante perceber as principais contribuições que essa infraestrutura agrega a uma organização, sendo elas (TECHEXCEL, 2012):

- Melhoria dos serviços de TI;
- Diminuição dos custos;

- Melhoria na satisfação do cliente através de uma abordagem mais profissional de prestação de serviços;
- Melhoria da produtividade;
- Melhoria da utilização das competências e experiência;
- Melhoria da prestação de serviço de terceiros.

Outro autor (TSO, 2012) complementa que a governança ITIL produz maior disponibilidade de serviço, o que diretamente impacta no aumento da lucratividade, e também melhora o processo de tomada de decisão o que conduz à diminuição dos riscos. Arraj (2013) também destaca os benefícios que a abordagem ITIL deposita na organização:

> **Alinhamento com as necessidades da empresa** a ITIL torna-se um trunfo para o negócio quando uma organização de TI Recomenda proativamente soluções como uma resposta a uma ou mais necessidades de negócios. Ela é recomendada pois possui uma característica que provê oportunidade de entender as necessidades atuais e futuras do negócio além de desenvolver ofertas de serviços que consigam resolvê-los.
> **Negociação de níveis de serviço de negócios,** esse é um quesito onde a ITIL possui um poder de transformar o negócio e o provedor de serviços em parceiros, e quando acontece este alinhamento, torna-se possível essas duas variantes entrarem em comum acordo com intuito de aliar em nível de serviço, as necessidade com os custos acessíveis
> **Expectativas previsíveis e processos consistentes** A aplicação de processos previsíveis e de forma consistente conforme a ITIL recomenda, produz uma conformidade e uma facilidade de atender as expectativas do cliente, Ao mesmo tempo, também é possível aliar aos processos de boas práticas, e através de suas solidas bases é possível estabelecer um alicerce necessário e que promove um bom entendimento dos requisitos regulamentares da conformidade;
> **Medições, melhoria de serviços e processos,** é citado que é preciso conhecer e fazer medições para poder administrar, a ITIL trata a consistência e coerência dos processos como um modo de medi-los, com intuito da constante melhora nos processos e na sua governança conforme suas necessidades (ARRAJ, 2013).

Vistos os benefícios que a infraestrutura ITIL estabelece para uma organização, é importante agora, entender como funcionam os processos e suas boas práticas de governança ITSM, e como eles são divididos. A ITIL segundo MODIRI (2012) é dividida em cinco publicações nas quais são tratadas como um guia específico de cada fase do ciclo de gestão do serviço. Na imagem a seguir é demonstrado como cada fase é englobada neste ciclo de vida dos requisitos de serviços ITIL.

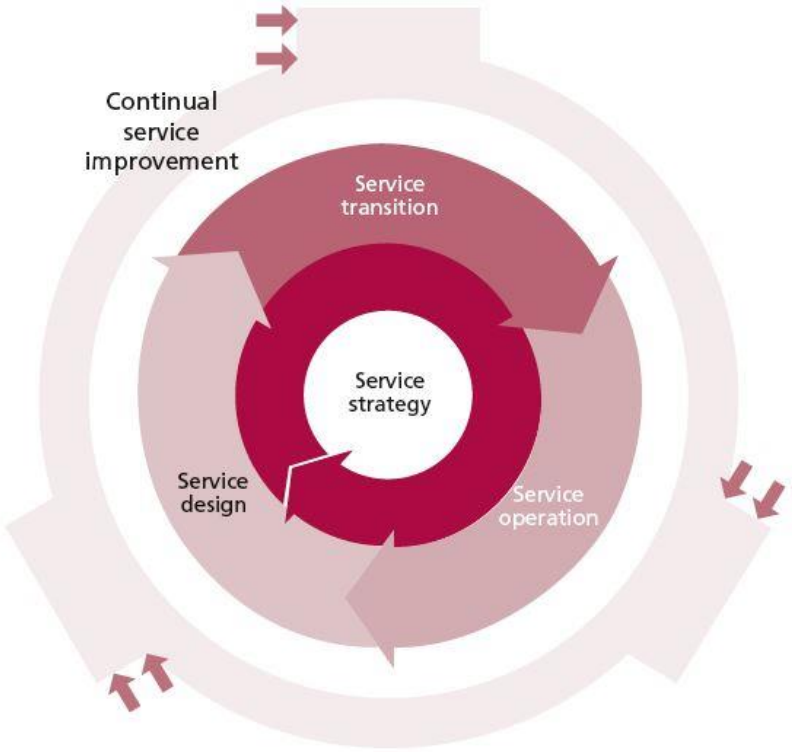

Figura 6. Ciclo de vida de serviços ITIL Fonte: Tso 2012

De acordo com Verheijen (2008) o ciclo de vida de serviços ITIL está baseado no conceito de gestão de serviço, no qual é relacionado com os conceitos de serviço, que é descrito pelo mesmo como a entrega de valores aos clientes e na facilitação de resultados com a diminuição de riscos ou custos.

O serviço pode melhorar o desempenho além de reduzir a pressão, fatores que aumentam as chances de obtenção de resultados desejados. Outro conceito descrito é o de valor que é mencionado pelo autor como sendo "O núcleo de valor do conceito de serviço." Ele ainda continua expondo que o conceito de valor possui no ponto de vista do cliente dois principais componentes, a utilidade e a garantia no qual os apresenta como "O utilitário é o que o cliente recebe, e a garantia é como ele é fornecido". Ambas consideradas características que são adeptas das boas práticas ITIL.

Em sequência, serão descritos tópicos que descrevem os requisitos que compõe o ciclo de vida de serviços da ITIL e suas principais propriedades.

3.1.1 Fases do Ciclo de vida ITIL

Após observarmos na Figura 6 que representa as fases do ciclo de vida ITIL é relevante entendermos de maneira simples o papel que cada uma dessas fases desempenha neste ciclo.

Dentro do processo a Estratégia de serviço é encontrada no coração do ciclo ela é responsável por definir o valor do serviço e suas estratégias para atingi-lo, enquanto o design de serviço tem como responsabilidade desenhar esses serviços e agregar um valor a ele, já na fase de transição dos serviços é produzido um aspecto que transforma o processo em um ser vivo que está em constante mudança e transição é responsável pela sua consistência quando surge mudança ou atualização, para que então, seja papel da equipe de operação de serviço assegurar que o serviço e valor, seja entregue, e por fim o serviço de melhoria continua que tem como finalidade, dentro do ciclo, de estabelecer a melhoria continua dos processos e serviços de TI (TSO 2012). Para confirmar este argumento é dito que:

> A estratégia de serviço é o eixo do ciclo de vida do serviço que impulsiona todas as outras fases; é a fase de formulação de politicas e definição de objetivos. O serviço de Design, Serviços de transição são guiados por esta estratégia a sua melhoria continua é a adaptação e mudança, A fase de melhoria de serviço continua, significa estar aprendendo e melhorando, e abraça todas as outras fases do ciclo de vida, nesta fase são iniciados programas e projetos de melhoria, e os prioriza com base na estratégia e objetivos da organização (VERHEIJEN, 2008).

A partir disso será percorrida cada etapa deste processo em sequência de maneira mais ampla além de ser contextualizado as principais características de cada componente dos processos que compõe esse ciclo de vida.

1) Estratégia de serviço

De acordo com TSO (2012) o propósito do serviço de estratégia é estabelecer um plano que esteja alinhado ao conjunto de princípios e que solucione o problema de negócio, também é visto como um valor que está voltado principalmente para entender e atender as necessidades dos clientes, os termos mais usados para definir o propósito do serviço de estratégia dentro do ciclo de vida ITIL, são:

- **Fornecer** uma solução para um problema de negócio;
- **Identificar** ativos estratégicos utilizados para a vantagem competitiva;
- **Entender** as necessidades do cliente e o por que delas e quando elas ocorrem.

Em sequência foi proposto algumas interrogativas que foram elaboradas e discorridas por (VERHEIJEN, 2008) como perguntas que o serviço de estratégia deve responder, são elas: “Que serviços para oferecer aos clientes? Como se diferenciar dos concorrentes? Como criar valor para os clientes? Como fazer um caso de investimentos estratégicos? Como definir e melhorar a qualidade do serviço? Como alocar eficientemente os recursos através de um

portfólio de serviços?". Dentro dos conceitos básicos que são utilizados para responder essas perguntas e formular uma estratégia, que são definidos os quatro P's formulados (VERHEIJEN apud MINTZBER 1994) que são usadas como ponto de partida para responder as questões anteriores:

- Perspectiva - Ter uma visão clara e concentrar-se;
- Posição - Tome uma posição claramente definida;
- Plano - Formar uma noção precisa de como a organização deve desenvolver-se;
- Padrão - Manter a consistência nas decisões e ações.

Como visto anteriormente na figura 5 o processo de estratégia de serviço está situado no coração do ciclo de vida de serviços ITIL, é sobre ele que está o papel de ajudar e guiar todos os outros serviços do seu ciclo de vida, e para que isso seja bem estruturado, é importante definir os seguintes conceitos chaves que também ajudam a responder as perguntas que objetivam o serviço de estratégia. Os conceitos estão descritos na tabela a seguir.

Conceito	Método
Serviço	Definir o mercado que eles vão operar e identificar e compreender os seus clientes; Explorar as oportunidades e limitações, quantificar o resultados e classificar os serviços; Todos os prestadores de serviços devem procurar alinhar-se com as expectativas dos clientes.
Valor de Serviço	O tipo de Serviço que o cliente recebe em termos de resultados suportes e / ou restrições; Garantia serviço, Como o serviço é prestado e sua usabilidade, em termos de disponibilidade, capacidade, continuidade e segurança.
Tipos de prestadores de serviço	Defini-los e separa-los por tipos: Tipo I existe dentro de uma organização exclusivamente para prestar um serviço se a uma unidade de negócios específica; Serviços Tipo II várias unidades de negócios na mesma organização; Tipo III funciona como um prestador de serviços externo servindo vários clientes externos.

Gerenciamento de serviços como um ativo estratégico	Transformar as capacidades de gerenciamento de serviços em ativos estratégicos; Definir as Capacidades do provedor, em termos de gestão, organização, processos, conhecimento e pessoas para coordenar, controlar e implantar recursos; Definir os recursos e entradas diretas para a produção de serviços (Ex: financeiros, capitais, infraestrutura, aplicativos, informações e pessoas).
Fatores críticos de sucesso	Fatores críticos de sucesso são identificados, avaliados a fim de determinar os ativos de serviços necessário para implementar com sucesso a estratégia de serviço desejado.
Economia de Serviços	Definir uma gestão financeira; gestão da procura e do serviço; Compreender o equilíbrio entre o custo de prestação do serviço, o valor do resultado obtido e o retorno sobre o investimento.
Estratégias de prestação de serviços	Definir e conhecer os prestadores de serviços e o impacto de suas entregas, a gestão financeira deve implementar um analise das variantes por categorias e analises de impacto de cada prestador de serviço.

Tabela 3. Conceitos chaves dos Serviços de estratégias Fonte: VERHEIJEN, 2008 adaptado pelo autor

Como esta fase do ciclo de vida tem como objetivo melhorar as competências básicas da organização é necessário definir alguns processos e atividades chaves que impulsionem e acarretem no cumprimento de objetivos. Esses processos e atividades são separadas por TSO (2012) como:

- Primeiro, estratégia de gestão de serviços de TI que é uma gestão estratégica voltada aos ativos tecnológicos com planos operacionais que garantes que todas as alterações no contexto do negócio sejam atualizadas no plano estratégico para garantir sua coerência. O autor descreve que "A finalidade de uma estratégia de serviço é articular como um provedor do serviço o que permitira a organização atingir seus resultados e ter uma maneira mais eficaz e eficiente de gerenciar esses serviços". Com isso é possível afirmar que o motivo pelo qual esta gestão estratégica tende ser definida é para assegurar que objetivos estão sendo atingidos.

- Segundo, serviço de gestão de portfolio, que possui como finalidade de acordo com o (TSO 2012) "Equilibrar o investimento em TI com a capacidade de entender os resultados de negócios";
- Terceiro, a gestão da procura, que deve se atentar a capacidade de atender as demandas de fornecimento, não somente estar disponível quando a procura é grande, como também evitar a sobra dos ativos quando a demanda for menor, é importante conhecer esses parâmetros para regular e utilizar de táticas para que a demanda se torne constante e se adeque ao padrão de atividades do negócio;
- Quarto que é a gestão de relacionamento da empresa, que possui um processo que deve estabelecer uma relação com o cliente e identificar suas necessidades além garantir que tais estão sendo atendidas de forma eficaz e de maneira estratégica.

Por fim neste tópico de estratégia de serviços, os papéis chaves que devem ser desempenhados nesta fase do ciclo de vida ITIL, que estão falados na seguinte tabela. (TSO 2012).

Papel	Responsabilidades
Gerente estratégico de TI	Formular e comunicar a estratégia de TI e se assegurar de estão sendo aplicadas.
Gestor de avaliação TI	Responsável pela governança corporativa e a avaliação geral da estratégia de TI.
Diretor gestor dos serviços de TI	Responsável por todos os processos de gerenciamento de serviços de TI e da criação de um departamento de gerenciamento de serviços.
Gerente de serviços de portfolio	Definir serviços e atendimentos, gerência e manter o portfolio e manter a relação de comunicação a todas as partes interessadas.
Gerente de relacionamento do negócio	Manter uma relação com o cliente, compreendendo-o e combinando suas necessidades com os resultados obtidos e necessidades.
Gerente financeiro	Manter modelos financeiros com as informações de custo e valor dos serviços de TI.
Gerente de demanda	Identificar os perfis de atividade dos usuários e garantir que o recursos atendam a demanda.
Chefe de recursos	Responsável por liderar e dirigir a terceirização dentro da organização.

Tabela 4. Papéis chaves da Estratégia de serviço. Fonte: Tso, 2012. Adaptado pelo autor.

2) Design de serviço

O design de serviço é um estágio do ciclo de vida ITIL que é projetado para entender mudanças e novos serviços, e exigências do negócio. Segundo TSO (2012) "As principais atividades dentro desta fase incluem o planejamento e coordenação das atividades de design, garantindo projetos consistentes de serviços, processos, informações e métricas, melhoria das atividades de serviços e processos." Dentro desta fase existem cinco aspectos fundamentais que devem ser atentados são eles: "Soluções de serviços para serviços novos ou modificados; Sistemas e ferramentas de informação de gestão; Tecnologia e gestão de informação; Processos; Métodos de medição e métricas.".

Para que esta etapa seja bem desenvolvida existe uma abordagem que foi estabelecida que descreva os processos e atividades chaves que devem ser feitos para um bom exercício dessa fase, que estão descritas na seguinte tabela 5 (TSO 2012).

Processo	Atividade
Coordenação de projetos	Atividades relacionadas ao ciclo de vida de design de serviço global, que está ligado a gestão do processo de coordenação de design; Atividades relacionadas a cada projeto individual, que pode ser realizada por um gerente de projetos.
Serviço de gerenciamento de catalogo	Este serviço de catálogo provê uma fonte de informações sobre todos os serviços de TI entregues á empresa pelo serviço de organização do fornecedor. Assegurando que exista um quadro consistente com todas as informações disponíveis e seus detalhes e status.
Gerenciamento de nível de serviço	Assegurar que toda a operação de serviços e seu desempenho sejam medidos de forma consistente, de forma profissional em toda a organização de TI e que os serviços e os relatórios produzidos atendam as necessidades do negócio.
Gestão de disponibilidade	Otimizar e melhorar continuamente a forma proativa de disponibilidade de serviços de TI e suas organizações de apoio, fornecendo um ponto de apoio a gestão de todas as

	questões relacionadas a disponibilidade aplicada aos serviços, componentes e recursos.
Capacidade de Gestão	Fornecer um ponto de foco e gestão relacionada ao desempenho dos serviços.
Gestão da segurança da informação	Fornecer orientação estratégica, garantindo que os objetivos sejam alcançados, determinando riscos e gerenciando eles de forma correta, verificando se os recursos da empresa estão sendo utilizados de forma eficaz.
Gestão de fornecedores	Garantir que o serviço dos fornecedores apoiem as metas e expectativas do negócio, que eles estejam em conformidade com os termos e condições dos processos e de contrato.
Atividades chave da fase de concepção de serviços	Coleção de requisitos de negocio e analise e documentação clara; Desenvolvimento de soluções adequadas a processos e serviços; Produção e revisão da documentação; Planejamento das atividades e conexão delas com outros projetos aliados; Produção e manutenção de politicas e documentação de design; Gestão de riscos e de todos os processos; Alinhamento com todas as estratégias e políticas organizacionais e de TI.

Tabela 5. Processos e atividades chaves de design de serviço Fonte: Tso 2012, adaptado pelo autor.

Papel	Responsabilidades
Gerente coordenador do processo de design	Responsável pelo planejamento, e coordenação dos serviços e atividades de design para serviços novos ou modificados.
Gerente de processos	Responsável pela produção e manutenção precisa de serviços; Garantir que os níveis de serviço e qualidade acordados sejam cumpridos.
Gerente de disponibilidade de processos	Garantir que todos seus serviços cumpram as

	metas de disponibilidade acordados.
Gerente de processos e capacidades	É responsável por garantir que a capacidade dos ativos de TI sejam correspondentes a demanda.
Gerente de segurança de processos	Assegurar de que as politicas de segurança estão alinhadas com as políticas e necessidades do negócio.
Planejador de TI	Responsável pela produção e coordenação de planejamento de processos de TI.
Arquiteto de TI, TI Designer.	Responsável pelo design geral das necessidades tecnológicas do sistema de gerência e de projetos.

Tabela 6. Papéis chaves do processo de Design de serviço. Fonte: Tso 2012, Adaptado pelo autor.

3) Serviço de Transição

Esta fase tem como intuito dentro do ciclo de vida que seja atentado as questões voltada a gestão de mudanças, é importante que seja garantido que durante essa transição que todos os aspectos do serviço estejam sendo garantidos e que suas expectativas estejam sendo cumpridas, além de facilitar as mudanças ou da inclusão de novos serviços de forma eficiente (TSO, 2012).

Dentro desta operação foram definidos alguns princípios fundamentais que proporcionam um suporte, e quando seguidos garantem que nesse estágio do ciclo de vida, na transição de serviço seja gerenciado de forma que todos os aspectos sejam implementados e adaptados com o fim de assegurar que o valor de negócio esperado seja entregue (TSO 2012). É explicitado pelo autor como sendo eles:

> Definir e implementar as diretrizes e procedimentos para a Transição de Serviço; Implementar todas as mudanças através de Transição de Serviço; Utilizar estruturas e padrões comuns; Reutilizar processos e sistemas existentes; Coordenar planos de transição do serviço com as necessidades do negócio; Criar relações com as partes interessadas e manter estes; Configurar controles eficazes sobre os bens, responsabilidades e atividades; Entregar sistemas para a transferência de conhecimentos e de apoio à decisão; Planejar pacotes para lançamentos e implantação; Antecipar e gerenciar mudanças nos planos; Gerenciar os recursos de forma proativa; Continuar a assegurar a participação das partes interessadas numa fase precoce no serviço; Assegurar a qualidade de um novos ou alterados serviços;

> Proativamente melhorar a qualidade do serviço durante a Transição de Serviço.

Alguns conceitos são definidos por Verheijen (2008) e descritos como importantes para que esta fase de transição seja aplicada de forma efetiva na organização, ele cita que "As seguintes políticas são importantes para uma transição de serviço eficaz". Elas ajudam a compreender todos os serviços conforme suas garantias e resultados, gerenciar a complexidade associada às mudanças no qual é importante que seja estabelecido um plano formal para tratar as atualizações e mudanças que devem ser implementadas garantindo todos os ricos e considerações importantes do serviço e ajudam no apoio a transferência de conhecimento, algo que é importante assegurar de que esses conhecimentos existentes estejam disponíveis pra uso, para consultas e reutilização em procedimentos semelhantes além de assegurar-se de que os colaboradores envolvidos estejam envolvidos com o processo de transição de serviços e que estejam cientes dos requisitos e de toda esta etapa do processo de ciclo de vida. Garantindo assim que todas as competências sejam entregues atingindo os objetivos e expectativas que esta fase possui dentro do ciclo.

Em sequência é importante tratar sobre os processos e atividades que estão envolvidos nesta fase de transição, e possui um valor muito grande a organização e deve estar alinhado com as necessidades organizacionais da empresa. Os processos e atividades importantes citados por Verheijen (2008) estão discorridos nas seguintes tabelas 7 e 8.

Processos	**Papel**
Planejamento de transição e apoio	Assegura o planejamento e coordenação dos recursos.
Gestão de mudanças	Garante que as mudanças estão sendo implementadas de forma controlada garantindo as fases do processo (Ex. Avaliação, planejamento, testes, implementação e documentação).
Gerenciamento de configuração de serviços e ativos	Gerência os ativos de serviços e seus itens de configuração.
Gerenciamento de liberação e implantação	Implementação, testes e implantação.
Serviço de validação e testes	Garantir que os processos novos ou alterados estejam aptos a uso e de acordo com seu propósito.
Avaliação	Verifica o desempenho e qualidade, se está de acordo com

	as expectativas.
Gestão do conhecimento	Gestão de tomada de decisão e garantia de que a o conhecimento seja confiável e disponível durante o ciclo de vida.

Tabela 7. Processos de transição de serviço Fonte: Verheijen 2008, Adaptado pelo autor.

Atividades	Objetivo
Comunicação	Estabelecer a comunicação entre as partes interessadas durante todo o processo de transição de serviço
Gerenciamento de mudanças	Deve gerenciar o ciclo de mudanças(choque, evasão, aceitação) criado por alguma alteração ou novo serviço,
Gerenciamento das partes interessadas	Analisar e gerenciar os interesses e exigências das partes interessadas

Tabela 8. Atividades de transição de serviço. Fonte: Verheijen 2008, Adaptado pelo autor.

4) Serviço de operação

O propósito da operação de serviço tem haver com a entrega do mesmo, é a fase onde acontece o suporte de operação estratégica para que seja realizada a entrega do valor de negócio, neste contexto é necessário que exista um alinhamento com todos os processos de serviços anteriores para assegurar de que o valor a ser entregue esteja de acordo com as expectativas. Esta fase possui operações muito bem definidas descritas por (VERHEIJEN, 2008) pelas características de contato com os usuários, lidar com incidentes e solicitações além de ser o ponto de apoio a estrutura de TI, onde a gestão técnica e de operações são atividades operacionais características desse serviço e que compõe a aplicação de gestão de acordo com os padrões e gerência do ciclo de vida e de melhoria dos serviços de TI.

Em suma o *Service Desk* tem como responsabilidade manter o ponto de contato com os usuários da TI, no qual lida com as responsabilidades de reparos de incidentes e requisições de acesso e qualquer outro processo ou atividade. Enquanto o *Service Desk* lida com o usuário a gestão técnica é responsável pelo conhecimento técnico das operações de gestão da infraestrutura de TI além de planejar, implementar e manter uma estrutura consistente operando. E por fim a gestão de aplicação que tem como papel a gestão das aplicações dentro do ciclo de vida, servindo de suporte para os serviços de TI.

Em sequencia é tratado os processos e atividades fundamentais que englobam esta fase do ciclo de vida, relacionados na tabela 9 e 10 a seguir.

Processos de operação de serviços	Papel
Gerenciamento de eventos	Monitorar todos os eventos que acontecem na infraestrutura de TI com a finalidade de estruturar comportamentos normais e determinar quando existe anomalias comportamentais.
Gerenciamento de incidentes	Realiza a restauração no caso de falhas com o intuito de causar o mínimo impacto possível.
Gerenciamento de problemas	Realiza um diagnóstico das atividades com o intuito de contextualizar os problemas, sua origem e solução.
Solicitação de cumprimento	Tem como um papel servir de canal de solicitação entre os usuários e a gestão de infraestrutura.
Gerenciamento de acesso	Realizar a autorização de acesso a determinados usuários e serviços.

Tabela 9. Processos de operação de serviço. Fonte: Verheijen 2008, Adaptado pelo autor

Atividades de operação	Objetivos
Atividade de operações de TI	Cumprir as atividades operacionais necessárias para a gestão da infraestrutura.
Monitoramento e controle	Fornecer, apoiar e melhorar os serviços.
Atividades operacionais	Garantir que a tecnologia coincida com o objetivo dos serviços e processos.
Gestão do centro de dados	Gestão dos componentes de gestão de instalações da TI (Ex. equipamentos, dados, informações, energia, edifícios).

Tabela 10. Atividades de operação de serviços. Fonte: Verheijen 2008, Adaptado pelo autor.

5) Serviço de Melhoria Continua

Depois desse detalhamento de cada processo das fases do ciclo de vida ITIL por fim vem a etapa de serviço de melhoria contínua, esta etapa tem como intuito de fazer a contínua melhoria dos processos com o fim da melhora na qualidade dos serviços, sua meta principal é

o contínuo alcance da eficácia e eficiência dos serviços de TI, nos quais podem ser alcançados na redução de custos e erros, automatização de operações entre outros métodos (TSO 2012).

Antes de começar a operação de melhoria, foi definido por VERHEINJEN (2008) um modelo de questões que devem ser respondidas para garantir que o processo e atividades seja direcionado corretamente. São elas: "Qual a visão? Onde estamos agora? Onde queremos chegar? Como vamos chegar lá? Será que vamos chegar lá? Como vamos manter o ritmo?". A partir da respostas obtidas nestas interrogativas é feito o processo de melhoria dos sete passos que será formulado um caminho do processo de melhoria, e este caminho está marcado por um processo baseados no modelo *PDCA(Plan, Do, Check)* que possui "A finalidade de definir e gerenciar os passos necessários para identificar e reunir dados significativos, analisar esses dados para identificar tendências e questões, para implementar as melhorias." Esses passos estão demonstrados na figura 5 a seguir, e a partir deles é feito um relatório de serviço sobre os resultados desenvolvidos e por fim uma edição dos valores adquiridos e por fim uma avaliação para ver se as expectativas foram atendidas (TSO 2012).

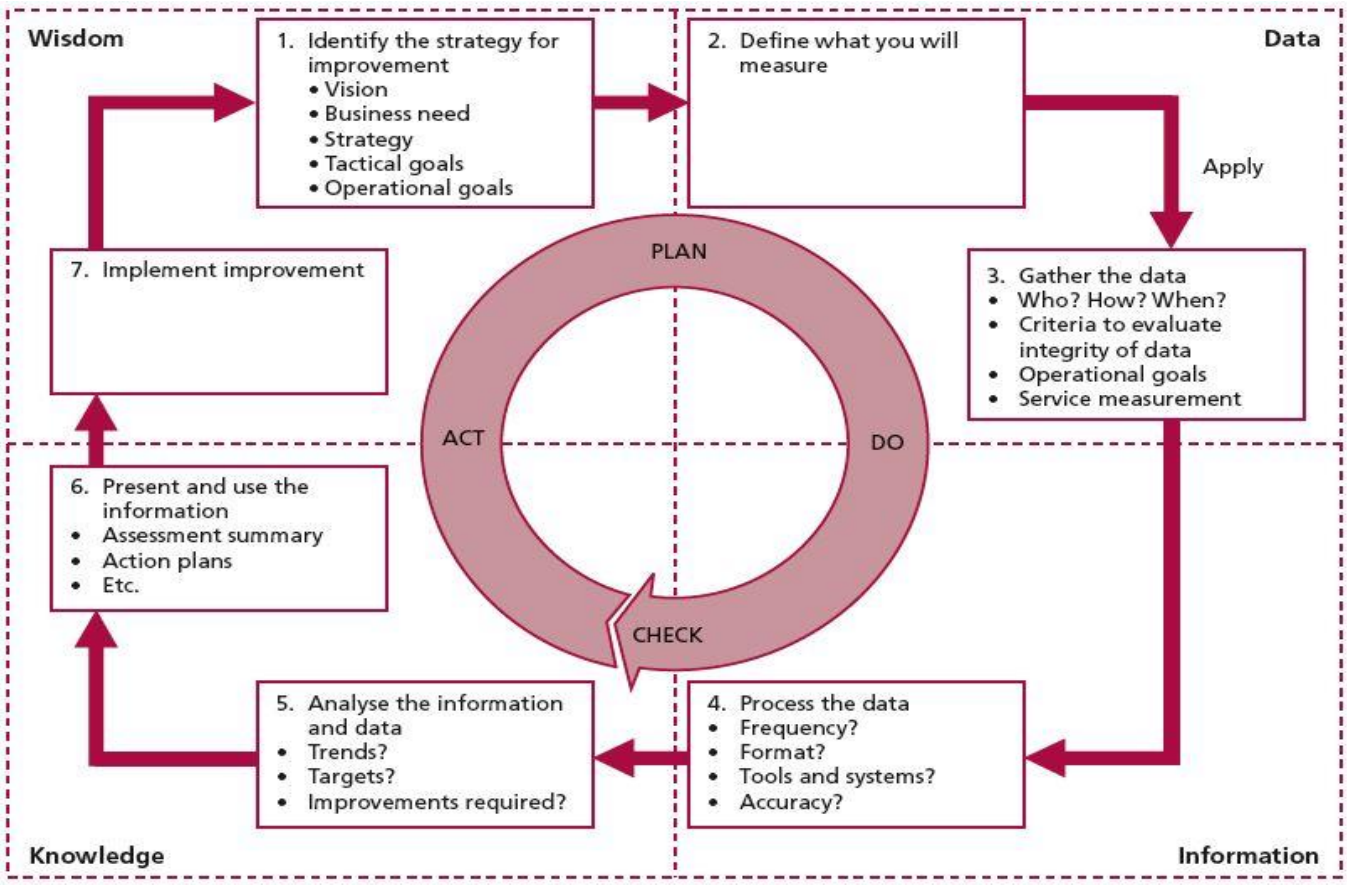

Figura 7. Sete passos do processo de melhoria Fonte: Tso 2012

Cada passo dessa estrutura demonstrada na figura 7 faz parte das táticas de estruturação estratégicas que são definidas no ciclo de vida, durante a estratégia de serviço e o design de serviço, esses passos servem para identificar a estratégia para a melhoria.

Como é indicado na figura 7 o passo de número um em seguida no passo de número dois, deve ser definido o que será medido, enquanto que no passo três é necessário reunir os dados, para que seja feita uma medição com o objetivo de identificar onde melhorias podem ser implantadas para que em seguida no passo quatro os dados sejam processados, esse passo é visto como chave para se entender o impacto desses componentes sobre a infraestrutura de TI.

Enquanto no passo cinco cabe analisar informações, processando os resultados e notando os comportamentos e rotinas resultantes e analisar se as seguintes questões são respondidas: "Estamos cumprindo as metas? Existem tendências claras? É necessária uma ação corretiva? Qual seu custo?".

E a partir disso, no passo seguinte, passo seis, é usado para apresentar e usar as informações até agora coletadas de forma clara e consistente, para que por fim no passo sete, seja implementado as melhorias que foram constatadas de acordo com o conhecimento adquirido nesse processo. E uma vez terminado esses passos ele deve ser reiniciado em um *loop* de volta ao ponto inicial (TSO 2008).

3.1.2 Considerações ITIL

A OGC (2014) delibera a importância que a implementação dos processos que compõe o ciclo de vida ITIL que estrutura um modelo operacional de alto nível para a organização, seus processos compõem uma estrutura composta por processos de melhoria .

É recomendado por Moura (2007) que seja feita de forma gradual para que seus processos fiquem bem definidos e consistentes e seu gerenciamento de serviços bem estruturado de forma que seus processos fiquem interligados uns aos outros (como no ciclo de vida) fazendo com que o a estrutura da organização seja viva em um ciclo constante de amadurecimento e melhoria.

3.2 Riscos e vulnerabilidades

Segundo o dicionário Michaelis (2009) a definição de ameaça constitui de um "ato delituoso pelo qual, alguém, verbalmente ou por escrito, por gesto ou por qualquer outro meio simbólico e inequívoco, promete fazer injustamente um mal grave a determinada pessoa; um prenuncio ou qualquer coisa má". Visto isso fica apropriado dizer que ameaça pode ser olhada como algo que pode gerar algum perigo a um bem. Sob a ótica de Rosa (2004) informações armazenadas podem sofrer vários tipos de ameaças sendo elas cometidas por:

> **Intrusos** – utilizadores não autorizados a aceder ou modificar informações, tentam fazê-lo.
> **Utilizadores autorizados maliciosos** – utilizadores autorizados a utilizar o sistema, aproveitam para praticar atos ilícitos atuam como intrusos, acedendo ou modificando dados de uma forma ilícita.
> **Utilizadores autorizados e negligentes** – utilizadores autorizados a aceder a informação que de uma forma não deliberada realizam certas ações que levam a modificação da informação ou permitem que pessoas não autorizadas o façam. (ROSA, 2004)

Muitas vezes a fragilidade de uma estrutura se vem de princípios técnicos básicos cometidos no início de um controle de gerenciamento, como a escolha de uma tecnologia ultrapassada ou ruim por falta de conhecimento e faz com que se sejam feitas más escolhas e se utilizem de tecnologias defasadas ou ruins. Essas falhas podem acontecer na escolha da aplicação, do sistema operacional, dos equipamentos de rede da instalação elétrica entre outros.

Quando o assunto é recursos humanos a escolha de Profissionais não adequados e não devidamente capacitados, podem resultar em uma má configuração de um sistema, ou acontecem quando os equipamentos de rede são configurados erroneamente, as contas do sistema e do administrador e/ou usuário são previsíveis, a política de segurança mal administrada quando o administrador de segurança não se atenta ao treinamento e conscientização dos usuários, falta políticas internas, quando os controles de acessos não são cobrados, ou a administração de segurança é negligente na monitoração e auditoria, ou há falta de um plano de contingência. Todos aspectos de crucial importância na consistência da composição da segurança.

Outro componente abordado quando se trata de ameaças a segurança da informação são os riscos e ameaças que a segurança física pode ocasionar.

De acordo com Rhodes-Ousley (2013) é um assunto crucial assinalado como um ponto de vista importante quando se discute uma ameaça referente a segurança física. O autor classifica os ativos em categorias para assim determinar o grau de proteção contra ameaças. A

avaliação física feita pelo autor baseia-se em medições de exposição a um risco aplicável, o mesmo aconselha realizar um "walk-through" nas instalações físicas para identificar possíveis falhas na segurança física.

São mencionadas quatro áreas principais que devem fazer parte de qualquer avaliação de vulnerabilidade física sendo elas: edifícios, dispositivos de computação e periféricos, documentos, registros e equipamentos. O autor cita o seguinte exemplo como avaliação de detecção que devem ser atendidas.

> A rede de conexão Wi-Fi na recepção ou na sala de conferência é pública? A conexão é disponível para visitantes? Se assim for, ela está pegando um endereço IP via DHCP? É necessário fazer login? Identificar o problema, mas também avaliar o que (se houver) justifica sua necessidade de negócio. Se uma necessidade comercial legitima não existe, o risco ultrapassa qualquer potencial de retorno, e a responsabilidade de existência tem uma condição para existir e deve ser corrigido. (RHODES-OUSLEY, 2013)

Subsequente uma abordagem importante seria do aspecto de ameaças de segurança física seria as causas naturais, como queda de energia, condições ambientais, desastres naturais, danos causados pela água, contato com materiais tóxicos, terremotos, incêndios, exposição a altas temperaturas e umidade (BAGCHI, 2009).

São os fenômeno da natureza descrito pelo autor que podem aumentar o nível de ameaças da estrutura física da segurança, como foi percebido nos exemplos citados, algumas dessas ameaças físicas naturais não podem ser previstas porém podem ser prevenidas tais como quedas de energia que pode ser prevenida com o uso de nobreaks e geradores, incêndios e exposição a altas temperaturas podem ser precavidas.

Uma política de segurança específica contra ameaças naturais físicas, deve começar desde uma boa instalação elétrica quanto ao número de extintores de incêndio disponíveis.

Medidas como essas podem fazer uma significante diferença na prevenção de incidentes e na melhoria do grau de exposição a ameaças da estrutura da informação.

O impacto resultante na ocorrência de uma ameaça pode significar uma perda muito grande para a organização, por isso é importante que seja feita uma gerencia de riscos. "A avaliação de risco consiste em: identificação e avaliação de risco, identificação e avaliação dos impactos de riscos, recomendações de medidas de redução de risco" (BAGCHI, 2009). o processo de gestão de risco de acordo com o mesmo autor, minimiza o impacto das ameaças realizadas e fornece uma base para uma gestão eficaz de tomada de decisão e que é um processo importante e que deve fazer parte do ciclo de vida de desenvolvimento do sistema.

Quando se trata de vulnerabilidade, que é considerada uma fraqueza em um sistema de informação que pode fornecer um resultado prejudicial para o sistema ou seu funcionamento. (TECHEXCEL, 2012). O mesmo conceito pode ser definido como "Uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças". ARRAJ (2013,

apud ISO/IEC). Em ambos os casos vulnerabilidade é sinônimo de uma condição de risco para um sistema. Segundo a ISO 27005 as vulnerabilidades são classificadas em vulnerabilidade de hardware, software, rede, pessoal, instalações e estrutura organizacional.

A vulnerabilidade normalmente é explorada como porta de entrada onde o atacante cultiva essa fraqueza até conseguir o que procura, por isso é importante fazer uma análise dessas vulnerabilidades. Segundo ARRAJ (2013, apud ISO/IEC 27005, 2007) é recomendável o uso de ferramentas específicas para a caracterização dessas vulnerabilidades. Que são elas:

> **Ferramenta automatizada de análise de vulnerabilidades** Aplica-se à análise de redes de computadores e busca identificar portas abertas em hosts e vulnerabilidades associadas a essas portas;
> **Teste e avaliação de segurança** Baseada na elaboração e execução de scripts de teste;
> **Testes de penetração** Técnica amplamente variável e aplicável a vários canais tecnológicos (sites web, redes de telecom, redes sem fio, prédios, perímetros militares);
> **Revisão de código** Técnica aplicável a software, onde o código-fonte de um programa é inspecionado visualmente por programadores, a fim de identificar vulnerabilidades a ataques;
> **Entrevistas** Aplicáveis a colaboradores e usuários;
> **Questionários** Para coleta de grandes volumes de dados
> **Inspeção física** Visitas ao local;
> **Análise de documentos** Análise de documentos de incidentes; (ARRAJ, 2013, apud ISO/IEC 27005)

Essas práticas e métodos de gerência de vulnerabilidades são usados como um dos métodos de prevenção, controle e de resposta eficaz a ataques, também pode ser usada no processo de classificar, remediar e investigar as vulnerabilidades. Esses métodos podem ser classificados baseados nesse modelo e regras que os ditam.

Esses métodos de análise são modelos adotados a pesquisa e são baseadas no alicerce da segurança da informação, confidencialidade, integridade e disponibilidade e são atributos de uma nova ideia de como lidar com as vulnerabilidades antes tratada com menos importância, mas através da norma ISO/IEC 27005 em particular este citado anteriormente manifesta-se que este campo de pesquisa vem crescido e despertado o interesse devido a sua importância na segurança dos serviços da informação em rede.

3.2.1 Ataques

Um sistema de computador possui três componentes distintos, hardware, software e dados. Segundo Bsi (2014) cada um destes ativos oferece um valor diferente para os membros afetados deste sistema. O mesmo autor expõe que ataque acontece quando uma pessoa que explora uma vulnerabilidade o que resulta em ataque ao sistema, e prejudica

alguma propriedade dos componentes desse sistema. Ao entender como funcionam os métodos utilizados para explorar essas vulnerabilidades é possível que "Compreendendo as múltiplas variáveis de ataques e tratamentos a organização pode construir um método mais robusto de medidas de defesa" (BAGCHI, 2009).

Como já explicado anteriormente um ataque pode ser causado por uma brecha, uma vulnerabilidade que é explorada e se tornam o ponto de acesso dos agentes atacantes. Esses ataques são variados e podem possuir uma identidade específica dependendo do objetivo do atacante, que podem ser diversos, sendo os mais comuns:

> Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos;
> Prestigio: vangloriar-se perante outros atacantes;
> Motivação financeira: coletar e utilizar informações confidenciais de usuários para aplicar golpes;
> Motivação ideológicas: tonar inacessível ou invadir sites que divulguem conteúdo contrário a opinião do atacante;
> Motivação comercial: tornar inacessível ou invadir sites de computadores de empresas concorrentes, para tentar impedir acesso dos clientes ou comprometer a reputação destas empresas. (MODIRI, 2012)

A motivação de um atacante e como ele age são características importantes que podem ser identificadas através da abordagem que ele utiliza para o ataque. Existem diversos tipos característicos existentes de abordagem de ataques, são eles (MICHAEL E. WHITMAN, 2011):

Código malicioso, Os ataques de código malicioso são diversos e variados, socialmente podem ser chamados de vírus, são conhecidos pelos famosos Cavalos-de-Tróia, dentro deste tipo também se encontra os *worms*, e *scripts* da *web* ativa, possuem a intenção de destruir, roubar ou interceptar informações.

Esses tipos de ataques como qualquer outro explora uma vulnerabilidade tanto do sistema como do usuário, sua variedade vem crescendo e está cada vez mais robusto e nocivo.

Já os ***Back Doors*** são simples "portas traseiras" abertas passadas despercebidas pelo administrador de rede, são entradas vulneráveis utilizadas por agentes nocivos para penetrar e ter acesso a dados.

Outros tipos de técnicas como por exemplo a **quebra de senhas**, a de **força bruta** que é a utilização de todas as combinações e recursos computacionais para fazer a quebra de uma chave de segurança ou de uma criptografia. Subsequente as essas técnicas existe outras mais robustas, como ***a Denial-of-Service (DoS)*** que segundo (MICHAEL E. WHITMAN, 2011) "Em um ataque DoS, o invasor envia um grande numero de conexões ou informações, solicitações para um destino, são tantas solicitações que o sistema destino fica sobrecarregado e não pode responder aos pedidos legítimos de serviço do sistema." Este tipo de ataque tem como objetivo tornar o sistema alvo indisponível ou incapaz de realizar suas tarefas. Dentro

ainda deste ataque existe uma variante dele chamada **DDoS**, que é uma versão distribuída, no qual os ataques estão distribuídos em vários sistemas, "As máquinas comprometidas são transformadas em zumbis, são dirigidas remotamente pelo atacante".

Em sequência é possível encontrar uma técnica chamada ***Spoofing,*** é uma técnica que utiliza uma tática que troca endereços IP's que mascaram de onde a mensagem está vindo ou para obter acesso a uma rede, é uma tática que falsifica os endereços IP's alterando seu cabeçalho para conseguir ter o acesso autorizado.

Outra técnica muito conhecida é a de ***Spam*** e ***Mail Bombing***, que possuem como tática o envio de e-mails indesejados ao alvo com intuito ou de infiltrar ou de deixar o serviço indisponível.

E por fim os ***Sniffers***, que normalmente são programas "Utilizados para gerenciamento de redes, porém na mão de hackers são usados para roubar senhas e informações sigilosas. Este tipo de ataque tem como característica a captura de pacotes que contenham informações sigilosas".

Essas são umas das técnicas utilizadas por agentes maliciosos na tentativa de acessar, destruir, controlar, modificar, dados, informações ou recursos de algum sistema ou rede.

3.2.2 Atacantes

Depois de falar sobre as ameaças, fraquezas, vulnerabilidades, e dos ataques é imprescindível falarmos sobre os atacantes. Quando falamos de atacantes estamos falando de um agente que explora fraquezas e vulnerabilidades de um sistema ou rede.

Segundo Sterling Bruce (1993), os hackers podem ter infinitas motivações para um ataque, sendo as mais comuns: lucro, protesto, desafio ou prazer. Nas classificações dos tipos desses agentes, existem algumas diferenças que valem a pena serem citadas, como a definição de hacker e cracker, existe essa confusão desses dois termos, pois ambos servem para nomear pessoas com habilidades invasoras, porém segundo o a revista Olhar Digital (2013) cada grupo utiliza suas habilidades de maneira distintas.

> "Os Hackers utilizam todo o seu conhecimento para melhorar de forma legal e nunca invadem um sistema com intuito de causar danos. No entanto os crackers tem como prática a quebra da segurança e usam seu conhecimento de forma ilegal portanto criminosa" (DIGITAL, 2013).

Além desta básica classificação hackers e crackers existem outro tipo mais específicos de classificação quando se trata de agentes externos.

São eles: ***White Hats,*** Os chamados hackers de chapéu branco, ou hacker ético são os agentes externos que usam suas habilidades para razões não maliciosas, muitas vezes eles são chamados para testar um sistema ou rede para encontrar falhas de segurança, esses agentes também são chamados para realizar alguns testes de penetração e vulnerabilidade. Hoje eles são chamados de hackers éticos que fazem tais trabalhos dentro de um contrato acordado.

Já o ***black hat,*** é "Um hacker que quebra a segurança e invade um sistema ou rede de forma maliciosa ou sem consentimento do atacado. Ele usa seus conhecimentos para violar o funcionamento do servidor, roubar informações ou por razões pessoais" (CROVITZ, 2013).

E existem também os chamados e**ngenheiros sociais,** a engenharia social é um dos métodos de abordagem que são ou podem ser utilizados por um *black hat* hacker. As táticas de engenharia social são usadas para conseguir informações para ter acesso a rede. Uma das táticas comuns da engenharia social é abordar um empregado ou usuário da rede e engana-lo para conseguir endereços ou informações que levem a quebra de portas ou senhas de segurança.

Acredita-se que o elo mais fraco da segurança da informação seja a engenharia social, pois ela está associada aos recursos humanos, onde o engenheiro social analisa o alvo e o momento mais propicio para fazer a abordagem em busca das informações necessárias.

Isso (CLAYTON S.SILVA, 2012), explica o porquê de a engenharia social ser o método de abordagem mais vulnerável no aspecto de segurança da informação, pois o objeto de ataque a princípio são usuários e empregados que sem o devido treinamento acabam sendo manipulados sem que ele note, esses tipos de abordagem não podem ser previstos ou detectados por algum sistema ou administrador, tornando-se assim um método eficaz para a quebra, e violação da segurança.

4 A SEGURANÇA DA INFORMAÇÃO EM MPES (Micros e pequenas empresas)

4.1. Perfil das MPES

No Brasil, conforme o Estatuto da Microempresa e Empresa de Pequeno Porte, (MDICE, 1999 Lei nº 9.841/99 ; Lei nº 9.317/96,) elas podem ser classificadas de acordo com sua receita bruta anual ou número de pessoas ocupadas.

Segundo o (SEBRAE, 2014b) este termo pode ser empregado a pequenos negócios que são divididos na seguinte categoria "Microempreendedor Individual com Faturamento

anual de até R$ 60 mil; microempresa com faturamento anual de até R$ 360 mil; empresa de pequeno porte com faturamento anual entre R$ 360 mil a R$ 3,6 milhões".

Outra forma de classificar uma MPE é através do número de pessoas ocupadas, como demostrado na figura 8 a seguir.

PORTE	ATIVIDADES ECONÔMICAS	
	SERVIÇOS E COMÉRCIO	INDÚSTRIA
MICROEMPRESA	ATÉ 09 PESSOAS OCUPADAS	ATÉ 19 PESSOAS OCUPADAS
PEQUENA EMPRESA	DE 10 A 49 PESSOAS OCUPADAS	DE 20 A 99 PESSOAS OCUPADAS
MÉDIA EMPRESA	DE 50 A 99 PESSAS OCUPADAS	DE 100 A 499 PESSOAS OCUPADAS
GRANDE EMPRESA	ACIMA DE 100 PESSOAS	ACIMA DE 500 PESSOAS

Figura 8. Classificação de empresas conforme a ocupação. Fonte: Sebrae, 2014

Visto isso pode-se afirmar que uma MPE constitui-se de qualquer tipo de organização legalmente formalizada que possui um potencial econômico de movimentação de emprego que se adeque a esta categoria legalmente declarada na receita.

Essas MPEs, de acordo com (CAMPONAR, 2004) "As micro e pequenas empresas assumem características próprias de gestão, competitividade e inserção no mercado".

Segundo com o que foi relatado pelo Sebrae (2014a), as MPEs geraram em 2011, 27% do PIB brasileiro, e ainda seguem em crescimento.

A unidade de gestão estratégica do Sebrae segue demonstrando as dimensões que esse setor possui, dos quais as MPEs representam no contexto de serviços e comércios cerca de 98% e 99% respectivamente do total de empresas formalizadas, além de representar aproximadamente 44% de empregos formais e 70% de empregos gerais. Com esse levantamento fica clara a importância estratégica que as MPEs possuem na economia brasileira.

Apesar desses números promissores a taxa de mortalidade das MPEs apesar de serem menores ainda sim é considerada grande. Segundo a Exame (2011) essa taxa chegou a 28,1%. Apesar desses números não indicarem os motivos de fechamento dessas MPEs é importante que o empreendedor possua maturidade para estruturar sua empresa de maneira que ela ultrapasse o período decisivo de sobrevivência, que é considerado pelo Sebrae (2014) como os primeiros dois anos de vida.

Aprofundando essa análise de características é também possível discutir, as principais propriedades que se encontram na estrutura de gestão de uma MPE, segundo a tabela 11 a seguir que descreve suas principais características.

Características Organizacionais	Características de tomada de decisão	Características Individuais
-Pobreza de recursos; -Gestão Central; -Situação extra organizacional incontrolável; -Fraca Maturidade organizacional; -Fraqueza das partes no mercado; -Estrutura simples e leve; -Ausência de planejamento; -Fraca especialização; estratégia intuitiva; -Sistema de informações simples.	-Tomada de decisão intuitiva; -Horizonte temporal de curto prazo; -Inexistência de dados quantitativos; -Alto grau de autonomia decisória; -Racionalidade econômica, política e familiar.	-Onipotência do proprietário/dirigente; identidade entre pessoa física e jurídica; -Dependência perante certos funcionários; -Influência pessoal do proprietário / dirigente; -Simbiose entre patrimônio social e pessoal; -Propriedade dos capitais; -Propensão a riscos calculados.

Tabela 11. Características de estrutura da MPE. Fonte: Camponar 2004 apud Leone 1999, adaptado pelo autor

É possível concluir que as MPEs possuem um nível de maturidade de gestão muito baixo, que é observado através do alto grau de centralização, ausência de planejamento, autonomia decisória, racionalidade de recursos entre outros inúmeros fatores que são indicadores da baixa qualidade gerencial que uma MPE está propensa.

4.2 Como é tratada a segurança da informação nas MPEs

Quando o assunto é a segurança da informação no contexto de MPEs os recursos para pesquisa são escassos, visto que micros e pequenas empresas possuem a tendência de não darem atenção a esse assunto pelo fato de se considerarem muito pequenas dentro de um grande contexto nacional ou global. Apesar desta visão muitas vezes se confirmar em um contexto regional, a Internet atualmente transforma qualquer informação que trafega sobre

ela, alvo de roubo, interceptação, alteração ou simplesmente se perder na rede, contexto que contribui para a diminuição da confiabilidade do sistema de informação.

Outro aspecto muito negligenciado é a discriminação sobre a estrutura que asseguram a informação que começa no pensar que a segurança da informação é apenas garantir com ferramentas de software que seus recursos e equipamentos estejam livres de vírus e ataques maliciosos. Porém a segurança deveria se aprofundar tanto na adoção de ferramentas no contexto software, hardware, mas também no contexto estratégico de gestão de recursos físicos e humanos.

Algumas questões como o que está garantindo a confidencialidade e a disponibilidade de seus ativos se houver uma queda de energia? Quais os recursos disponíveis que garantem a segurança em caso de tentativa de roubo ao patrimônio da empresa? São questões importantes que são tratadas quando existe uma política de segurança da informação, e que estão inseridas no contexto ambiental de uma MPE e que não são tratadas como uma estratégia de governança dos ativos de TI. A falta de conhecimento ou talvez de recursos impeça que a MPEs satisfaçam essas necessidades que a *ISMS* impõe.

Trata-se agora do contexto de gestão de uma MPE e sobre como é tratado em dimensões estratégicas e organizacionais as implicações de *ISMS*.

De acordo com Thong (2001), as MPEs não costumam possuir um processo formal definido de gestão, muitas vezes o CEO são proprietários e tomam decisões sobre a maioria dos aspectos da empresa sendo eles tecnológicos, organizacionais, recursos humanos entre outros. Não ter um processo formal ou uma equipe especialista de tomada de decisões para certos assuntos muitas vezes cria dependências com a alta gestão e deficiências em alguns setores, pois as decisões são mais intuitivas do que estratégicas.

Outro aspecto bastante considerado por Thong é sobre a falta de planejamento a longo prazo. As MPEs possuem uma tendência de fazer planejamentos de curto prazo, que são menos burocráticos, menos complexos e possuem resultados mais rápidos porém tendem a não ser tão duradouros.

Ainda dentro da questão da estrutura de gestão, a falta de recursos é apresentada por Thong (2001) como sendo uma das problemáticas mais importantes quando se pensa em implementar uma estrutura de segurança da informação.

Facilmente se é encontrado argumentos de que a organização não é grande o suficiente ou não possui recursos suficientes para esse tipo de estrutura.

Também é discutido por (THONG 2001 apud GALÊS; WHITE 1981) sobre recursos de tempo que são tratados de maneira mais restritos em pequenas empresas, nos quais os colaboradores tendem a lidar com quantidades de responsabilidades maiores devido ao numero limitado de colaboradores. Esse argumento é confirmado quando os mesmos citam

que “As características únicas das pequenas empresas são seus exemplos de condições de pobreza de recursos, sob as severas restrições de tempo, financeiras e de especialização nas quais elas operam”.

Apesar de todas essas problemáticas, existe um lado positivo, que caso aconteça a implementação da ISMS em uma MPE é mais fácil de ser estruturada devido ao número menor de pessoas envolvidas, ao fluxo de informação que é consideravelmente mais baixo, custo de treinamento, adaptação, atualização são menores em relação a uma grande corporação.

4.3 Metodologia empregada

Sob a ótica de LAKATOS(apud Ander-Egg 1978), a pesquisa é “um procedimento sistemático, controlado e crítico, que permite descobrir novos fatos ou dados, em qualquer campo do conhecimento”. Com base no que foi dito, entende-se que uma pesquisa é um método de encontrar novas variantes, conceitos ou dados sobre determinado assunto.

De acordo com os objetivos do trabalho o desenvolvimento da etapa de levantamento foi utilizada os procedimentos de pesquisa para se atingir aos objetivos de trabalho.

De acordo com Lakatos (2003) a pesquisa um método ou procedimento formal de traça uma linha de pensamento reflexivo, e que necessita de métodos definidos para traçar um caminho para se descobrir verdades ou reconhecer a realidade estudada. O mesmo define que o desenvolvimento de uma pesquisa compreende nos seguintes passos:

1. Seleção do tópico ou problema para investigação
2. Definição e diferenciação do problema
3. Levantamento de hipóteses de trabalho
4. Coleta, sistematização e classificação dos dados
5. Analise e interpretação dos dados
6. Relatório do resultados da pesquisa.

A preparação da pesquisa foi elaborada conforme Lakatos define, onde os objetivos foram especificados e determinados para que fosse delimitada a natureza do trabalho e definido quais tipos de estudos e métodos seriam aplicados.

Na etapa de levantamento e coleta dos dados foram utilizados alguns procedimentos, a pesquisa bibliográfica que “é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados ao tema”. Onde a pesquisa bibliográfica e seus benefícios de ampliar o campo de conhecimentos sobre o tema que atrelado à pesquisa de contato direto, mais prática que fornece dados de fontes diretas e mais aplicáveis (LAKATOS, 2003).

A seleção dos métodos de pesquisa que foi empregada, delimita que os métodos sejam empregados de acordo com as necessidades específicas do problema em questão. Afirma-se ainda afirma que "A seleção do instrumental metodológico está, portanto, diretamente relacionada com o problema a ser estudado". (LAKATOS, 2003)

A escolha depende de diversos fatores que foram levados em consideração e julgados adequados para que o diagnóstico se adequa-se ao problema estudado bem como se confirma as variantes levantadas no procedimento de pesquisa bibliográfica.

A seleção dos métodos de avaliação da pesquisa de campo foi definida como qualitativa, foi escolhida pela exposição da necessidade avaliadas pela quantidade e não da quantidade.

Os objetos de estudos foram avaliados em caráter observatório dentro de sua natureza e fenômenos que são avaliados como numéricos e não numéricos, como cita Lakatos que a pesquisa qualitativa "é o conteúdo interno do processo de desenvolvimento, da conversão das mudanças quantitativas em mudanças qualitativas".

Baseadas nestas questões, a pesquisa regional realizada no Vale do Araranguá foi feita para entender o problema em raiz e sobre os mecanismos de segurança e, sobretudo o conhecimento do usuário sobre ferramentas ou requisitos, normas e estruturas de segurança e qual a sua capacitação sobre tal nas empresas da região.

Esta pesquisa foi realizada para dar uma capacidade de visualizar melhor onde está o problema, se os recursos estão sendo aproveitados ou se não há recursos suficientes para auxiliar e facilitar o acompanhamento da segurança da rede no setor MPEs no vale do Araranguá e identificar uma possível solução para tal. A seguir é demonstrada as características das empresas visitadas que estão dispostas na tabela 12.

Representação	Porte	Ocupação	Setor
Empresa 1	Micro empresa	7 colaboradores	Desenvolvimento de sites e artes digitais
Empresa 2	Pequena empresa	33 colaboradores	Provedor de serviços de internet
Empresa 3	Pequena empresa	12 colaboradores	Desenvolvimento de software
Empresa 4	Pequena empresa	50 colaboradores	Desenvolvimento de sistemas governamentais
Empresa 5	Pequena empresa	15 colaboradores	Desenvolvimento de aplicativos e sistemas comerciais

Tabela 12. Caracterização do porte, ocupação e setor das empresas avaliadas.

Fonte: Realizada pelo autor

Assim sendo, o levantamento foi feito através de uma pesquisa com questões relevantes ao tema utilizando técnicas de aplicação de questionário e de um bate-papo aberto depois da análise documental sobre o tema.

Com a soma das coletas dos dados a da pesquisa documental foi possível obter resultados que ajudassem a entender as principais dificuldades ou o porquê que uma MPE não possui uma estrutura adequada de segurança da informação ou até de suporte as TICs.

Os resultados foram obtidos utilizando dois dos procedimentos definidos por Lakatos, através da pesquisa bibliográfica e de contatos diretos.

Através da pesquisa bibliográfica foi elaborada questões consideradas relevantes ao tema e aos objetivos pretendidos para que assim o suporte desta análise documental servisse como base de conhecimento para a visita às empresas para que o material coletado fosse apanhando de maneira adequada, através de uma pesquisa com questionário anexo e de um bate-papo aberto realizado em cada uma das empresas após a entrevista. Os resultados desta coleta estão apresentados na seguinte seção.

4.4 Levantamento

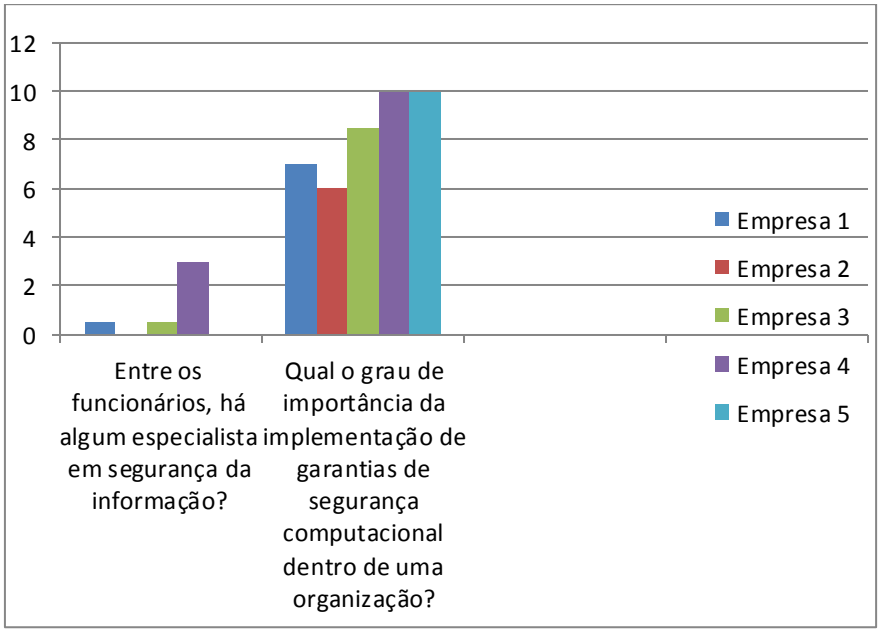

Gráfico 1 Representação do número de especialistas formalmente contratados e do grau de importância observado da área para a organização.

Fonte: Realizada pelo autor

Conforme o gráfico 1 demonstra a questão que ressalta a dúvida sobre a existência de funcionários especialista em segurança da informação.

O critério utilizado para definir 0,5 empregados definidos na empresa número 1 destacada em azul e da empresa número 3 destacada em verde foi que ambas possuíam profissionais que indiretamente tratavam de assuntos relacionados a segurança da informação porém eles não eram formalmente contratados para a área.

Com base no que foi respondido, entre as empresas que foram abordadas somente uma, a empresa de número 4 possuía especialistas formalmente contratados para a área correspondente.

Já na questão do gráfico que aborda qual o grau de importância na opinião do entrevistado sobre implementações de segurança da informação, é demonstrado que apesar de não haver nenhum funcionário na área de segurança grande parte dos entrevistados consideraram a área muito importante para a segurança informacional da organização.

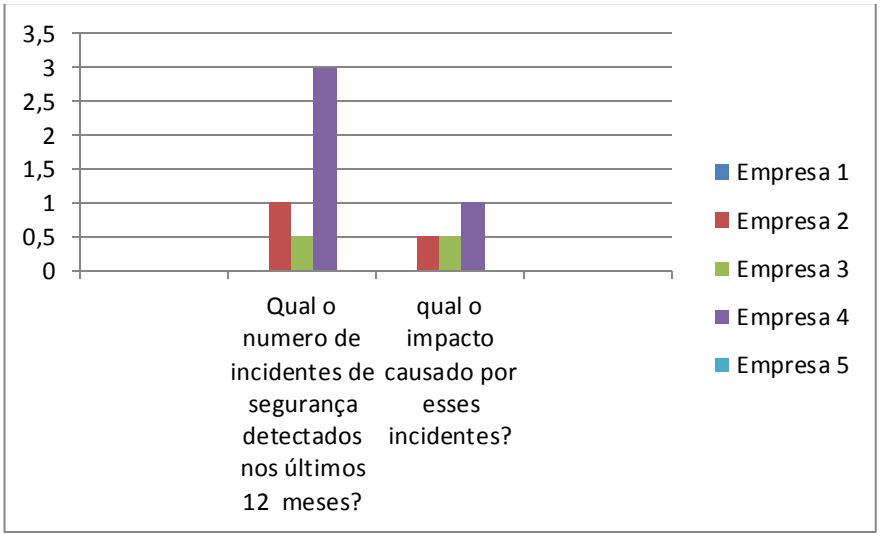

Gráfico 2 Representação do número de incidentes nos últimos 12 meses e do impacto causado pelos incidentes dentro da organização.

Fonte: Realizada pelo autor

O gráfico 2 indica o número de incidentes ocorridos em um período de 12 meses, no qual demonstra que somente a empresa de número 4 foi vítima de 3 incidentes no período de 12 meses.

Porém quando fora explicitado que quedas de energia, perda de dados, roubo são considerados incidentes de segurança a empresa 2 relatou uma queda de energia que acarretou em problemas, e a empresa 3 relatou uma tentativa de roubo ao patrimônio da empresa que por não ter sido concretizada foi representado no gráfico como meio incidente.

Visto isso, os índices não foram considerados alto com uma média de 1,5 anuais, sendo assim o impacto causado pelos mesmos é diretamente proporcional aos incidentes acusados.

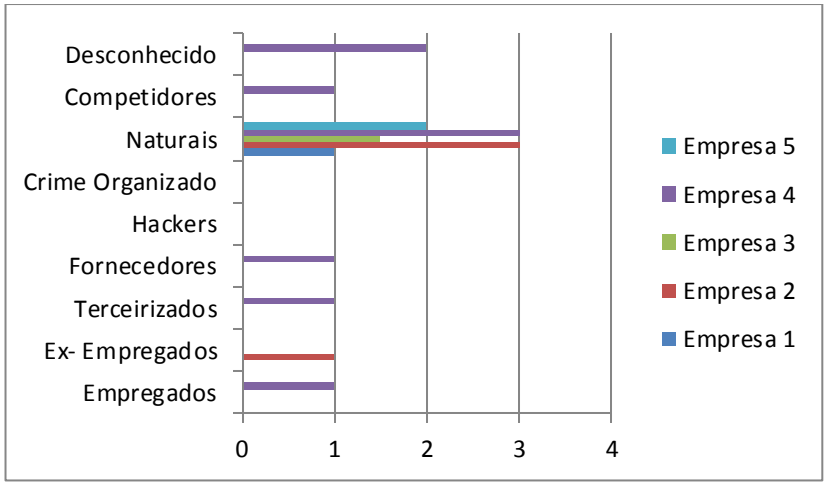

Gráfico 3 Representação das causas dos incidentes relatados.

Fonte: Realizada pelo autor

O gráfico 3 acusa as causas dos incidentes relatados nos últimos 12 meses e foi demonstrado por quantidade de incidentes no qual os números de 0 a 4 indicam o número de vezes que determinado incidente ocorreu dentro da organização.

Visto isso, o gráfico demostra que a estimativa de causas dos incidentes em sua grande maioria foram naturais, desconhecidas, e as outras que são inexistentes ou iguais a um.

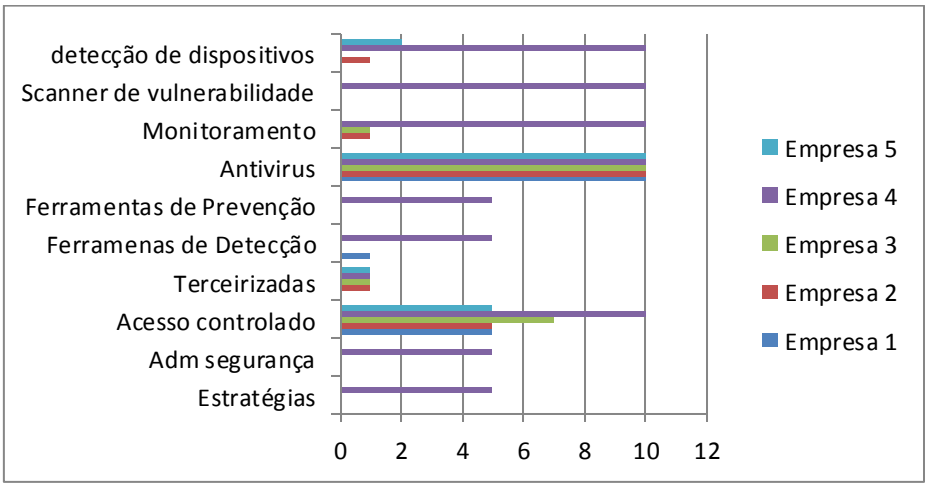

Gráfico 4 Representação das ferramentas de segurança da informação implementada na organização.

Fonte: Realizada pelo autor

Sobre os mecanismos de segurança utilizados foram detectados algumas variantes comuns entre as empresas levanto em conta que os mais frequentemente utilizados foram demonstrados pela numero 10 e os menos utilizados foram demonstrados pelo grau de importância explicitado durante a respostas dos gestores.

Visto isso foi observado que os mais utilizados são os mais genéricos, e os mais citados, ou seja, antivírus e acesso controlado, por serem fáceis de utilizar e implementar, enquanto os mais característicos de ambientes de segurança suas variantes no gráfico foram menores ou inexistentes.

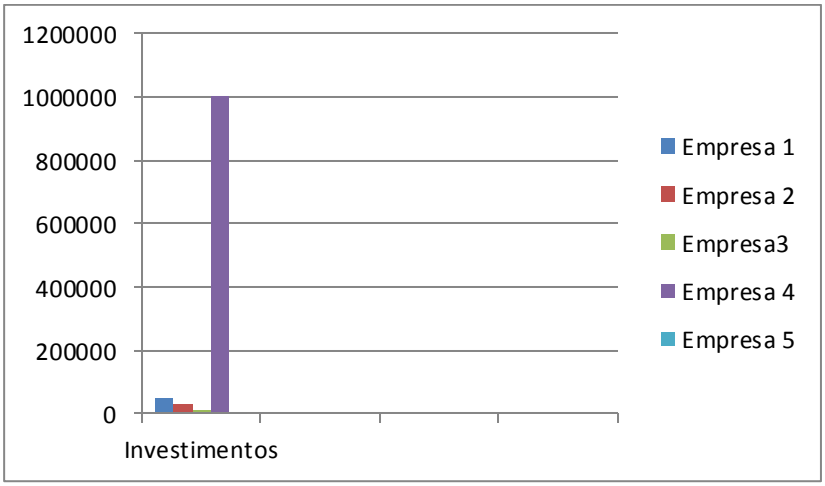

Gráfico 5.Representação em reais do valor de investimento formalmente declarado na área.
Fonte: Realizada pelo autor

Como demonstrado no gráfico a questão que aborda os investimentos futuros ou antigos realizados, foi constatado que a quantidade de investimento que o setor de segurança recebe anualmente é muito baixo visto que grande parte das empresas entrevistadas não possuíam o setor de segurança, ou recursos disponíveis para a implantação de tais estruturas, porém algumas relatavam que havia investimento em segurança indiretamente através de outros setores.

Após a realização das perguntas foi realizada em cada uma das empresas, uma conversa aberta sobre as dificuldades que as mesmas possuíam em relação ao tema, quando foram discutidas questões de perda de dados, falta de backup, quedas de energia, e até roubo são requisitos que entram no contexto da estrutura da segurança da informação. Foi notado que houve uma melhora no quadro de preocupação com o tema e de investimento sobre tal.

A partir disto é demonstrado que a falta de conhecimento dos gestores tem sido um problema que a segurança da informação tem enfrentado na região.

Outro fato que passou a existir dentro da conversa foi a questão de falta de experiência de colaboradores e que os mesmos estevam sobrecarregados o que muitas vezes foi descrito que grande parte dos colaboradores levavam trabalho para suas residências tornando o dado vulnerável e suscetível a danos, perda ou roubo.

Baseado nesses resultados foi possível entender as barreiras enfrentadas neste setor. No decorrer da investigação foi percebido que o usuário é um dos maiores problemas quando se

trata de segurança computacional, visto que existe alto grau de receio além de uma falta de treinamento muito grande sobre alguns requisitos considerados básicos, nas duas das maiores empresas analisadas, empresa 4 com cerca de 50 colaboradores e empresa 2 com aproximadamente 33 colaboradores, constatou-se que em somente uma possuía estratégias de segurança, porém ambas documentaram que o usuário não educado e familiarizado com a políticas de segurança da organização se tornam um problema. Muitas vezes os mesmos realizam praticas não autorizadas ou que ferem às normas de segurança por falta de conhecimento ou por comodidade, destacando ainda que uma vez que os padrões de segurança são implantados, estes trazem um nível de desconforto e menos liberdade para o usuário que muitas vezes reclama da dificuldade de realizar tarefas pelo nível de segurança imposto.

Isto dificulta a implantação de alguns mecanismos nas empresas que demoram a adota-los até se deparar com situações que as obrigam a impor tais práticas, foi o que aconteceu na empresa de número quatro.

No transcorrer da pesquisa também foi notado que nas empresas menores como a empresa de número 1 com 7 colaboradores , a empresa 3 com 12 e por fim a empresa 5 com 15 colaboradores, os gestores entrevistados acreditavam que a segurança era importante e sabiam da existência das normas e padrões de segurança da informação, porém, admitiram ter um conhecimento ralo e não as tinham implantadas em sua organização, assim sendo foi lançado a pergunta do porque tais normas não são praticadas, e com base nas respostas foi feito uma média de que cerca de 6,8% das empresas entrevistadas acreditavam que o orçamento de segurança é muito alto para o porte da empresa e 1,3% admitiu ser por falta de conhecimento na área e 2,1% por estarem sobrecarregados e não terem tempo.

Em contrapartida as duas outras maiores empresas visitadas alegaram que a criação da estratégia de segurança é satisfatória e um aspecto básico para a estrutura da empresa.

Então se conclui que o investimento e a implementação de políticas e ferramentas de segurança está diretamente proporcional ao porte da empresa.

Esta problemática, tentar incluir as boas práticas de governança em TI (ITIL, ISO/IEC 27001) para ajudar a satisfazer as necessidades de pequenas empresas, e ao mesmo tempo em que se encaixe em seu contexto organizacional e minimize riscos de rejeição e grandes custos de implementação. Essas são as principais questões nas quais inúmeras universidades do mundo inteiro vêm desenvolvendo pesquisas na área, que estão começando a responder questionamentos sobre o porquê das falhas do descaso e da aplicação em novos requisitos de segurança em meios de tecnologia.

4.5 Identificações do novo modelo para MPEs

A partir das informações analisadas da ISO 27001 e do ITIL considerando os processos e políticas que foram estudados são evidentes as necessidades que em suma devem ser praticadas para cobrir as obrigações e normas que são necessárias para um bom funcionamento geral da organização. Elas nos oferecem um conjunto de requisitos que provê a organização e normalização de como possuir uma estrutura de TI e de governança da informação segura e tecnicamente efetiva.

Ambas as técnicas já foram discutidas em seus contextos, requisitos e processo e agora chega o momento em que ambas devem alinhar-se de acordo com o também visto, modelo estrutural de micros pequena empresa e seus parâmetros e requisitos, com intuito de que que este novo modelo de boas práticas cubra todas as necessidades e questões críticas encontradas em uma MPE.

A ITIL em todos seus princípios e requisitos tem como característica principal orientar o gerenciamento da TI e seus serviços dentro de uma organização, enquanto a mesma pode ser usada como uma ferramenta para alcançar a objetivos que envolvem a segurança da informação através de uma estruturação de processos e serviços que permitem que esse objetivo seja alcançado, A ISO/IEC 27001 tem como objetivo único gerenciar a organização em prol da segurança da informação, seu conjunto de boas práticas e requisitos possibilita que o contexto de segurança seja coberto de maneira eficaz, eficiente e consistente. As duas práticas possuem muitas processos em comum, visto que ambas tratam da gestão de estruturas de TI. Apesar de suas similaridades, Juntas possuem um alinhamento da estrutura de TI com as estratégias de negócio voltadas às boas práticas de gestão do mercado levando em consideração os aspectos de segurança desses ativos.

Hoje o desafio é combinar esse conjunto de boas práticas que ambas suportam, dentro do ambiente limitante e desafiador que existe no contexto de micros e pequena empresa.

Levando em conta o tópico discutido sobre como é tratado esta problemática em uma MPE, no qual é discutido os principais problemas que são encontrados dentro deste contexto, e explicitado quais são suas necessidades mais emergenciais, a partir dessa análise de necessidade sobre uma MPE é proposta um conjunto de questões que define a partir das resposta, todos os requisitos que devem ser garantidos pelos processos e práticas da ITIL e ISSO 27001. As questões são as seguintes:

- Quais as maiores problemáticas enfrentadas no escopo de estrutura de uma MPE?
- Quais dessas problemáticas impactam no escopo de segurança e estrutura da TI?

- Quais os grupos de variáveis que impactam diretamente no contexto de segurança ISO e estrutura ITIL?
- Quais os grupos de constantes que devem ser respeitados?

A partir dessas perguntas foi possível identificar requisitos importantes que permeiam o comportamento organizacional mais característico observado em uma MPE, na tabela a seguir é determinada as constantes da MPE que foram consideradas e que devem ser tratadas:

Variáveis	Comportamento
Perfil do gestor	O perfil do gestor muitas vezes não se encaixa no papel de líder, resultando em um ambiente em que os colaboradores se sentem pouco a vontade.
Perfil da empresa	O perfil da empresa muitas vezes não é levado em conta quanto a tomada de decisões ou no próprio negócio e gestão dos colaboradores.
Administração de Ferramentas	Colaboradores inexperientes ou não capacitados não sabem tirar o máximo proveito das ferramentas disponíveis.
Valor da informação	A falta de conhecimento faz com que o valor da informação não seja respeitado pelo grupo de colaboradores, trazendo consequências como ser violação, perda ou modificação.

Tabela 13. Variáveis consideradas referentes a estrutura MPE. Fonte: Sebrae, 2010

Constantes	Comportamento
Resultados	Em pequenas empresas normalmente o impacto de resultados é colhido através da produtividade de seus colaboradores e nas suas entregas aos clientes, os resultados devem ser definidos em uma prévia avaliação e discutido e demonstrado a todos envolvidos para que os objetivos e metas sejam alcançados e melhorados continuamente.
Planejamento	Foi constatado que MPEs possuem escassos planejamentos de longo prazo, fazer grandes projetos e investimentos a longo prazo solidifica a estrutura da organização e resulta em investimentos duradouros, além de trazer eficiência na utilização de recursos de tempo e dinheiro que um processo formalizado acarreta.

Tempo	O tempo limitado é um requisito que impacta nos processos realizados na empresa, por isso é importante dividir e definir processos e tarefas por cargo ou departamentos para que nenhum colaborador ou gerente se sinta sobrecarregado.
Recursos	O recursos limitados é uma constante características de uma MPE, muitas vezes ela é piorada por um gestor que não tem habito de fazer controle de gastos ou evita fazer investimentos quando necessário por economia, é preciso saber no que gastar, quando gastar e como gastar para uma gestão eficiente dos recursos financeiros.
Especialidades	Em muitos casos de MPEs existe uma politica familiar de contratação e também de contratação de profissionais genéricos, a falta de especialistas e de profissionais que saibam o que estão fazendo resulta no chamado "faz tudo mas não faz nada" o que acaba sendo um recurso dispendioso e mal aproveitado para a organização.

Tabela 14. Constantes consideradas na estrutura MPE. Fonte: Sebrae

Partindo desses comportamentos e das variáveis e constantes definidas, foi possível modelar quais os requisitos de ambas estruturas que devem levados em conta na estruturação desse novo modelo para que todas as necessidades e requisitos sejam supridos.

Subsequente a isso foram elaboradas as seguintes questões que foram respondidas pelo autor levando em consideração a pesquisa bibliográfica que explorou as características encontradas dentro de uma MPE e das práticas que foram julgadas importantes e aplicáveis dentro deste segmento de MPE, para assim, facilitar o entendimento da elaboração até a finalização deste novo modelo.

Questão 01. Quais requisitos que compõe o fluxo *PDCA* no contexto ISO/IEC 27001 são relevantes para a organização?

- Contexto organizacional
- Contexto de liderança
    - Liderança e compromisso
    - Estabelecimento de politicas de segurança
    - Estabelecimento de papeis organizacionais e responsabilidades
- Contexto de planejamento

- Estabelecer e responder questões gerais sobre metas e parâmetros importantes que devem ser atingidos e que cobrem o contexto organizacional definido, e um planejamento de como alcançá-los.

- Contexto de suporte
  - Comunicação entre as partes relacionadas
  - Documentação da informação
- Contexto de avaliação de desempenho
  - Análise e avaliação dos projetos e suas metas alcançadas e dificuldades

Questão 02. Quais os requisitos que compõe o ciclo de vida de serviços ITIL são relevantes para a organização?

- Serviço de Estratégia
- Serviço de Design
- Serviço de Operações
- Serviço de Melhoria continua

Questão 03. Como ficaria esse novo ciclo de vida? Quais seriam seus componentes e como eles estariam organizados? Esses requisitos de forma que eles fiquem alinhados em prol das necessidades organizacionais?

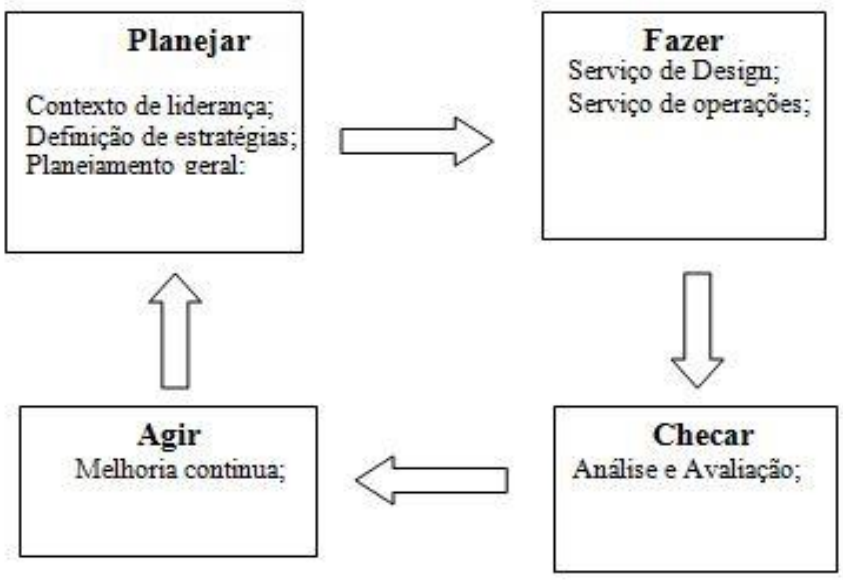

Figura 9. Modelo de ciclo de vida baseado em *PDCA* Fonte: Realizada pelo autor

Questão 04. Como o alinhamento desses processos ficaria organizado de forma que eles atendam às necessidades organizacionais?

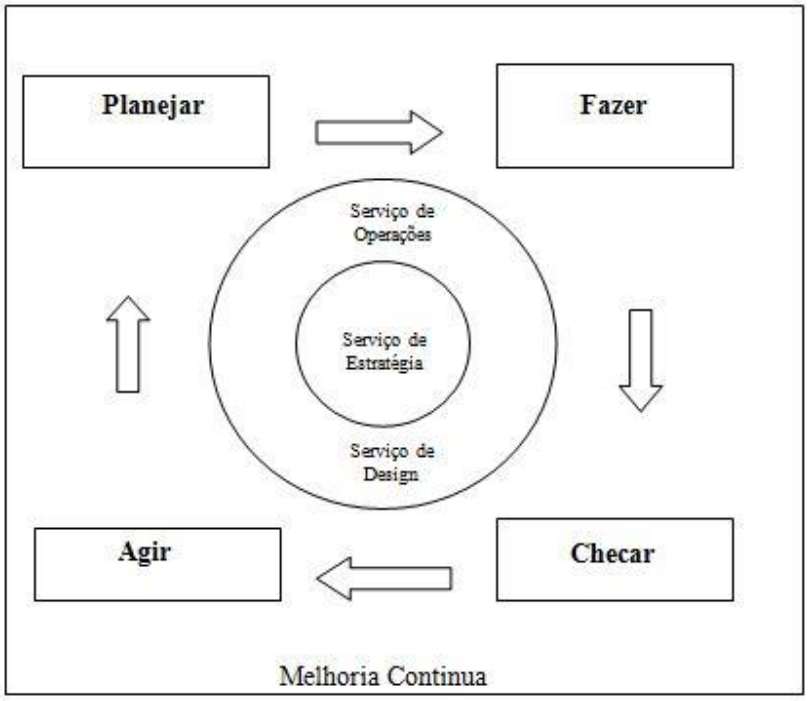

Figura 10. Modelo de passos do processo baseado em PDCA e ciclo de vida ITIL. Fonte: Realizado pelo autor

Existem diversos e variados pontos em que os dois modelos podem ser interconectados dentro de seus processos, ambos podem ser considerados complementares um para o outro.

Enquanto a ITIL possui um foco na gestão dos processos de TI a ISO 27001 está focalizada nas melhores práticas de segurança da informação, ao perceber isso e depois de investigarmos sobre um contexto específico, o de MPEs, foi possível fazer uma combinação dos processos que serão mais uteis no cotidiano de uma MPE. Depois de terem sido respondidas diversas questões sobre este novo modelo agora será explicitado o por que da inclusão desses processos e quais os benefícios que os mesmos resultam no âmbito de uma micro e pequena empresa.

Como ponto inicial observa-se o ciclo de vida PDCA que se pode encontrar tanto nos processos da ITIL como no da ISO 27001. Mantêm-se então alguns conceitos que ajudam na formalização dos processos que uma empresa independente de seu porte deve possuir.

Na etapa de planejamento é um momento no qual se define tudo o que a empresa representa, em que escopo ela está inserida, quais são seus objetivos e como esses objetivos serão alcançados. É nesta etapa em que o planejamento estratégico e de processos são definidos e alinhados com as necessidades e contexto da organização, além de definir e deixar claro o papel de cada líder dentro desse processo.

Esse é um comportamento que se considera crucial e que deve estar enraizado e claro para a equipe de governança ou para o dono da empresa pois é um processo no qual todos os outros se baseiam. Uma pergunta muito relevante que pode ser feita diante deste processo é como essa etapa absolutamente administrativa implica no processo de segurança da informação?

Através de processos claros e formalizados, eles são fáceis de ser compreendidos, seguidos e mudados, quando existe uma falha, ameaça ou risco em algum requisito de segurança é possível fazer os passos reversos do processo de gestão para reconhecer de onde o erro está vindo, reduzir desperdícios, diminuir tempo de processamento, fazer o reparo e atualizações, ou para simplesmente entender a estrutura do negócio e suas necessidades para assim atendê-las de maneira mais eficiente e eficaz, pois compreendendo as necessidades exigidas pelos processos que envolvem o negócio é mais fácil administrá-lo de forma que evite qualquer dano que possa ser causado que afete de alguma forma a disponibilidade, confiabilidade e qualidade tanto em âmbito de processos e tomadas de decisões internas, como no produto ou serviço oferecido pela organização.

Subsequente a isso no ciclo existe o processo de Fazer (Do), que engloba as características ITIL de design de serviço e serviço de operações, e também é tratado na norma sob o ponto de vista operacional.

A partir disto é necessário manter os componentes extraídos na etapa de planejamento e agir conforme foi objetivado, manter padrões de processos e métricas que ajudam a manter a consistência operacional e o alcance de objetivos e metas de forma sólida.

Todos esses processos julga-se importantes para uma empresa, principalmente, quando a mesma possui metas a atingir e uma qualidade de processos e produto a atender, e como demonstrado na pesquisa anteriormente. Boas práticas e processos formalizados e consistentes implicam diretamente no cumprimento de prazos e entregas, consistência do produto ou serviço bem como sua qualidade.

Todas as variantes que são notadas pelo cliente final o que resulta para a empresa como vantagem competitiva em um nicho de uma MPE na qual está inserida.

Adiante, no ciclo encontra-se a etapa de checagem, que dentro deste contexto engloba processos de análise e avaliação tanto do desempenho da equipe como do produto ou serviço do negócio, acredita-se na importância de entender e enxergar quais os obstáculos enfrentados para atingir os objetivos acertados no processo de planejamento, além de ter a oportunidade de visualizar os problemas ocorridos durante a fase de processamento para enfim, avançar para a fase de Agir, que baseia-se em programar ações corretivas que melhorem o processo e sua qualidade.

Esta é a fase na qual se introduz a rotatividade do ciclo, fazendo com que a gestão da organizacional da infraestrutura de segurança da informação seja tratada como um organismo vivo que mesmo com processos fixos é capaz de se adaptar e estar sempre evoluindo em um processo de melhoria contínua.

Esta é uma etapa que julga-se importante para uma micro pequena empresa que busca estar sempre conectada com as tendências de mercado, o que faz com que sejam diferenciadas de suas competidoras e se torna uma vantagem competitiva, pois é um processo que as ajudam a acompanhar as tendências de mercado e as deixa capaz de atualizarem-se e serem diferenciadas ou adquirir esse diferencial que as destaque do seu ambiente competitivo.

Englobando todos esses processos é importante enxergar que a governança de TI e as boas práticas de segurança são um importante objeto de medição de qualidade e competências que poucas MPEs conhecem ou exploram.

Essas técnicas que não somente englobam a segurança de ativos da informação, mas que através de suas boas práticas resultam em processos bem definidos que derivam na melhor utilização de recursos físicos, lógicos e humanos, reduzem custos, evita erros, fraudes, diminuem consequências de acidentes maliciosos ou naturais, protege o ativo informacional da empresa e melhora a qualidade do serviço ou produto. Assim sendo nota-se que estes são todos importantes requisitos que fazem "O diferencial" que as empresas procuram, e principalmente as micros e pequenas empresas que estão inseridas em um espaço no qual qualquer vírgula faz a diferença entre o cliente escolher a empresa do João ou a empresa de Maria.

5 CONCLUSÃO

O ambiente organizacional de micros pequena empresa é desafiador,. Por ser pequena ela se torna dinâmica e livre de processos e estruturas definidas. Ao tratar de gestão de boas práticas e governança de TI torna-se uma problemática que é pouco vista e abordada, visto que através do levantamento regional realizado, demonstra-se que as MPEs não se atentam a uma estrutura de segurança da informação e muito menos de suporte a TI.

Observa-se que a segurança da informação possui estereótipos a serem quebrados e barreiras a serem ultrapassadas, pois em muitas MPEs a mesma é tratada como estrutura para grandes empresas ou como um luxo caro e dispendioso.

Quando as normas e padrões são tratados observa-se que ela possui um contexto muito além que a de se proteger de hackers e vírus de computadores, percebe-se que a estrutura de

governança de TI ITIL é uma ferramenta extremamente útil para a gestão desses ativos que acarretam processos consistentes, melhoria na qualidade, redução de custos e aumento no alcance de metas. Apesar disso, partindo do levantamento realizado, considera-se que o investimento e a implementação de políticas e ferramentas de segurança está diretamente proporcional ao porte da empresa, ou seja, quanto maior a empresa maior a atenção e investimento em *SGSI* possui.

O desafio atualmente é difundir a necessidade do modelo para uma MPE e implementar as boas práticas de governança em TI (ITIL, ISO/IEC 27001) para ajudar a satisfazer às necessidades de pequenas empresas, e ao mesmo tempo que se encaixe em seu contexto organizacional e minimize riscos de rejeição e grandes custos de implementação.

Essas são as principais questões nas quais inúmeras universidades do mundo inteiro vêm desenvolvendo pesquisas na área, que estão começando a responder questionamentos sobre o porquê do descaso sobre o assunto de segurança da informação e da aplicação de requisitos de segurança em meios de tecnologia dentro dos ambientes de micro e pequenas empresas.

Esta é uma problemática, e motivação para implementação deste modelo e para trabalhos futuros para obtenção de dados e resultados mais conclusivos.

6 TRABALHOS FUTUROS

Nesta seção estão listadas algumas propostas para trabalhos futuros:

- Fazer a aplicação prática deste modelo em micro ou pequena empresa
- Realizar a avaliação de resultados dos efeitos e consequências de aplicação deste modelo neste segmento de mercado.
- Avaliar o nível de aceitação do segmento sobre a estrutura de segurança da informação aplicada as MPEs.

7 REFERÊNCIAS

ABNT. **ABNT NBR ISO/IEC 17799: tecnologia da informação: técnicas de segurança - código de prática para a gestão da segurança da informação**. ABNT. Rio de Janeiro**:** 120pg p. 2005.

ARRAJ, V. ITIL: the basics. **AXELOS**, 04/06/2015 2013. Disponível em: < http://www.best-management-practice.com/gempdf/itil_the_basics.pdf >.

BAGCHI, A. S. C. M. A. **A formal methodology for detection of vulnerabilities in a enterprise information system**. Risk and security of internet and systems (Crisis) 2009 fourth international conference Indian Statistical institute 2009.

BAR, A. A. **PKI ASSESSMENT GUIDELINES**: AMERICAN BAR ASSOCIATION 2003.

BSI. **The new ISO/IEC 27001:2013 structure**. BSI 2014.

CAMPONAR, L. O. C. M. C. Micro e pequenas empresas: Caracteristicas estruturais e gerenciais. Faculdade de administração, Economia e Contabilidade da Universidade de São Paulo FEA/USP, 2004. Disponível em: < http://www.unifafibe.com.br/revistasonline/arquivos/hispecielemaonline/sumario/10/19042010081633.pdf >. Acesso em: 11/06/2015.

CLAYTON S.SILVA, A. C. M. R., DANIEL F. CHAIM, ROBERTO J. CARVALHO, VANESSA C. G. CHIMENDES. **Engenharia Social: O elo mais frágil da segurança nas empresas**. Revista Eletrônica do alto Vale do Itajaí: REAVI. 02 2012.

COMUNICAÇÕES, D. D. S. D. I. E. **Gestão de riscos de segurança da informação e comunicações - GRSIC**. 04/IN01/DSIC/GSI/PR 2013.

CROVITZ, L. G. The white Hats vs Black Hats. **The Wall Street Journal**, 2013.

DIGITAL, O. Qual a diferença entre hacker e cracker? **Olhar Digital**, 2013. Disponível em: < http://olhardigital.uol.com.br/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024 >. Acesso em: 20/05/2015.

E. H. DINIZ, T. A. Gestão de Segurança em Internet Baking: Estudo de casos Brasileiros. 17/12/2014 2010. Disponível em: < http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/2339/67929.pdf?sequence=3&isAllowed=y >.

G. C. BOWKER , D. R., F. MILLERAND, K. BAKER, D. RIBES. TOWARD INFORMATION INFRASTRUCTURE STUDIES: WAYS OF KNOWING IN A NETWORKED ENVIRONMENT. **international handbook of internet research**, 2010.

HARRIS, S. **CISSP Certification: all-in-one**. United States of America: McGraw-Hill/Osborne, 2002.

IBGE, I. B. D. G. E. E.-. Pesquisa Sobre o Uso das Tecnologias da Informação e Comunicação nas Empresas. **IBGE**, 2010.

ISO/IEC. **ISO IEC 27001 Information technology - Security techniques - Information security management systems - Requirements**. ISO/IEC. Geneva: ISO copyright office**:** 32 p. 2013.

KUROSE, J. F. **Redes De Computadores e a Internet**. Pearson, 2010. 614

LAKATOS, M. D. A. M. E. M. **Fundamentos de metodologia científica**. 5º. São Paulo: Editora ATLAS, 2003.

MDICE, M. D. D. I. E. C. E. **Novo Estatuto da ME EPP REGULAMENTAÇÃO DA LEI Nº 9.841**. EXTERIOR, M. D. D. I. E. C. 1999.

MICHAEL E. WHITMAN, H. J. M. **Principles Of Information Security**. 4. Boston: 2011.

MICHAELIS. MICHAELIS: Editora Melhoramentos ltda. 2009.

MODIRI, R. S. N. A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. **Indian Journal of Science and Technology,** v. 5, n. 2, Feb 2012 2012.

MOURA, J. N. D. A. H. P. D. Implantando a Gestão de Serviços de TI: Uma abordagem horizontal baseada no catalogo de serviços de TI. Recife, 2007. Disponível em: < http://www.lbd.dcc.ufmg.br/colecoes/sbsi/2008/0016.pdf >. Acesso em: 11/06/2015.

NFS, C. C. NSF's Cyberinfrastructure vision of 21st century discovery v. 7.1, 16/12/2014 2006. Disponível em: < http://www.nsf.gov/pubs/2007/nsf0728/nsf0728.pdf >.

OGC, O. G. O. C. Service manual Operations service management UK, 2014. Disponível em: < https://www.gov.uk/service-manual/operations/service-management.html >. Acesso em: 11/06/2015.

PELTIER, T. R. **INFORMATION SECURITY FUNDAMENTALS**. Second edition. CRC press: Taylor & francis group, 2013.

QUINTAO, B. D. P. R. L. M. S. P. L. **Segurança da informação: difinições, mecanismos, mercado e estratégia de negocio**. XXV Encontro Nac. de Eng. de Produçao. Porto Alegre 2005.

RHODES-OUSLEY, M. **Information Security The Complete Reference**. 2th. The McGraw-Hill Companies, 2013. 833

ROSA, I. B. D. Segurança de sistemas de informação na cidade da Praia. consultado dia 22/12/2014 2004. Disponível em: < Disponível em http://bdigital.unipiaget.cv:8080/jspui/bitstream/10964/241/1/Seguranca%20dos%20SI%20na%20Praia%20-%20V2.pdf >.

SCHNEIER, B.; VIEIRA, D. **Segurança.com: segredos e mentiras sobre a proteção na vida digital**. Campus, 2001. ISBN 9788535207552.

SEBRAE. Participação das Micro e Pequenas Empresas na Economia Brasileira. Serviço Brasileiro de apoio as micros e pequenas empresas unidade de gestão estratégica - UGE, 2014a. Disponível em: < http://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Estudos%20e%20Pesquisas/Participacao%20das%20micro%20e%20pequenas%20empresas.pdf >. Acesso em: 11/06/2015.

_____. Perfil dos pequenos negócios. 2014b. Disponível em: < http://www.sebrae.com.br/sites/PortalSebrae/estudos_pesquisas/Quem-s%C3%A3o-os-pequenos-neg%C3%B3cios%3F,destaque,5 >. Acesso em: 11/06/2015.

TANENBAUM, A. S. **Computer Networks**. 5TH. Pearson, 2011.

TECHEXCEL. ITIL Implementation and Process Guide. 04/06/2015 2012. Disponível em: < http://www.techexcel.com/resources/TechExcel_ITIL_Guide.pdf >.

THONG, J. Y. L. Resource constraints and information systems implementation in Singaporean small businesses. **Omega** n. 143-156, p. 14, 2001.

TSO. **An Introductory Overview of ITIL 2011**. London: itSMF ltd, TSO 84 p. 2012.

TSO, I. **O ciclo de vida dos serviços ITIL**. London: TSO**:** Figura 3 p. 2012.

VERHEIJEN, A. D. J. A. K. M. P. R. T. A. V. D. V. T. **ITIL V3 Foundation Exam - The Study Guide**. First. Van Haren Publishing, Zaltbommel, 2008. ISBN 978 90 8753 069 3.

YOURDON E. **Byte Wars: The impact of september 11 on information technology**. Prentice Hall 2002.

ANEXO

A pesquisa

Dados Gerais

1. Nome/Função do entrevistado:
2. Qual a principal área de atuação desta empresa?
3. Qual o número de funcionários?

Opinativa

4. Entre os funcionários, há algum especialista em segurança da informação? Se sim, quantos?

5. Existe uma estrutura formal (departamento ou terceiros) que tratam da segurança da informação?

6. Em sua opinião profissional qual o grau de importância da implementação de garantias de segurança computacional dentro de uma organização?
    - Alta
    - Moderada
    - Neutra
    - Nenhuma
7. Se fosse pra implementar algum mecanismo quais seriam?

8. Qual a importância que sua organização trata a segurança da informação?

9. Você está familiarizado com as vantagens ocasionadas na implementação de uma infraestrutura adequada da informação em uma organização?

Incidentes

10. Qual o numero de incidentes de segurança detectados nos últimos 12 meses?

    - 0 ou nenhum
    - 1 a 9
    - 10 a 40
    - 50 ou mais

- Não sei

11. Qual foi a estimativa da provável fonte dos incidentes de segurança?

- Empregados
- Ex- empregados
- Terceiros contratados (terceirizadas)
- Fornecedores, parceiros,sócios
- Hackers
- Crime organizado
- Ativistas
- Competidores
- Desconhecido

12. Qual foi o impacto causado pelo incidente de quebra de segurança?

- Informações de clientes foram comprometidas
- Informações de funcionários foram comprometidas
- Informações foram roubadas
- Perda de informações, quebra maquinas ou servidor derrubado
- Reputação da organização foi manchada
- Má exposição legal

Investimento

13. Existe algum tipo de controle de gastos direcionados para projetos desse contexto?

14. Qual o orçamento anual alocado para projetos de implementação, melhoria ou controle da segurança da informação?

- pequeno
- médio
- inexistente
- não sei

Mecanismos

15. Que tipo de mecanismos de prevenção da informação sua organização possui?

- Estratégias de segurança específica aliada as necessidades do negócio
- Foi contratado um administrador de segurança
- Acessos de segurança controlados
- Treinamento de empregados e conscientização das práticas de segurança praticadas dentro da empresa
- Contratação de organizações terceiras especializadas
- Não possui
- Não sei

16. Quais implementações de segurança relacionadas a proteção sua organização possui?

- Acesso controlado
- Criptografia de e-mail e mensagens
- Ferramentas de detecção de intrusão
- Ferramenta de prevenção de perdas
- Não possui
- Não sei

17. Quais implementações de segurança relacionadas a detecção de intrusão sua organização possui?

- Ferramentas de detecção de intrusos
- Antivírus
- Ferramentas de monitoramento de acesso não autorizado
- Ferramentas de monitoramento da informação
- Scanner de vulnerabilidade
- Ferramenta de detecção de dispositivos não autorizados
- Não possui
- Não sei

18. Quais implementações relacionadas a resposta e prevenção sua organização possui?

- Eventos e cursos de atualização de novas técnicas para administradores de segurança
- Sistema tático de recuperação da consistência e segurança da informação

- Não possui
- Não sei

19. Você conhece as normas de padronização de garantias de segurança da informação ISO 27000/27001 ou 27002?

    - Sim
    - Não
    - Não sei

20. Sua organização possui certificação ISO 27000/27001 ou 27002?

    - Sim
    - Não
    - Não sei

21. Você conhece a infraestrutura ITIL?

    - Sim
    - Não

22. Sua organização possui implementado alguns tipo de processos que estão relacionados aos processos ITIL? De seu conhecimento?

    - Sim
    - Não
    - Não sei

23. Quais as políticas de segurança implementadas em sua organização?

Dificuldades

24. Quais as dificuldades encontradas na organização ao implantar esses mecanismos?

Satisfação

Qual o grau de satisfação com as ferramentas de proteção que sua organização utiliza?